GENEROLO JONO ŽEMAIČIO LIETUVOS KARO AKADEMIJA
GENERAL JONAS ŽEMAITIS MILITARY ACADEMY OF LITHUANIA

JUNGTINIŲ TAUTŲ IR EUROPOS SĄJUNGOS INFORMACIJOS APSAUGA

NORMINIŲ TEISĖS AKTŲ RINKINYS

LEGISLATIVE INSTRUMENTS REPORT

THE PROTECTION OF THE UNITED NATIONS AND THE EUROPEAN UNION INFORMATION

GENEROLO JONO ŽEMAIČIO LIETUVOS KARO AKADEMIJA

JUNGTINIŲ TAUTŲ IR EUROPOS SĄJUNGOS INFORMACIJOS APSAUGA

NORMINIŲ TEISĖS AKTŲ RINKINYS

Vilnius, 2021

Leidinio bibliografinė informacija pateikiama Lietuvos nacionalinės Martyno Mažvydo bibliotekos Nacionalinės bibliografijos duomenų banke (NBDB).

Leidinys *„Jungtinių Tautų ir Europos Sąjungos informacijos apsauga: norminių teisės aktų rinkinys“* skirtas Generolo Jono Žemaičio Lietuvos karo akademijos kariūnams ir klausytojams, studijuojantiems informacijos saugumo studijų dalyką, taip pat Europos Sąjungos ir NATO valstybių narių karo akademijų kadetams ir gynybos universitetų studentams, studijuojantiems informacijos saugumo studijų dalyką anglų kalba. Leidinys turėtų būti naudingas Lietuvos Respublikos krašto apsaugos sistemos ir kitų nacionalinį saugumą užtikrinančių institucijų darbuotojams, dirbantiems su Jungtinių Tautų ir Europos Sąjungos įslaptinta informacija ar besirengiantiems tarnybai Jungtinių Tautų ar Europos Sąjungos institucijose ar misijose.

Leidinys apsvarstytas, patvirtintas ir rekomenduotas spausdinti Generolo Jono Žemaičio Lietuvos karo akademijos Humanitarinių mokslų katedros posėdyje 2020 m. vasario 4 d., protokolo Nr. VL-34.

Sudarytojas – Andrius TEKORIUS, Generolo Jono Žemaičio Lietuvos karo akademija

Atsakingasis redaktorius – dr. Vladas TUMALAVIČIUS, Generolo Jono Žemaičio Lietuvos karo akademija

ISBN 978-609-8277-11-1

GENERAL JONAS ŽEMAITIS MILITARY ACADEMY OF LITHUANIA

THE PROTECTION OF THE UNITED NATIONS AND THE EUROPEAN UNION INFORMATION

LEGISLATIVE INSTRUMENTS REPORT

Vilnius, 2021

Leidinio bibliografinė informacija pateikiama Lietuvos nacionalinės Martyno Mažvydo bibliotekos Nacionalinės bibliografijos duomenų banke (NBDB).

The Protection of the United Nations and the European Union Information: Legislative Instruments Report is aimed at the cadets and course participants studying Information Security Studies at General Jonas Žemaitis Military Academy of Lithuania, cadets of the European Union (EU) and NATO member countries' military academies and students of defence universities studying Information Security. The publication may also be useful to the employees of the Lithuanian National Defence System and other institutions ensuring national security and working with the United Nations (UN) and EU classified information or in the course of preparation for the service in the UN and EU institutions or missions.

The publication was discussed, approved and recommended for printing during the meeting of the Department of Humanities, General Jonas Žemaitis Military Academy of Lithuania. Report of Proceedings No. VL-34 of 4 February 2020.

Compiler – Andrius TEKORIUS, General Jonas Žemaitis Military Academy of Lithuania.

Managing Editor – Dr. Vladas TUMALAVIČIUS, General Jonas Žemaitis Military Academy of Lithuania

ISBN 978-609-8277-11-1

TURINYS / CONTENTS

PRATARMĖ

Informacijos apsauga – viena svarbiausių visų valstybių ir tarptautinių organizacijų saugumo užtikrinimo sričių. Siekdamos užtikrinti įslaptintos informacijos apsaugą nuo neteisėto atskleidimo ar praradimo Jungtinės Tautos (toliau – JT) ir Europos Sąjunga (toliau – ES) priėmė specialius šių organizacijų vidaus teisės aktus ir pasirašė susitarimus su valstybėmis narėmis dėl informacijos apsaugos standartų ir taisyklių.

Lietuvos Respublika ir kitos JT ir ES valstybės narės įsipareigojo užtikrinti tinkamą šių tarptautinių organizacijų įslaptintos informacijos apsaugą, taikyti vienodus informacijos apsaugos principus, standartus ir procedūras.

Leidinyje *„Jungtinių Tautų ir Europos Sąjungos informacijos apsauga: norminių teisės aktų rinkinys“* pateikti pagrindiniai neįslaptinti JT ir ES norminiai teisės aktai, reglamentuojantys šių organizacijų paslaptį sudarančios informacijos įslaptinimo, saugojimo, naudojimo, perdavimo, išslaptinimo ir apsaugos veiksmų koordinavimo, kontrolės pagrindus ir tvarką, taip pat nustatantys atskirų įslaptintos informacijos apsaugos sričių (personalo patikimumo, fizinės apsaugos, įslaptintos informacijos administravimo, įslaptintos informacijos ryšių ir informacinių sistemų apsaugos, įslaptintų sandorių saugumo) reikalavimus.

Rinkinyje pateikti norminiai teisės aktai sudaro JT ir ES informacijos apsaugos sistemos teisinį pagrindą. Rinkinio struktūrą sudaro 4 skyriai: 1) JT teisės aktai; 2) ES teisės aktai; 3) JT ir ES norminiuose teisės aktuose vartojamos santrumpos ir 4) JT ir ES terminų, susijusių su įslaptintos informacijos apsauga, žinynas.

Norminių teisės aktų rinkinys *„Jungtinių Tautų ir Europs Sąjungos informacijos apsauga: norminių teisės aktų rinkinys“* – tai trečiasis Generolo Jono Žemaičio Lietuvos karo akademijos leidinys, skirtas įslaptintos informacijos apsaugai.

Pirmajame dviejų dalių leidinyje *„Valstybės ir tarnybos paslapčių apsauga“*, išleistame 2014 metais, pateikti pagrindiniai Lietuvos Respublikos norminiai teisės aktai, reglamentuojantys įslaptintos informacijos apsaugos sistemą Lietuvoje, antrajame dviejų dalių leidinyje *„NATO informacijos apsauga“*, išleistame 2015 metais, pateikti pagrindiniai NATO norminiai teisės aktai, reglamentuojantys šios organizaci-

jos įslaptintos informacijos apsaugos sistemą.

Šio rinkinio tikslas – supažindinti skaitytoją su JT ir ES informacijos apsaugos organizavimo, koordinavimo ir kontrolės sistema, pagrindiniais įslaptintos informacijos apsaugos principais ir minimaliais standartais, taip pat informacijos apsaugos metodais, priemonėmis ir procedūromis.

Leidinyje JT ir ES teisės aktai pateikti lietuvių ir anglų kalbomis. Jo pabaigoje pateikiamas teisės aktuose vartojamų santrumpų sąrašas ir terminų žinynas. Tai, sudarytojo nuomone, turėtų skatinti geresnį JT ir ES terminijos, susijusios su specifine informacijos apsaugos sritimi, įsisavinimą.

Leidinys *„Jungtinių Tautų ir Europos Sąjungos informacijos apsauga: norminių teisės aktų rinkinys“* skirtas Generolo Jono Žemaičio Lietuvos karo akademijos kariūnams ir klausytojams, studijuojantiems informacijos saugumo studijų dalyką, taip pat ES ir NATO valstybių narių karo akademijų kadetams ir gynybos universitetų studentams, studijuojantiems informacijos saugumo studijų dalyką anglų kalba. Leidinys turėtų būti naudingas Lietuvos Respublikos krašto apsaugos sistemos ir kitų nacionalinį saugumą užtikrinančių institucijų darbuotojams, dirbantiems su JT ir ES įslaptinta informacija ar besirengiantiems tarnybai JT ar ES institucijose ar misijose.

Rinkinyje pateiktų teisės aktų redakcija aktuali nuo 2020 metų liepos 1 dienos.

Rinkinio sudarytojas Andrius TEKORIUS

FOREWORD

Information security is one of the principal domains ensuring security to all states and international organizations. In order to guarantee the protection of classified information from its unauthorized disclosure or loss, the United Nations (UN) and the European Union (EU) adopted special internal legal acts and signed agreements with Member States on the standards and regulations of information security.

The Republic of Lithuania and other UN and EU Member States are committed to ensuring proper security of classified information of the aforementioned international organizations and applying common principles, standards, and procedures of information security.

The publication *The Protection of the United Nations and the European Union Information: Legislative Instruments Report* presents the main unclassified legal documents of the UN and the EU that regulate a legal framework and order of classifying, archiving, utilizing, transferring, declassifying, coordinating and controlling the process of protecting information and constitute the secrecy of the above-mentioned organizations. They also set requirements for separate fields of the EU classified information protection (Personnel Security, Physical Security, Management of Classified Information, Protection of Classified Information Handled in Communication and Information Systems, and Industrial Security) of classified information.

The legal documents stipulated in the report lay legal foundations for a system of protecting information within the UN and the EU. The report is comprised of four chapters: Chapter One deals with the UN legal documents, Chapter Two presents the EU legal documents, Chapter Three includes current abbreviations provided in the UN and EU legislative documents and Chapter Four embraces a glossary of the UN and EU terms related to the protection of classified information.

The Protection of the United Nations and European Union Information: Legislative Instruments Report is the third publication on classified information security issued by General Jonas Žemaitis Military Academy of Lithuania.

The first two-volume publication *Valstybės ir tarnybos paslapčių apsauga* (*The Protection of State and Service Secrets)*, published in 2014, presents the main legal documents of the Republic of Lithuania

regulating classified information security system in Lithuania. The second two-volume publication *The Protection of NATO Information*, published in 2015, encompasses NATO's principal legal documents governing its security system of classified information.

This report aims to familiarize the reader with the system of organizing, coordinating, and controlling the UN and EU information security, essential principles and minimal standards pertaining to classified information security, as well as with the methods, means, and procedures of information security.

In this publication, the UN and EU legal documents are presented in Lithuanian and English. A list of abbreviations used in legal documents and a glossary of terms are given in the appendices. In the opinion of the compiler, both should encourage better awareness of the UN and EU terms related to the specific field of information security.

The Protection of the United Nations and the European Union Information: Legislative Instruments Report is aimed at the cadets and course participants studying Information Security Studies at General Jonas Žemaitis Military Academy of Lithuania, cadets of the EU and NATO member states' military academies and students of defence universities studying Information Security. The publication may also be useful to the employees of the National Defence System and other institutions ensuring national security and working with the UN and EU classified information or in the course of preparation for the service in the UN and EU institutions and missions.

The versions of the UN and EU legal documents presented in the report are valid as of 1 July 2020.

Andrius TEKORIUS
Compiler

1.1. UNITED NATIONS SECRETARIAT. SECRETARY-GENERAL'S BULLETIN. INFORMATION SENSITIVITY, CLASSIFICATION AND HANDLING

SECRETARY-GENERAL'S BULLETIN

12 February 2007

INFORMATION SENSITIVITY, CLASSIFICATION AND HANDLING

ST/SGB/2007/6

The Secretary-General, for the purposes of ensuring the classification and secure handling of confidential information entrusted to or originating from the United Nations, promulgates the following:

Section 1
Classification principles

1.1 The overall approach to classifying information entrusted to or originating from the United Nations is based on the understanding that the work of the United Nations should be open and transparent, except insofar as the nature of information concerned is deemed confidential in accordance with the guidelines set out in the present bulletin.

1.2 Information deemed sensitive shall include the following:

(a) Documents created by the United Nations, received from or sent to third parties, under an expectation of confidentiality;

(b) Documents whose disclosure is likely to endanger the safety or security of any individual, violate his or her rights or invade his or her privacy;

(c) Documents whose disclosure is likely to endanger the security of Member States or prejudice the security or proper conduct of any operation or activity of the United Nations, including any of its peacekeeping operations;

(d) Documents covered by legal privilege or related to internal investigations;

(e) Internal inter-office or intra-office documents, including draft documents, if disclosure would undermine the Organization's free and independent decision-making process;

(f) Documents containing commercial information, if disclosure would harm either the financial interests of the United Nations or those of other parties involved;

(g) Other kinds of information, which because of their content or the circumstances of their creation or communication must be deemed confidential.

1.3 Classifications should be used judiciously and only in cases where disclosure of the information may be detrimental to the proper functioning of the United Nations or the welfare and safety of its staff or third parties or violate the Organization's legal obligations. In such cases, the procedures set out below should be strictly observed to ensure that such information is not compromised either purposely or inadvertently.

Section 2
Classification levels

2.1 Sensitive information may be classified as "confidential" or "strictly confidential".

2.2 The designation "confidential" shall apply to information or material whose unauthorized disclosure could reasonably be expected to cause damage to the work of the United Nations.

2.3 The designation "strictly confidential" shall apply to information or material whose unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to or impede the conduct of the work of the United Nations.

2.4 The designation "unclassified" shall apply to information or material whose unauthorized disclosure could reasonably be expected

not to cause damage to the work of the United Nations.

Section 3
Identification and markings

3.1 The originator of the information concerned, or its recipient if the information is received from an outside source, under the overall supervision and guidance of the head of department or office, shall decide whether the information is sensitive and mark it with the appropriate classification as detailed in section 4 below.

3.2 Where information from an external source contains prior sensitivity markings, it shall retain those markings or shall be assigned a classification that provides a degree of protection greater than or equal to that of the entity that furnished the information.

3.3 The originator of the information concerned, or its recipient if the information is received from an outside source, under the overall supervision and guidance of the head of department or office, shall, whenever practicable, indicate on the document in question when classified information constitutes a small portion of an otherwise unclassified document.

Section 4
Declassification

4.1 The originator of the information concerned, or its recipient if the information is received from an outside source, under the overall supervision and guidance of the head of department or office, shall, where appropriate, establish and mark on the document in question a date or an event which will trigger declassification. Upon reaching the date or event, the information shall be declassified automatically. The date or event shall not exceed the time frame established in paragraph 4.3 of this section.

4.2 If no date or event for declassification was specified, information may be declassified at any time by the originator or its recipient if the information is received from an outside source, by the Secretary-General or by such officials as the Secretary-General so authorizes.

4.3 Review for possible declassification shall take place before records are transferred to the custody of the Archives and Records Management Section, in accordance with Secretary-General's bulletin ST/SGB/2007/5, on record-keeping and the management of United Nations archives. Subject to the provisions of any other applicable administrative rule or any applicable legal undertaking on the part of the Organization, classified records that have been transferred to the Archives and Records Management Section maintaining their original classification, shall be declassified as follows:

(a) Records that are classified as "strictly confidential" shall be reviewed on an item-by-item basis by the Secretary-General, or by such officials as the Secretary-General so authorizes, for possible declassification when 20 years old. Those not declassified at that time shall be further reviewed, every 5 years thereafter, by the Secretary-General or by such officials as the Secretary-General so authorizes, for possible declassification.

(b) Records that are classified as "confidential" shall be declassified automatically by the Archives and Records Management Section when 20 years old.

4.4 When declassifying information received from an outside source, the Organization shall give due regard to expectations of confidentiality of that outside source and, if appropriate, shall seek the prior consent of the outside source.

Section 5

Handling of classified information

5.1 Heads of departments or offices shall ensure that the following minimal standards are maintained in the handling of classified information received by or originating from their department or office:

(a) All classified information must be transported in sealed envelopes or containers, and clearly marked as such;

(b) All outgoing and incoming classified information must be recorded in a special registry that lists the staff members who are authorized to handle such information;

(c) Classified materials may be duplicated only with the authorization of either their originator or the head of the receiving or originating

department or office, and such copies must be entered in the special registry;

(d) All classified information must be filed and stored under lock and key in a secure location within the department or office concerned, accessible only to the authorized staff members;

(e) A hard copy of classified information received in an electronic form must be printed when received, and filed and stored as detailed in subparagraph (d) above. The electronic file must be securely stored in accordance with section 5.4 below;

(f) Electronic transmission of classified information shall be performed only through the use of protected means of communication, in accordance with section 5.4 below.

5.2 With regard to classified information of a recurrent nature (such as situation reports, operational updates and periodic political assessments), departments or offices shall establish standard distribution lists to provide an auditable system for the distribution and control of such information.

5.3 The above minimum standards are without prejudice to the authority of heads of departments or offices to put in place stricter controls over the handling of classified information so long as such controls are consistent with the present bulletin.

5.4 Heads of departments and offices, in cooperation with the Information Technology Services Division of the Department of Management, shall establish procedures to ensure that automated information systems, including networks and telecommunications systems, that collect, create, communicate, compute, disseminate, process or store classified information, have controls that both prevent access by unauthorized persons, and ensure the integrity of the information.

5.5 The destruction by authorized means of non-current, classified documents that have no further administrative, fiscal, legal, historical or other informational value shall be authorized either by the originator or the head of the department or office concerned.

Section 6

Final provisions

6.1 The provisions of the present bulletin shall not apply to the classification and handling of records specifically covered in other Secretary-General's bulletins, other administrative issuances promulgated by the Secretary-General or legal undertakings made by the Organization to third parties.

6.2 Secretary-General's bulletin ST/SGB/272, on security of information, and administrative instruction ST/AI/189/Add.16, on regulations for the control and limitation of documentation: classification and declassification of documents, are hereby abolished.

6.3 The present bulletin shall enter into force on 15 February 2007.

(*Signed*) Ban Ki-moon
Secretary-General

2.1. 2013 M. BALANDŽIO 15 D. EUROPOS PARLAMENTO BIURO SPRENDIMAS DĖL KONFIDENCIALIOS INFORMACIJOS TVARKYMO EUROPOS PARLAMENTE TAISYKLIŲ

EUROPOS PARLAMENTO BIURO SPRENDIMAS

2013 m. balandžio 15 d.

dėl konfidencialios informacijos tvarkymo Europos Parlamente taisyklių

2014/C 96/01

EUROPOS PARLAMENTO BIURAS,

atsižvelgdamas į Europos Parlamento darbo tvarkos taisyklių 23 straipsnio 12 dalį,

kadangi:

(1) atsižvelgiant į 2010 m. spalio 20 d. pasirašytą Pagrindų susitarimą dėl Europos Parlamento ir Europos Komisijos santykių ([1]) (Pagrindų susitarimas) ir į 2014 m. kovo 12 d. pasirašytą Europos Parlamento ir Tarybos tarpinstitucinį susitarimą dėl Tarybos turimos įslaptintos informacijos klausimais, nesusijusiais su bendra užsienio ir saugumo politika, perdavimo Europos Parlamentui ir tvarkymo Europos Parlamente ([2]) (Tarpinstitucinis susitarimas), būtina nustatyti konkrečias konfidencialios informacijos tvarkymo Europos Parlamente taisykles;

(2) pagal Lisabonos sutartį Europos Parlamentui pavedamos naujos užduotys ir siekiant plėtoti Parlamento veiklą tose srityse, kuriose reikalingas tam tikras konfidencialumas, būtina nustatyti konfidencialios informacijos, įskaitant įslaptintą informaciją, tvarkymo Europos Parlamente pagrindinius principus, būtiniausius saugumo standartus ir tinkamas procedūras;

(3) šiame sprendime nustatytų taisyklių tikslas – užtikrinti atitinkamus apsaugos standartus ir suderinamumą su kitų institucijų, įstaigų, tarnybų ir agentūrų, įsteigtų pagal Sutartis arba remiantis jomis, arba valstybių narių priimtomis taisyklėmis, siekiant užtikrinti sklandų Europos Sąjungos sprendimų priėmimo procesą;
(4) šio sprendimo nuostatos nedaro poveikio esamoms ir būsimoms taisyklėms (dėl galimybės susipažinti su dokumentais), priimtoms pagal Sutarties dėl Europos Sąjungos veikimo (SESV) 15 straipsnį;
(5) šio sprendimo nuostatos nedaro poveikio esamoms ir būsimoms taisyklėms dėl asmens duomenų apsaugos, priimtoms pagal SESV 16 straipsnį,

PRIĖMĖ ŠĮ SPRENDIMĄ:

1 straipsnis

Tikslas

Šiame sprendime reglamentuojamas Europos Parlamento vykdomas konfidencialios informacijos valdymas ir tvarkymas, įskaitant tokios informacijos rengimą, gavimą, perdavimą ir laikymą siekiant tinkamai apsaugoti jos konfidencialų pobūdį. Šiuo sprendimu įgyvendinamas Tarpinstitucinis susitarimas ir Pagrindų susitarimas, visų pirma, jo II priedas.

2 straipsnis

Apibrėžtys

Šiame sprendime:
a) **informacija** – rašytinė ar žodinė informacija, kokia bebūtų jos laikmena ar autorius;
b) **konfidenciali informacija** – įslaptinta informacija ir neįslaptinta kita konfidenciali informacija;
c) **įslaptinta informacija** – ES įslaptinta informacija ir lygiavertė įslaptinta informacija;

d) **ES įslaptinta informacija (ESĮI)** – bet kokia informacija ir medžiaga, pažymėta slaptumo žymomis TRÈS SECRET UE/EU TOP SECRET, SECRET UE/EU SECRET, CONFIDENTIEL UE/EU CONFIDENTIAL arba RESTREINT UE/EU RESTRICTED, kurią atskleidus be leidimo gali būti padaryta įvairaus laipsnio žalos Europos Sąjungos interesams arba vienos ar daugiau valstybių narių interesams, neatsižvelgiant į tai, ar ta informacija buvo parengta institucijose, įstaigose, tarnybose ar agentūrose, įsteigtose pagal Sutartis arba jomis remiantis, ar yra gauta iš valstybių narių, trečiųjų šalių ar tarptautinių organizacijų. Šiuo atveju informacija ir medžiaga žymima slaptumo žymos laipsniu:

– **TRÈS SECRET UE/EU TOP SECRET** – tai informacija ir medžiaga, kurią atskleidus be leidimo gali būti padaryta ypatingai didelė žala esminiams Europos Sąjungos arba vienos ar daugiau valstybių narių interesams;

– **SECRET UE/EU SECRET** – tai informacija ir medžiaga, kurią atskleidus be leidimo gali būti rimtai pakenkta esminiams Europos Sąjungos arba vienos ar daugiau valstybių narių interesams;

– **CONFIDENTIEL UE/EU CONFIDENTIAL** – tai informacija ir medžiaga, kurią atskleidus be leidimo gali būti pakenkta esminiams Europos Sąjungos arba vienos ar daugiau valstybių narių interesams;

– **RESTREINT UE/EU RESTRICTED** – tai informacija ir medžiaga, kurių atskleidimas be leidimo gali būti nenaudingas Europos Sąjungos arba vienos ar daugiau valstybių narių interesams;

e) **lygiavertė įslaptinta informacija** – įslaptinta informacija, kurią parengė valstybės narės, trečiosios valstybės arba tarptautinės organizacijos, kuri pažymėta slaptumo žyma, lygiaverte vienai iš slaptumo žymų, naudojamų ESĮI, ir kurią Europos Parlamentui perdavė Taryba arba Komisija;

f) **kita konfidenciali informacija** – bet kokia kita neįslaptinta konfidenciali informacija, įskaitant informaciją, kuriai taikomos duomenų apsaugos taisyklės arba kuriai taikoma tarnybinės paslapties prievolė, ir kuri parengta Europos Parlamente ar Europos Parlamentui perduota kitų institucijų, įstaigų, tarnybų ir agentūrų, įsteigtų pagal Sutartis arba jomis remiantis, ar valstybių narių;

g) **dokumentas** – bet kokia fiksuota informacija, neatsižvelgiant į jos fizinę formą ar charakteristikas;

h) **medžiaga** – dokumentas arba bet kokie pagaminti ar gaminami įrenginiai ar įranga;

i) **principas „būtina žinoti“** – asmens būtinybė susipažinti su konfidencialia informacija, kad jis galėtų atlikti oficialias pareigas ar užduotį;
j) **leidimas** – sprendimas suteikti asmeninę prieigą prie konkretaus laipsnio įslaptintos informacijos, kurį priima Parlamento pirmininkas, jei sprendimas susijęs su Europos Parlamento nariais, arba generalinis sekretorius, jei sprendimas susijęs su Europos Parlamento pareigūnais ir kitais Europos Parlamento darbuotojais, kurie dirba frakcijose, remdamasis teigiamais nacionalinės institucijos pagal nacionalinę teisę ir pagal I priedo 2 dalies nuostatas atlikto asmens patikimumo patikrinimo rezultatais;
k) **laipsnio sumažinimas** – įslaptinimo laipsnio sumažinimas;
l) **išslaptinimas** – bet kokios slaptumo žymos panaikinimas;
m) **kita žyma** – kitai konfidencialiai informacijai suteikiama žyma, pagal kurią atpažįstami iš anksto nustatyti konkretūs dokumento naudojimo nurodymai arba jame aptariama sritis. Šia žyma taip pat gali būti pažymėta įslaptinta informacija siekiant nustatyti papildomus jos naudojimo reikalavimus;
n) **kitos žymos panaikinimas** – bet kokios kitos žymos panaikinimas;
o) **rengėjas** – konfidencialios informacijos tinkamai įgaliotas autorius;
p) **saugumo pranešimai** – techninės įgyvendinimo priemonės, nustatytos II priede;
q) **naudojimo nurodymai** – techniniai nurodymai Europos Parlamento tarnyboms dėl konfidencialios informacijos valdymo.

3 straipsnis

Pagrindiniai principai ir būtiniausi standartai

1. Tvarkydamas konfidencialią informaciją Europos Parlamentas laikosi I priedo 1 dalyje nustatytų pagrindinių principų ir būtiniausių standartų.

2. Europos Parlamentas pagal pagrindinius principus ir būtiniausius standartus parengia Informacijos saugumo valdymo sistemą (ISVS). ISVS sudaro saugumo pranešimai, naudojimo nurodymai ir atitinkami Darbo tvarkos taisyklių straipsniai. Jos tikslas – palengvinti parlamentinę ir administracinę veiklą bei užtikrinti visos Parlamento tvarkomos konfidencialios informacijos apsaugą visapusiškai laikantis tokios informacijos rengėjo nustatytų taisyklių, pateikiamų saugumo pranešimuose.

Konfidencialios informacijos tvarkymas naudojant Europos Parlamento automatines ryšių ir informacijos sistemas (RIS) įgyvendinamas laikantis informacijos saugumo užtikrinimo (ISU) koncepcijos, kaip numatyta saugumo III pranešime.

3. Europos Parlamento nariai, neturėdami asmens patikimumo patvirtinimo, gali susipažinti su įslaptinta informacija iki slaptumo žymos RESTREINT UE/EU RESTRICTED laipsniu įskaitytinai.

4. Kai susijusi informacija pažymėta slaptumo CONFIDENTIEL UE/EU CONFIDENTIAL žyma arba jai lygiaverte, su ja leidžiama susipažinti tiems Europos Parlamento nariams, kuriems Parlamento pirmininkas suteikė leidimą pagal 5 dalį arba kurie pasirašė oficialų pareiškimą, kad neatskleis tos informacijos turinio tretiesiems asmenims, kad laikysis įsipareigojimo saugoti slaptumo CONFIDENTIEL UE/EU CONFIDENTIAL žyma pažymėtą informaciją ir kad yra susipažinę su šio įsipareigojimo nesilaikymo pasekmėmis.

5. Kai susijusi informacija pažymėta slaptumo SECRET UE/EU SECRET, TRÈS SECRET UE/EU TOP SECRET žyma arba jai lygiaverte, su ja leidžiama susipažinti tiems Europos Parlamento nariams, kurie gavo Pirmininko leidimą po to, kai:

a) jų patikimumas buvo patikrintas pagal šio sprendimo I priedo 2 dalį arba
b) kompetentinga nacionalinė institucija pranešė, kad atitinkamiems nariams buvo išduotas tinkamas leidimas atsižvelgiant į jų atliekamas funkcijas pagal nacionalinius įstatymus ir kitus teisės aktus.

6. Prieš Europos Parlamento nariams suteikiant teisę susipažinti su įslaptinta informacija, jie informuojami apie pareigą saugoti tokią informaciją ir pripažįsta tokią pareigą pagal I priedą. Jie taip pat informuojami apie tokios apsaugos užtikrinimo priemones.

7. Europos Parlamento pareigūnai ir kiti Parlamento darbuotojai, dirbantys frakcijose, gali susipažinti su konfidencialia informacija, jeigu jie laikosi principo „būtina žinoti“, ir su įslaptinta aukštesnio laipsnio, pvz., slaptumo žyma RESTREINT UE/EU RESTRICTED pažymėta informacija, jeigu jie turi atitinkamo lygmens asmens patikimumo patvirtinimą. Jiems leidžiama susipažinti su įslaptinta informacija, jei jie buvo informuoti apie pareigą saugoti tokią informaciją ir apie tokios apsaugos užtikrinimo priemones bei gavo raštiškus nurodymus šiuo klausimu ir pasirašė pareiškimą, kuriuo patvirtino tokių nurodymų gavimą ir įsipareigojo jų laikytis pagal esamas taisykles.

4 straipsnis

Konfidencialios informacijos rengimas ir administracinis tvarkymas Europos Parlamente

1. Europos Parlamento pirmininkas, susijusio Parlamento komiteto pirmininkai ir generalinis sekretorius ir (arba) asmuo, kuriam jis tinkamai suteikė leidimą raštu, gali parengti konfidencialią informaciją ir (arba) įslaptinti informaciją, kaip numatyta saugumo pranešimuose.

2. Rengdamas įslaptintą informaciją, rengėjas taiko atitinkamą slaptumo žymos laipsnį pagal tarptautinius standartus ir I priede nustatytas apibrėžtis. Rengėjas taip pat paprastai nustato gavėjus, kuriems turi būti suteiktas leidimas susipažinti su informacija, atitinkančia slaptumo žymos laipsnį. Ši informacija suteikiama Įslaptintos informacijos skyriui (ĮIS), kai jam pateikiamas dokumentas.

3. Kita konfidenciali informacija, kuriai taikoma tarnybinės paslapties saugojimo prievolė, tvarkoma laikantis I ir II priedų ir naudojimo nurodymų.

5 straipsnis

Konfidencialios informacijos gavimas Europos Parlamente

1. Apie Europos Parlamento gautą konfidencialią informaciją pranešama:

a) prašymą pateikusio Parlamento organo ar atitinkamas pareigas einančio asmens sekretoriatui arba tiesiogiai ĮIS – apie informaciją, pažymėtą slaptumo žyma RESTREINT UE/EU RESTRICTED arba jai lygiaverte, ir apie kitą konfidencialią informaciją;

b) ĮIS – apie informaciją, pažymėtą slaptumo žymų CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ar TRÈS SECRET UE/EU TOP SECRET laipsniais arba jiems lygiaverčiais.

2. Konfidencialios informacijos registravimu, laikymu ir atsekamumu, atsižvelgiant į konkretų atvejį, užsiima informaciją gavęs Parlamento organo sekretoriatas ar atitinkamas pareigas einantis asmuo arba ĮIS.

3. Komisijai pagal Pagrindų susitarimo II priedo 3.2 punktą perduodamos konfidencialios informacijos atveju arba Tarybai pagal Tarpinstitucinio susitarimo 5 straipsnio 4 dalį perduodamos įslaptintos

informacijos atveju suderintos nuostatos, kurios turi būti nustatytos bendru sutarimu ir kuriomis siekiama išsaugoti informacijos konfidencialumą, pateikiamos atitinkamai Parlamento organo ar atitinkamas pareigas einančio asmens sekretoriatui arba ĮIS.

4. 3 dalyje minimos nuostatos taip pat gali būti taikomos mutatis mutandis, kai konfidencialią informaciją perduoda kitos institucijos, įstaigos, tarnybos ir agentūros, įsteigtos pagal Sutartis ar jomis remiantis, arba valstybės narės.

5. Siekdama užtikrinti apsaugos lygį, atitinkantį slaptumo žymą TRÈS SECRET UE/EU TOP SECRET arba jai lygiavertę, Pirmininkų sueiga įsteigia priežiūros komitetą. Informacija, pažymėta slaptumo žyma TRÈS SECRET UE/EU TOP SECRET arba jai lygiaverte, perduodama Europos Parlamentui pagal papildomas nuostatas, dėl kurių susitaria Europos Parlamentas ir informaciją teikianti Europos Sąjungos institucija.

6 straipsnis

Europos Parlamento vykdomas įslaptintos informacijos perdavimas trečiosioms šalims

Europos Parlamentas, gavęs išankstinį raštišką įslaptintos informacijos rengėjo arba Europos Parlamentui ją perdavusios Europos Sąjungos institucijos sutikimą, gali persiųsti tokią įslaptintą informaciją trečiosioms šalims, jeigu jos užtikrina, kad tokia informacija jų tarnybose ir pastatuose tvarkoma laikantis šiame sprendime nurodytoms taisyklėms lygiaverčių taisyklių.

7 straipsnis

Saugios patalpos

1. Konfidencialios informacijos tvarkymo Europos Parlamente tikslais Europos Parlamentas įrengia saugią zoną ir saugias skaityklas.

2. Saugioje zonoje numatomos patalpos įslaptintai informacijai registruoti, skaityti, archyvuoti, perduoti ir tvarkyti. Jose turi būti įrengta, inter alia, skaitykla ir posėdžių salė, kuriose būtų galima susipažinti su įslaptinta informacija ir kurias prižiūrėtų ĮIS.

3. Už saugios zonos ribų gali būti įrengtos saugios skaityklos, kuriose būtų galima susipažinti su ne aukštesne kaip slaptumo žyma RESTREINT UE/EU RESTRICTED arba jai lygiaverte pažymėta informacija ir kita konfidencialia informacija. Už tas saugias skaityklas atsakingos Parlamento organo ar atitinkamas pareigas užimančio asmens sekretoriato kompetentingos tarnybos arba ĮIS. Jose užtikrinamas saugus laikymas ir nėra kopijavimo aparatų, telefonų, faksų, skaitytuvų ar kitų dokumentų dauginimo ar perdavimo priemonių.

8 straipsnis

Konfidencialios informacijos registravimas, tvarkymas ir saugojimas

1. Informaciją, pažymėtą slaptumo žyma RESTREINT UE/EU RESTRICTED arba jam lygiaverte, ir kitą konfidencialią informaciją gali registruoti ir saugoti Parlamento organo ar atitinkamas pareigas einančio asmens sekretoriato kompetentingos tarnybos arba ĮIS, priklausomai nuo to, kas gavo informaciją.

2. Taikomos šios slaptumo žyma RESTREINT UE/EU RESTRICTED arba jai lygiaverte pažymėtos informacijos ir kitos konfidencialios informacijos tvarkymo sąlygos:

a) dokumentai asmeniškai perduodami sekretoriato vadovui, jis šiuos dokumentus įregistruoja ir išduoda gavimo patvirtinimą;
b) faktiškai nenaudojami dokumentai laikomi užrakintoje vietoje ir už juos atsako sekretoriatas;
c) jokiu atveju informacija negali būti išsaugota kitoje laikmenoje arba perduota kitam asmeniui. Tokius dokumentus galima dauginti tik tinkamai akredituota įranga, kaip apibrėžta saugumo pranešimuose;
d) prieiga prie tokios informacijos suteikiama tik rengėjo arba Europos Sąjungos institucijos, kuri perdavė informaciją Europos Parlamentui, nurodytiems asmenims pagal 4 straipsnio 2 dalyje arba 5 straipsnio 3, 4 ir 5 dalyse numatytą tvarką;
e) Parlamento organo ar atitinkamas pareigas užimančio asmens sekretoriatas pildo asmenų, kurie susipažino su informacija, ir datų bei laiko, kai su jais susipažinta, registrą ir perduoda šį registrą ĮIS tuo metu, kai ĮIS pateikiama informacija.

3. Informaciją, pažymėtą slaptumo žymų laipsniais CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ar TRÈS SECRET

UE/EU TOP SECRET arba jiems lygiaverčiais, saugioje zonoje registruoja ir saugo ĮIS pagal atitinkamą slaptumo žymos laipsnį ir kaip apibrėžta saugumo pranešimuose.

4. Jei pažeidžiamos 1–3 dalyse nustatytos taisyklės, Parlamento organo ar atitinkamas pareigas užimančio asmens sekretoriato, arba ĮIS atsakingas pareigūnas apie tai praneša generaliniam sekretoriui ir šis perduoda šį klausimą Pirmininkui, jei su tuo susijęs Europos Parlamento narys.

9 straipsnis

Teisė patekti į saugias patalpas

1. Į saugią zoną gali patekti tik šie asmenys:

a) asmenys, kurie pagal 3 straipsnio 4–7 dalis turi leidimą susipažinti su joje laikoma informacija ir kurie pateikė prašymą pagal 10 straipsnio 1 dalį;
b) asmenys, kurie pagal 4 straipsnio 1 dalį turi leidimą rengti įslaptintą informaciją ir kurie pateikė prašymą pagal 10 straipsnio 1 dalį;
c) Europos Parlamento pareigūnai, dirbantys ĮIS;
d) už ĮIS valdymą atsakingi Europos Parlamento pareigūnai;
e) kai būtina, už saugumą ir priešgaisrinę saugą atsakingi Europos Parlamento pareigūnai;
f) valytojai – bet tik esant ir atidžiai prižiūrint ĮIS pareigūnui.

2. ĮIS gali atsisakyti į saugią zoną įleisti asmenis, neturinčius leidimo. Prašymą patekti į patalpas pateikę Europos Parlamento nariai, norėdami užginčyti atsisakymą įleisti, kreipiasi į Pirmininką, kiti asmenys – į generalinį sekretorių.

3. Generalinis sekretorius gali leisti surengti nedidelio skaičiaus asmenų posėdį posėdžių salėje, esančioje saugioje zonoje.

4. Į saugią skaityklą gali patekti tik šie asmenys:

a) Europos Parlamento nariai, Europos Parlamento pareigūnai ir kiti Europos Parlamento darbuotojai, dirbantys frakcijose, kurių tapatybė tinkamai nustatyta susipažinimo su konfidencialia informacija arba jos rengimo tikslais;
b) Europos Parlamento pareigūnai, atsakingi už ĮIS valdymą, informaciją gavusio Parlamento organo ar atitinkamas pareigas einančio asmens sekretoriato pareigūnai ir ĮIS pareigūnai;
c) kai reikia, už saugumą ir priešgaisrinę saugą atsakingi Europos Parlamento pareigūnai;

d) valytojai – bet tik esant ir atidžiai prižiūrint atitinkamai Parlamento organo ar atitinkamas pareigas einančio asmens sekretoriato arba ĮIS pareigūnui.

5. Atsakingas Parlamento organo ar atitinkamas pareigas einančio asmens sekretoriatas arba ĮIS, priklausomai nuo atvejo, gali atsisakyti į saugią skaityklą įleisti asmenis, neturinčius leidimo. Prašymą patekti į patalpas pateikę Europos Parlamento nariai, norėdami užginčyti atsisakymą įleisti, kreipiasi į Pirmininką, kiti asmenys – į generalinį sekretorių.

10 straipsnis

Susipažinimas su konfidencialia informacija ir jos rengimas saugiose patalpose

1. Asmuo, norintis susipažinti su konfidencialia informacija arba ją rengti saugioje zonoje, iš anksto praneša savo vardą ir pavardę ĮIS. ĮIS patikrina to pateikusio asmens tapatybę ir patikrina, ar tam asmeniui pagal 3 straipsnio 3–7 dalis, 4 straipsnio 1 dalį arba 5 straipsnio 3, 4 ir 5 dalis leidžiama susipažinti su konfidencialia informacija arba ją rengti.

2. Asmuo, norintis pagal 3 straipsnio 3 ir 7 dalis susipažinti su konfidencialia informacija, pažymėta slaptumo žyma RESTREINT UE/EU RESTRICTED laipsniu arba jai lygiaverte, ir su kita konfidencialia informacija saugiose skaityklose, iš anksto praneša savo vardą ir pavardę Parlamento organo ar atitinkamas pareigas einančio asmens sekretoriato kompetentingoms tarnyboms arba ĮIS.

3. Išskyrus ypatingus atvejus (pvz., per trumpą laikotarpį gaunama daug prašymų leisti susipažinti su konfidencialia informacija), su konfidencialia informacija susipažinti saugioje patalpoje vienu metu leidžiama tik vienam asmeniui, esant Parlamento organo ar atitinkamas pareigas einančio asmens sekretoriato arba ĮIS pareigūnui.

4. Susipažįstant su dokumentais draudžiama bendrauti su išorine aplinka (įskaitant draudimą naudotis telefonu ar kitomis technologijų priemonėmis), užsirašinėti ir dauginti ar fotografuoti konfidencialią informaciją, su kuria susipažįstama.

5. Prieš leisdamas asmeniui išeiti iš saugios patalpos, Parlamento organo ar atitinkamas pareigas einančio asmens sekretoriato arba ĮIS pareigūnas patikrina, ar konfidenciali informacija, su kuria asmuo susipažino, vis dar yra vietoje, nesugadinta ir tebėra išsami.

6. Jei pažeidžiamos pirmiau nustatytos taisyklės, Parlamento organo ar atitinkamas pareigas einančio asmens sekretoriato arba ĮIS pareigūnas apie tai praneša generaliniam sekretoriui ir šis informuoja Pirmininką, jei pažeidimas susijęs su Europos Parlamento nariu.

11 straipsnis

Susipažinimo su konfidencialia informacija uždarame posėdyje, vykstančiame *nesaugiose* patalpose, būtiniausi standartai

1. Parlamento komitetų arba kitų Europos Parlamento politinių ar administracinių organų nariai gali susipažinti su informacija, pažymėta slaptumo žymos RESTREINT UE/EU RESTRICTED laipsniu arba jam lygiaverčiu, ir kita konfidencialia informacija uždarame posėdyje nesaugiose patalpose.

2. 1 dalyje nurodytomis aplinkybėmis už posėdį atsakingas Parlamento organo ar atitinkamas pareigas einančio asmens sekretoriatas užtikrina, kad būtų laikomasi šių sąlygų:

a) į posėdžio salę įleidžiami tik kompetentingo komiteto ar organo pirmininko nurodyti asmenys, kurie turi dalyvauti posėdyje;
b) visi dokumentai sunumeruojami, išdalijami posėdžio pradžioje ir surenkami posėdžio pabaigoje, nedaromi šių dokumentų nuorašai ir šie dokumentai nedauginami ir nefotografuojami;
c) posėdžio protokole nenurodomas aptariamos informacijos turinys. Gali būti užrašomas tik atitinkamas sprendimas, jei jis priimamas;
d) konfidencialiai informacijai, kuri pateikiama žodžiu Europos Parlamento gavėjams, taikomas toks pat konfidencialios informacijos apsaugos lygis, koks taikomas raštu pateikiamai informacijai;
e) posėdžių salėje nelaikomi jokie papildomi dokumentai;
f) dalyviams ir vertėjams žodžiu posėdžio pradžioje išdalijama tik tiek dokumentų kopijų, kiek būtina;
g) posėdžio pradžioje posėdžio pirmininkas aiškiai informuoja apie dokumentų įslaptinimo (kitos žymos) laipsnį;
h) dalyviai negali išsinešti dokumentų iš posėdžių salės;
i) Parlamento organo ar atitinkamas pareigas einančio asmens sekretoriatas posėdžio pabaigoje surenka visas dokumentų kopijas ir už jas atsiskaito;
j) į posėdžių salę, kurioje susipažįstama su konfidencialia informacija arba kurioje ji aptariama, negalima įsinešti jokių elektroninės komunikacijos priemonių ar kitų elektroninių įtaisų.

3. Kai, laikantis Pagrindų susitarimo II priedo 3.2.2 papunktyje ir Tarpinstitucinio susitarimo 6 straipsnio 5 dalyje nurodytų išimčių, informacija, pažymėta slaptumo žymos CONFIDENTIEL UE/EU CONFIDENTIAL laipsniu arba jam lygiaverčiu, aptariama uždarame posėdyje. Už posėdį atsakingas Parlamento organo ar atitinkamas pareigas einančio asmens sekretoriatas užtikrina ne tik 2 dalyje numatytas nuostatas, bet ir tai, kad posėdyje turintys dalyvauti nurodyti asmenys atitiktų 3 straipsnio 4 ir 7 dalyje išdėstytus reikalavimus.

4. 3 dalyje numatytu atveju ĮIS už uždarą posėdį atsakingam Parlamento organo ar atitinkamas pareigas einančio asmens sekretoriatui pateikia reikiamą dokumentų, kurie bus aptariami, kopijų skaičių. Po posėdžio jos grąžinamos ĮIS.

12 straipsnis

Konfidencialios informacijos saugojimas archyve

1. Saugioje zonoje teikiamos saugaus archyvo paslaugos. ĮIS yra atsakinga už saugaus archyvo tvarkymą laikantis standartinių archyvavimo kriterijų.

2. Įslaptinta informacija, galutinai pateikta ĮIS ir informacija, pažymėta slaptumo žymos RESTREINT UE/EU RESTRICTED laipsniu arba jam lygiaverčiu, pateikta Parlamento organo atitinkamas pareigas einančio asmens sekretoriatui, perkeliama į saugioje zonoje esantį saugų archyvą praėjus šešiems mėnesiams po to, kai su ja buvo paskutinį kartą susipažinta, ir vėliausiai per metus nuo tos dienos, kai ji buvo pateikta. Už kitos konfidencialios informacijos, jei ji nebuvo pateikta ĮIS, archyvavimą yra atsakingas atitinkamo Parlamento organo ar atitinkamas pareigas einančio asmens sekretoriatas pagal bendrąsias dokumentų tvarkymo taisykles.

3. Su saugiame archyve saugoma konfidencialia informacija gali būti susipažįstama laikantis šių sąlygų:

a) į archyvą susipažinti su konfidencialia informacija įleidžiami tik tie asmenys, kurių vardas, pavardė, funkcijos arba pareigos nurodyti lydraštyje, pildomame perduodant saugoti tą informaciją;
b) prašymas susipažinti su konfidencialia informacija turi būti teikiamas ĮIS, o ši perkelia reikiamą dokumentą iš archyvo į saugią skaityklą;
c) taikoma 10 straipsnyje nustatyta susipažinimo su konfidencialia informacija tvarka ir sąlygos.

13 straipsnis

Konfidencialios informacijos žymos laipsnio sumažinimas, išslaptinimas ir kitos žymos panaikinimas

1. Konfidencialios informacijos slaptumo žymos laipsnis gali būti sumažintas, ji gali būti visiškai išslaptinta ar jos kita žyma gali būti panaikinta tik gavus rengėjo išankstinį sutikimą ir, jei reikia, pasitarus su kitomis suinteresuotomis šalimis.

2. Dokumentų slaptumo žymos laipsnio sumažinimas arba jų išslaptinimas patvirtinamas raštu. Rengėjas atsako už to dokumento gavėjų informavimą apie slaptumo žymos pakeitimą, o šie atitinkamai atsako už kitų gavėjų, kuriems yra nusiuntę dokumentą arba jo kopiją, informavimą apie slaptumo žymos pakeitimą. Jei įmanoma, ant įslaptintų dokumentų jų rengėjai nurodo datą, laikotarpį arba įvykį, nuo kurio turinio slaptumo žymos laipsnis gali būti sumažintas arba dokumentas išslaptintas. Priešingu atveju rengėjai peržiūri dokumentus ne rečiau kaip kas penkerius metus, kad garantuotų, jog reikalingas pirminis įslaptinimas.

3. Saugiame archyve saugoma konfidenciali informacija atitinkamu laiku, bet ne vėliau kaip 25-aisiais metais nuo jos parengimo, patikrinama, siekiant nuspręsti, ar ji turėtų būti išslaptinta, ar turėtų būti sumažintas jos slaptumo žymos laipsnis, ar kita žyma turėtų būti panaikinta. Tokia informacija tikrinama ir skelbiama laikantis 1983 m. vasario 1 d. Tarybos reglamento (EEB, Euratomas) Nr. 354/83 dėl Europos ekonominės bendrijos ir Europos atominės energijos bendrijos istorinių archyvų atvėrimo visuomenei ([3]) nuostatų. Išslaptinimą atliks įslaptintos informacijos rengėjas arba tuo metu atsakinga tarnyba pagal I priedo 1 dalies 10 skirsnį.

4. Atlikus išslaptinimą, anksčiau saugiame archyve laikyta įslaptinta informacija perkeliama į Europos Parlamento istorinį archyvą, kuriame ji nuolat saugoma ir toliau tvarkoma pagal taikytinas nuostatas.

5. Panaikinus žymą, anksčiau kita konfidencialia informacija laikytai informacijai taikomos Europos Parlamento dokumentų tvarkymo taisyklės.

14 straipsnis

Konfidencialios informacijos saugumo pažeidimai, praradimas arba neteisėtas atskleidimas

1. Pažeidus konfidencialumą apskritai ir, visų pirma, pažeidus šio sprendimo nuostatas Europos Parlamento narių atžvilgiu taikomos atitinkamos Europos Parlamento darbo tvarkos taisyklių nuostatos dėl sankcijų.

2. Jei pažeidimą padaro Europos Parlamento darbuotojas, taikomos atitinkamai Pareigūnų tarnybos nuostatuose ir kitų Europos Sąjungos tarnautojų įdarbinimo sąlygose, nustatytose Reglamente (EEB, Euratomas, EAPB) Nr. 259/68 ([4]) („Tarnybos nuostatai“), numatytos procedūros ir sankcijos.

3. Parlamento Pirmininkas ir (arba) generalinis sekretorius organizuoja visus būtinus pažeidimo tyrimus, kaip apibrėžta VI saugumo pranešime.

4. Jei konfidencialią informaciją Europos Parlamentui perdavė kita Europos Sąjungos institucija arba valstybė narė, Pirmininkas ir (arba) generalinis sekretorius atitinkamai Europos Sąjungos institucijai arba valstybei narei praneša apie įrodytą ar įtariamą įslaptintos informacijos praradimą arba neteisėtą atskleidimą, tyrimo rezultatus bei priemones, kurių imtasi siekiant, kad tai nepasikartotų.

15 straipsnis

Šio sprendimo ir jo įgyvendinimo taisyklių keitimas ir metinė šio sprendimo įgyvendinimo ataskaita

1. Generalinis sekretorius siūlo visus šio sprendimo ir jo įgyvendinimo priedų pakeitimus ir teikia šiuos pasiūlymus Biurui, kad šis priimtų sprendimą.

2. Generalinis sekretorius yra atsakingas už tai, kaip Europos Parlamento tarnybos įgyvendina šį sprendimą, ir pagal šiame sprendime išdėstytus principus parengia naudojimo nurodymus dėl klausimų, kurie numatyti ISVS.

3. Generalinis sekretorius pateikia Biurui metinę šio sprendimo įgyvendinimo ataskaitą.

16 straipsnis

Pereinamojo laikotarpio ir baigiamosios nuostatos

1. ĮIS ar bet kuriame kitame Europos Parlamento archyve laikoma neįslaptinta informacija, kuri laikoma konfidencialia ir kuri pateikta prieš 2014 m. balandžio 1 d., šiame sprendime laikoma kita konfidencialia informacija. Jos rengėjas gali bet kuriuo metu pakeisti konfidencialumo laipsnį.

2. Nukrypstant nuo šio sprendimo 5 straipsnio 1 dalies a punkto ir 8 straipsnio 1 dalies, Tarybos pagal Tarpinstitucinį susitarimą pateikta informacija, pažymėta slaptumo žymos RESTREINT UE/EU RESTRICTED laipsniu ar jam lygiaverčiu, dvylika mėnesių nuo 2014 m. balandžio 1 d. pateikiama, registruojama ir laikoma ĮIS. Su tokia informacija galima susipažinti pagal Tarpinstitucinio susitarimo 4 straipsnio 2 dalies a ir c punktus ir 5 straipsnio 4 dalį.

3. 2011 m. birželio 6 d. Biuro sprendimas dėl konfidencialios informacijos tvarkymo Europos Parlamente taisyklių panaikinamas.

17 straipsnis

Įsigaliojimas

Šis sprendimas įsigalioja jo paskelbimo *Europos Sąjungos oficialiajame leidinyje* dieną.

([1]) OL L 304, 2010 11 20, p. 47.

([2]) OL C 95, 2014 4 1, p. 1.

([3]) OL L 43, 1983 2 15, p. 1.

([4]) OL L 56, 1968 3 4, p. 1.

I PRIEDAS

1 dalis.

KONFIDENCIALIOS INFORMACIJOS APSAUGOS PAGRINDINIAI SAUGUMO PRINCIPAI IR BŪTINIAUSI STANDARTAI

1. ĮVADAS

Šiose nuostatose nustatomi pagrindiniai konfidencialios informacijos apsaugos principai ir būtiniausi standartai, kurių turi laikytis Europos Parlamentas visose savo darbo vietose, taip pat visi įslaptintos informacijos ir kitos konfidencialios informacijos gavėjai, kad būtų užtikrinamas saugumas ir visiems susijusiems asmenims būtų galima garantuoti, jog taikomi bendri apsaugos standartai. Šiuos principus ir standartus papildo saugumo pranešimai, esantys II priede, ir kitos Parlamento komitetų ir kitų Parlamento organų ar atitinkamas pareigas einančių asmenų elgesio su konfidencialia informacija taisyklės.

2. PAGRINDINIAI PRINCIPAI

Europos Parlamento saugumo politika yra sudėtinė jo bendros vidaus valdymo politikos dalis ir todėl yra grindžiama tai bendrai politikai taikomais principais. Tie principai yra teisėtumas, skaidrumas, atskaitomybė ir subsidiarumas bei proporcingumas.

Teisėtumo principas atspindi būtinybę griežtai laikytis teisinės sistemos vykdant saugumo funkcijas ir būtinybę laikytis taikytinų teisinių reikalavimų. Tai taip pat reiškia, kad atsakomybė saugumo srityje privalo būti pagrįsta tinkamomis teisinėmis nuostatomis. Visa apimtimi taikomos Tarnybos nuostatų taisyklės, ypač jų 17 straipsnis dėl darbuotojų įpareigojimo neteisėtai neatskleisti informacijos, gautos einant pareigas, ir jų VI dalis dėl drausminių priemonių. Be to, saugumo pažeidimai neperžengiant Europos Parlamento atsakomybės ribų nagrinėjami vadovaujantis Europos Parlamento darbo tvarkos taisyklėmis ir jo drausminių priemonių politika.

Skaidrumo principas atspindi būtinybę užtikrinti visų saugumo taisyklių ir nuostatų aiškumą, įvairių tarnybų ir sričių pusiausvyrą (fizinis saugumas palyginti su informacijos apsauga ir pan.), taip pat nuoseklią bei konstruktyvią informavimo saugumo klausimais politiką. Be to, dėl skaidrumo taip pat reikalingos aiškios rašytinės saugumo priemonių įgyvendinimo gairės.

Atskaitingumo principas reiškia, kad turi būti aiškiai apibrėžtos pareigos saugumo srityje. Be to, atskaitingumas žymi poreikį reguliariai tikrinti, ar tos pareigos tinkamai vykdomos.

Subsidiarumo principas reiškia, kad saugumu turi būti pasirūpinama pačiu žemiausiu lygmeniu ir kuo arčiau Europos Parlamento generalinių direktoratų bei tarnybų.

Proporcingumo principas reiškia, kad saugumo veikla turi griežtai apsiriboti tomis sritimis, kurioms saugumas tikrai reikalingas, o saugumo priemonės turi būti proporcingos ginamiems interesams bei tikrai arba galimai grėsmei tiems interesams, siekiant, kad jie būtų ginami taip, kad būtų sukeliama mažiausiai nepatogumų.

3. INFORMACIJOS SAUGUMO PAGRINDAI

Patikimas informacijos saugumas grindžiamas:

a) tinkamomis ryšių ir informacijos sistemomis (RIS). Už jas yra atsakinga Europos Parlamento saugumo institucija (kaip apibrėžta I saugumo pranešime);
b) Europos Parlamente – Informacijos saugumo užtikrinimo institucija (kaip apibrėžta I saugumo pranešime), atsakinga už bendradarbiavimą su atitinkama saugumo institucija ir už informacijos ir konsultacijų apie technines grėsmes RIS ir apsaugos nuo tų grėsmių priemonių teikimą;
c) glaudžiu atsakingų Europos Parlamento tarnybų ir kitų Europos Sąjungos institucijų saugumo tarnybų bendradarbiavimu.

4. INFORMACIJOS APSAUGOS PRINCIPAI

4.1. *Tikslai*

Svarbiausi informacijos apsaugos tikslai yra:

a) apsaugoti konfidencialią informaciją nuo šnipinėjimo, neteisėto atskleidimo arba neleistino platinimo;
b) apsaugoti ryšių ir informacijos sistemose bei tinkluose tvarkomą įslaptintą informaciją nuo grėsmės jos slaptumui, vientisumui ir prieinamumui;
c) apsaugoti Europos Parlamento pastatus, kuriuose saugoma įslaptinta informacija, nuo sabotažo ir tyčinės žalos;
d) saugumo pažeidimo atveju įvertinti padarytą žalą, apriboti jos padarinius, atlikti saugumo tyrimus ir imtis būtinų jos pašalinimo priemonių.

4.2. *Įslaptinimas*

4.2.1. Siekiant, kad būtų užtikrintas konfidencialumas, atrenkant dėl slaptumo saugotiną informaciją bei medžiagą ir įvertinant, koks turi būti jos apsaugos laipsnis, reikalingas atidumas ir patirtis. Labai svarbu, kad saugotinos informacijos ir medžiagos apsaugos laipsnis atitiktų jų svarbą saugumo požiūriu. Siekiant užtikrinti sklandų informacijos srautą, imamasi veiksmų, kad įslaptinimas nebūtų nei per didelis, nei per mažas.

4.2.2. Įslaptinimo sistema – šioje dalyje nustatytų principų įgyvendinimo priemonė. Numatant ir organizuojant kovos su šnipinėjimu, sabotažu, terorizmu ir kitokiomis grėsmėmis veiksmus reikia laikytis panašios įslaptinimo sistemos, kad labiausiai būtų apsaugoti svarbiausi pastatai, kuriuose laikoma įslaptinta informacija, ir lengviausiai pažeidžiamos vietos tuose pastatuose.

4.2.3. Atsakomybė už informacijos įslaptinimą tenka tik susijusios informacijos rengėjui.

4.2.4. Slaptumo žymos laipsnis gali būti grindžiamas tik susijusios informacijos turiniu.

4.2.5. Tais atvejais, kai sugrupuojami keli informacijos vienetai, jiems skiriamas slaptumo žymos laipsnis turi būti ne mažesnis už aukščiausią slaptumo žymos laipsnį turinčio informacijos vieneto laipsnį. Tačiau informacijos rinkiniui galima suteikti aukštesnį už sudedamosioms dalims suteiktą slaptumo žymos laipsnį.

4.2.6. Slaptumo žymos dedamos tik tuomet, kai būtina, ir tik tokiam laikotarpiui, kokiam reikia.

4.3. *Saugumo priemonių paskirtis*

Saugumo priemonės:

a) taikomos visiems įslaptinta informacija, elektroninėmis laikmenomis, kuriose saugoma įslaptinta informacija, ir kita konfidencialia informacija galintiems naudotis asmenims, taip pat visiems pastatams, kuriuose yra tokios informacijos ir svarbių įrengimų;
b) sukuriamos taip, kad būtų galima nustatyti asmenis, kurių padėtis (prieigos teisės, ryšiai ar kt.) gali kelti grėsmę tokios informacijos ir svarbių įrengimų, kuriuose laikoma tokia informacija, saugumui, ir neprileisti tokių asmenų prie minėtos informacijos arba nušalinti nuo jos;
c) neleidžia jokiam leidimo neturinčiam asmeniui naudotis tokia informacija arba įrengimais, kuriuose ji laikoma;
d) užtikrina tokios informacijos skleidimą tik pagal visiems saugumo aspektams svarbiausią principą „būtina žinoti“;
e) užtikrina visos konfidencialios, tiek įslaptintos, tiek neįslaptintos, ir ypač elektromagnetinėse laikmenose laikomos, apdorotos arba perduotos informacijos vientisumą (užkerta kelią klastojimui, taisymui ar ištrynimui be leidimo) ir galimybę ja naudotis (tiems, kuriems ji reikalinga, ir turintiesiems leidimą ja naudotis).

5. BENDRI BŪTINIAUSI STANDARTAI

Europos Parlamentas užtikrina, jog visi įslaptintos informacijos gavėjai pačioje institucijoje ir jos kompetencijai priklausančiose institucijose, t. y. visos tarnybos ir sutarčių partneriai, laikytųsi bendrų būtiniausių saugumo standartų, kad tokia informacija būtų perduodama įsitikinus, jog ji bus taip pat atsakingai tvarkoma. Prie tokių būtiniausių standartų priskiriami asmens patikimumo patvirtinimo Europos Parlamento pareigūnams ir kitiems Parlamento darbuotojams, dirbantiems frakcijose, suteikimo kriterijai ir konfidencialios informacijos apsaugos procedūros.

Europos Parlamentas suteikia teisę trečiosioms šalims naudotis tokia informacija, tik jei šios užtikrina, kad tvarkydamos ją griežtai laikysis bent šiuos būtiniausius standartus tiksliai atitinkančių nuostatų.

Tokie bendri būtiniausi standartai taip pat taikomi, kai Europos

Parlamentas pagal sutartį ar susitarimą dėl leidimo pramonės ar kitokiems subjektams paveda atlikti užduotis, susijusias su konfidencialia informacija.

6. EUROPOS PARLAMENTO PAREIGŪNŲ IR KITŲ FRAKCIJOSE DIRBANČIŲ PARLAMENTO DARBUOTOJŲ SAUGUMAS

6.1. *Europos Parlamento pareigūnų ir kitų Parlamento darbuotojų, kurie dirba frakcijose, instruktavimas saugumo klausimais*

Europos Parlamento pareigūnai ir kiti Parlamento darbuotojai, kurie dirba frakcijose, einantys pareigas, sudarančias galimybes naudotis įslaptinta informacija, pradėdami eiti pareigas ir vėliau reguliariai nuodugniai instruktuojami apie saugumo svarbą ir jo užtikrinimo procedūras. Tokie asmenys privalo raštu patvirtinti, kad susipažino su taikytinais saugumo reikalavimais ir kad juos visiškai supranta.

6.2. *Vadovų atsakomybė*

Žinoti, kurie vadovų darbuotojai dirba su įslaptinta informacija arba gali naudotis saugiomis ryšių ar informacijos sistemomis, bei registruoti ir pranešti apie visus galinčius turėti įtakos saugumui incidentus arba pažeidimus, – turi būti tų vadovų atsakomybės dalis.

6.3. *Europos Parlamento pareigūnų ir kitų Parlamento darbuotojų, dirbančių frakcijose, saugumo statusas*

Nustatoma tvarka, užtikrinanti, kad, gavus nepalankios informacijos apie Europos Parlamento pareigūną ar apie kitą Parlamento darbuotoją, dirbantį frakcijose, imamasi veiksmų, siekiant nustatyti, ar tas asmuo darbo metu gali susipažinti su įslaptinta informacija arba naudotis saugiomis ryšių arba informacijos sistemomis, ir informuojama atsakinga Europos Parlamento tarnyba. Jei kompetentinga nacionalinė saugumo institucija nurodo, kad toks asmuo kelia grėsmę saugumui, jam neleidžiama atlikti pareigų arba jis nušalinamas nuo pareigų, kurias eidamas gali kelti grėsmę saugumui.

7. FIZINIS SAUGUMAS

Fizinis saugumas – fizinių ir techninių apsaugos priemonių taikymas siekiant užkirsti kelią leidimo neturintiems asmenims susipažinti su įslaptinta informacija.

7.1. *Apsaugos poreikis*

Fizinio saugumo priemonių, taikytinų užtikrinant įslaptintos informacijos apsaugą, veiksmingumo laipsnis turi būti proporcingas laikomos informacijos ir medžiagos slaptumui, kiekiui ir galimai grėsmei. Visi įslaptintos informacijos laikytojai laikosi vienodos tokios informacijos įslaptinimo praktikos ir privalo paisyti bendrų apsaugos standartų, susijusių su saugomos informacijos ir medžiagos laikymu, perdavimu ir naikinimu.

7.2. *Tikrinimas*

Prieš išeidami iš zonų, kuriose be priežiūros paliekama įslaptinta informacija, už jos laikymą atsakingi asmenys užtikrina, kad ji būtų paliekama saugiai ir kad būtų aktyvuotos visos apsaugos priemonės (užraktai, signalizacija ir kt.). Tolesni nepriklausomi tikrinimai atliekami po darbo valandų.

7.3. *Pastatų saugumas*

Pastatai, kuriuose kaupiama įslaptinta informacija arba laikomos saugios ryšių ir informacijos sistemos, saugomi, kad į juos nepatektų leidimo neturintys asmenys.

Įslaptintos informacijos apsaugos pobūdis, pvz., langų grotos, durų užraktai, apsauga prie įėjimų, automatizuotos prieigos kontrolės sistemos, apsaugos tikrinimai ir patruliai, signalizacijos sistemos, į įsibrovimą reaguojančios sistemos ir sarginiai šunys, priklauso nuo:

a) saugotinos informacijos ir medžiagos slaptumo lygio, kiekio ir jų laikymo vietos pastate;
b) atitinkamos informacijos ir medžiagos apsauginių talpyklų kokybės i
c) pastato fizinių savybių ir vietos.

Ryšių ir informacijos sistemų apsaugos pobūdis priklauso nuo laikomo turto vertės ir galimos žalos, jei kiltų grėsmė saugumui, įvertinimo, nuo pastato, kuriame sistema laikoma, fizinių savybių bei vietos ir nuo tos sistemos vietos pastate.

7.4. *Nenumatytų atvejų planai*

Iš anksto parengiami išsamūs įslaptintos informacijos apsaugos ištikus nenumatytam atvejui planai.

8. SLAPTUMO ŽYMOS GALIOJIMO ŽYMOS, KITOS ŽYMOS, ŽYMŲ NURODYMAS IR ĮSLAPTINIMO ADMINISTRAVIMAS

8.1. *Slaptumo žymos galiojimo žymos*

Nėra leidžiamos jokios kitos slaptumo žymos, kaip tik tos, kurios nurodytos šio sprendimo 2 straipsnio d punkte.

Slaptumo žymos galiojimo terminams nustatyti (įslaptintai informacijai, kuriai taikomas automatinis slaptumo laipsnio sumažinimas arba išslaptinimas) gali būti naudojama sutarta slaptumo žymos galiojimo žyma.

Slaptumo žymos galiojimo žymos naudojamos tik kartu su slaptumo žymomis.

Slaptumo žymos galiojimo žymos išsamiau reglamentuotos II saugumo pranešime ir nustatytos naudojimo nurodymuose.

8.2. *Kitos žymos*

Kita žyma naudojama, kai reikia tiksliai apibrėžti iš anksto numatytus konkrečius nurodymus dėl konfidencialios informacijos tvarkymo. Kitos žymos taip pat gali nurodyti tam tikro dokumento taikymo sritį, pažymėti specialų jo platinimą vadovaujantis principu „būtina žinoti“ ar nurodyti, kada baigiasi draudimas platinti (neįslaptintos informacijos atveju).

Kita žyma nėra slaptumo žyma, todėl vietoje jos nenaudojama.

Kitos žymos išsamiau reglamentuotos II saugumo pranešime ir nustatytos naudojimo nurodymuose.

8.3. *Slaptumo žymų ir slaptumo žymų galiojimo žymų nurodymas*

Slaptumo žymos, slaptumo žymų galiojimo žymos ir kitos žymos nurodomos pagal II saugumo pranešimo E dalį ir naudojimo nurodymus.

8.4. *Įslaptinimo administravimas*

8.4.1. *Bendra padėtis*

Informacija įslaptinama tik tuomet, kai tai būtina. Slaptumo žyma aiškiai ir teisingai nurodoma ir taikoma tik tol, kol informaciją reikia saugoti.

Atsakomybė už informacijos įslaptinimą ir už bet kokį paskesnį slaptumo žymos laipsnio sumažinimą arba informacijos išslaptinimą tenka tik informacijos rengėjui.

Europos Parlamento pareigūnai informaciją įslaptina, sumažina jos slaptumo laipsnį arba informaciją išslaptina tik gavę generalinio sekretoriaus nurodymą arba remdamiesi jo suteiktais įgaliojimais.

Detali įslaptintų dokumentų naudojimo tvarka parengiama taip, kad būtų užtikrinta derama juose esančios informacijos apsauga.

Asmenų, turinčių leidimą rengti slaptumo žymos TRÈS SECRET UE/EU TOP SECRET laipsniu žymimą informaciją, turi būti kuo mažiau, o jų vardai ir pavardės įtraukiamos į ĮIS sudarytą sąrašą.

8.4.2. *Slaptumo žymų naudojimas*

Dokumento slaptumo žymos laipsnis nustatomas pagal 2 straipsnio d punkte apibrėžtą jo turinio slaptumo laipsnį. Svarbu, kad slaptumo žymos būtų taikomos teisingai ir nuosaikiai.

Pridedamų dokumentų lydraščių arba pranešimų slaptumo žymos laipsnis atitinka priedų aukščiausio laipsnio slaptumo žymos laipsnį. Jei lydraščiai ar pranešimai pateikiami atskirai nuo priedų, rengėjas turi aiškiai nurodyti, koks slaptumo žymos laipsnis jiems suteikiamas.

Įslaptinamo dokumento rengėjas turi laikytis minėtų taisyklių ir vengti suteikti pernelyg aukštą ar pernelyg žemą slaptumo žymos laipsnį.

Prireikus atitinkamo dokumento atskiriems lapams, dalims, skyriams,

priedams, priedėliams ir pridedamiems dokumentams suteikti skirtingas slaptumo žymas, jie atitinkamai įslaptinami. Visas dokumentas įslaptinamas pagal aukščiausią slaptumo žymos laipsnį turinčią dokumento dalį.

9. PATIKRINIMAI

Europos Parlamento Saugos ir rizikos vertinimo direktoratas, kuris gali prašyti pagalbos Komisijos arba Tarybos saugumo tarnybų, reguliariai atlieka vidinius įslaptintos informacijos apsaugai skirtų saugumo priemonių patikrinimus.

Europos Sąjungos institucijų saugumo tarnybos ir kompetentingos tarnybos, vykdydamos vieno iš subjektų inicijuotą ir kitiems subjektams sutinkant pradėtą procedūrą, gali atlikti apsaugos priemonių, kuriomis siekiama apsaugoti įslaptintą informaciją, kuria apsikeista pagal atitinkamus tarpinstitucinius susitarimus, tarpusavio vertinimą.

10. IŠSLAPTINIMO IR KITŲ ŽYMŲ PANAIKINIMO PROCEDŪROS

10.1. ĮIS išnagrinėja savo registre laikomą konfidencialią informaciją ir prašo dokumento rengėjo leisti išslaptinti arba panaikinti kitas dokumento žymas ne vėliau kaip 25-aisiais metais nuo jo parengimo. Po pirmo patikrinimo neišslaptinti dokumentai arba dokumentai, kurių žymos nepanaikintos, dar kartą tikrinami periodiškai ir ne rečiau nei kas penkerius metus. Kitų žymų panaikinimo procedūra gali būti taikoma ne tik dokumentams, kurie šiuo metu jau saugomi saugioje zonoje esančiuose saugiuose archyvuose ir yra tinkamai įslaptinti, bet ir kitai konfidencialiai informacijai, laikomai Parlamento organo ar atitinkamas pareigas einančio asmens sekretoriate arba už Parlamento istorinius archyvus atsakingoje tarnyboje.

10.2. Sprendimą dėl dokumento išslaptinimo arba kitų žymų panaikinimo paprastai priima tik rengėjas arba, išimtiniais atvejais, prieš dokumento informaciją persiunčiant už Parlamento istorinius archyvus atsakingai tarnybai, toks sprendimas priimamas bendradarbiaujant su tokią informaciją turinčiu Parlamento organo ar atitinkamas pareigas einančio asmens sekretoriatu. Išslaptinti įslaptintą informaciją ar panaikinti jos žymą galima tik gavus išankstinį raštišką rengėjo sutikimą. Kitos konfidencialios informacijos atveju tokią informaciją turintis Parlamento or-

gano ar atitinkamas pareigas einančio asmens sekretoriatas, bendradarbiaudamas su informacijos rengėju, priima sprendimą dėl tokio dokumento žymos panaikinimo.

10.3. Rengėjo vardu ĮIS atsako už to dokumento gavėjų informavimą apie slaptumo žymos arba kitos žymos pakeitimą, o šie atitinkamai atsako už kitų gavėjų, kuriems jie yra nusiuntę dokumentą arba jo kopiją, informavimą.

10.4. Išslaptinimas neturi jokio poveikio kitoms slaptumo žymų galiojimo žymoms arba kitoms žymoms, galinčioms atsirasti ant dokumento.

10.5. Išslaptinimo atveju pradinė slaptumo žyma kiekvieno puslapio viršuje ir apačioje išbraukiama. Ant pirmo dokumento puslapio dedamas antspaudas ir pateikiama ĮIS nuoroda. Kitos žymos panaikinimo atveju pradinė žyma kiekvieno (antraštinio) pirmo puslapio viršuje išbraukiama.

10.6. Išslaptinto dokumento arba dokumento, kurio žyma panaikinta, tekstas pridedamas prie elektroninės formos ar atitinkamos sistemos, kurioje jis buvo registruotas.

10.7. Kai dokumentams taikoma išimtis, susijusi su privatumu ir asmens neliečiamumu ar fizinio arba juridinio asmens prekybiniais interesais ir kai dokumentai yra slapto pobūdžio, taikomas Reglamento (EEB, Euratomas) Nr. 354/83 2 straipsnis.

10.8. Be 10.1–10.7 papunkčių nuostatų, taip pat taikomos šios taisyklės:

a) kalbant apie trečiųjų šalių dokumentus ĮIS, prieš vykdydamas išslaptinimą arba panaikindamas kitą žymą, konsultuojasi su susijusia trečiąja šalimi;
b) kalbant apie taikomas išimtis, susijusias su privatumu ir asmens neliečiamumu, vykdant išslaptinimo arba kitos žymos panaikinimo procedūrą, yra ypatingai atsižvelgiama į susijusio asmens sutikimą arba, jei reikia, į tai, kad neįmanoma nustatyti susijusio asmens tapatybės;
c) kalbant apie taikomas išimtis, susijusias su fizinio ar juridinio asmens prekybiniais interesais, susijusiam asmeniui gali būti pranešama, paskelbus informaciją *Europos Sąjungos oficialiajame leidinyje*, ir jam gali būti suteiktas keturių savaičių terminas nuo informacijos paskelbimo dienos pastaboms pateikti.

2 dalis.

ASMENS PATIKIMUMO TIKRINIMO TVARKA

11. ASMENS PATIKIMUMO TIKRINIMO TVARKA, TAIKOMA EUROPOS PARLAMENTO NARIAMS

11.1. Kad galėtų susipažinti su slaptumo žymos CONFIDENTIEL UE/EU CONFIDENTIAL arba jam lygiaverčiu laipsniu pažymėta informacija, Europos Parlamento nariai turi turėti leidimą, suteiktą šio priedo 11.3 ir 11.4 papunkčiuose nustatyta tvarka arba būti pasirašę šio sprendimo 3 straipsnio 4 dalyje nurodytą oficialų pareiškimą neatskleisti informacijos.

11.2. Kad galėtų susipažinti su slaptumo žymos SECRET UE/EU SECRET arba TRÈS SECRET UE/EU TOP SECRET laipsniu arba jam lygiaverčiu pažymėta informacija, Europos Parlamento nariai turi turėti leidimą, suteiktą 11.14 ir 11.4 papunkčiuose nustatyta tvarka.

11.3. Leidimas suteikiamas tik tiems Europos Parlamento nariams, kurių patikimumą 11.9–11.14 papunkčiuose nurodyta tvarka yra patikrinusios valstybių narių kompetentingos nacionalinės institucijos. Pirmininkas atsakingas už leidimų suteikimą nariams.

11.4. Pirmininkas gali išduoti raštišką leidimą, gavęs valstybės narės kompetentingos nacionalinės institucijos nuomonę, pagrįstą 11.8–11.13 papunkčiuose nurodyta tvarka atlikto asmens patikimumo patikrinimo rezultatais.

11.5. Europos Parlamento Saugos ir rizikos vertinimo direktoratas veda nuolat atnaujinamą visų Europos Parlamento narių, kuriems buvo suteiktas leidimas, sąrašą, įskaitant laikinus leidimus, kaip nurodyta 11.15 punkte.

11.6. Leidimas galioja penkerius metus arba tą laikotarpį, kurio reikia užduotims, kurioms jis buvo išduotas, atlikti, atsižvelgiant į tai, kuris laikotarpis trumpesnis. Leidimą galima atnaujinti 11.4 papunktyje nurodyta tvarka.

11.7. Pirmininkas panaikina leidimą, jei mano esant tokiam panaikinimui pagrįstų priežasčių. Apie bet kokį sprendimą panaikinti leidimą turi būti pranešta atitinkamam Europos Parlamento nariui, kuris, prieš sprendimui įsigaliojant, gali prašyti, kad Pirmininkas jį išklausytų, taip

pat apie tai pranešama kompetentingai nacionalinei institucijai.

11.8. Asmens patikimumo patikrinimas atliekamas padedant atitinkamam Europos Parlamento nariui ir Pirmininko prašymu. Patikrinimą turi atlikti tik tos valstybės narės, kurios pilietis yra leidimo prašantis Parlamento narys, kompetentinga nacionalinė institucija.

11.9. Pagal tikrinimo tvarką reikalaujama, kad atitinkamas Europos Parlamento narys užpildytų asmens informacijos anketą.

11.10. Savo prašyme kompetentingai nacionalinei institucijai Pirmininkas patikslina įslaptintos informacijos, su kuria susipažins atitinkamas Europos Parlamento narys, laipsnį, kad jos galėtų atlikti patikrinimą.

11.11. Visa asmens patikimumo patikrinimo procedūra, kurią vykdo kompetentinga nacionalinė institucija, ir gauti rezultatai turi atitikti atitinkamoje valstybėje narėje galiojančias normas ir taisykles, įskaitant su apeliacijomis susijusias normas ir taisykles.

11.12. Gavęs kompetentingos nacionalinės institucijos teigiamą nuomonę, Pirmininkas gali atitinkamam Europos Parlamento nariui suteikti leidimą.

11.13. Apie neigiamą kompetentingos nacionalinės institucijos nuomonę pranešama atitinkamam Europos Parlamento nariui, kuris gali prašyti, kad Pirmininkas jį išklausytų. Pirmininkas, jei mano esant reikalinga, gali paprašyti kompetentingos nacionalinės institucijos papildomo paaiškinimo. Jei neigiama nuomonė patvirtinama, leidimas nesuteikiamas.

11.14. Visi Europos Parlamento nariai, kuriems pagal 11.3 papunktį suteiktas leidimas, leidimo suteikimo metu ir reguliariai po to gauna visus būtinus nurodymus, susijusius su įslaptintos informacijos apsauga ir šios apsaugos užtikrinimo priemonėmis. Tokie nariai pasirašo pareiškimą, kuriame patvirtina gavę tas instrukcijas.

11.15. Išskirtiniais atvejais Pirmininkas, pranešęs kompetentingai nacionalinei institucijai ir per vieną mėnesį negavęs tos institucijos atsakymo, kol laukiama 11.11 papunktyje nurodyto patikrinimo rezultatų, gali Europos Parlamento nariui ne ilgiau kaip šešiems mėnesiams suteikti laikinąjį leidimą. Laikinieji leidimai nesuteikia teisės susipažinti su slaptumo žymos TRÈS SECRET UE/EU TOP SECRET laipsniu ar jam lygiaverčiu pažymėta informacija.

12. ASMENS PATIKIMUMO TIKRINIMO TVARKA, TAIKOMA EUROPOS PARLAMENTO PAREIGŪNAMS IR KITIEMS PARLAMENTO DARBUOTOJAMS, DIRBANTIEMS FRAKCIJOSE

12.1. Tik Europos Parlamento pareigūnai ir kiti Parlamento darbuotojai, dirbantys frakcijose, kurie dėl savo pareigų ir tarnybos reikalavimų turi būti susipažinę su įslaptinta informacija arba turi ją naudoti, gali susipažinti su tokia informacija.

12.2. Kad atitinkami Europos Parlamento pareigūnai ir kiti Parlamento darbuotojai, dirbantys frakcijose, galėtų susipažinti su slaptumo žymos CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ar TRÈS SECRET UE/EU TOP SECRET laipsniu ar jam lygiaverčiu pažymėta informacija, jiems suteikiamas leidimas 12.3 ir 12.4 papunkčiuose nustatyta tvarka.

12.3. Leidimas išduodamas tik 12.1 papunktyje nurodytiems asmenims, kurių patikimumą 12.9–12.14 papunkčiuose nurodyta tvarka yra patikrinusios valstybių narių kompetentingos nacionalinės institucijos. Generalinis sekretorius atsakingas už leidimų suteikimą Europos Parlamento pareigūnams ir kitiems Parlamento darbuotojams, dirbantiems frakcijose.

12.4. Generalinis sekretorius gali išduoti raštišką leidimą gavęs valstybės narės kompetentingos nacionalinės institucijos nuomonę, pagrįstą 12.8–12.13 papunkčiuose nurodyta tvarka atlikto asmens patikimumo patikrinimo rezultatais.

12.5. Europos Parlamento Saugos ir rizikos vertinimo direktoratas veda nuolat atnaujinamą visų pareigų, kurias einantys asmenys turi turėti asmens patikimumo patvirtinimą ir kurias nurodo atitinkamos Europos Parlamento tarnybos, ir visų asmenų, kuriems suteiktas leidimas, įskaitant laikinąjį leidimą pagal 12.15 papunktį, sąrašą.

12.6. Leidimas galioja penkerius metus arba tą laikotarpį, kurio reikia užduotims, kurioms jis buvo išduotas, atlikti, atsižvelgiant į tai, kuris laikotarpis trumpesnis. Leidimą galima atnaujinti 12.4 papunktyje nurodyta tvarka.

12.7. Generalinis sekretorius panaikina leidimą, jei mano esant pagrįstų priežasčių tam panaikinimui. Apie bet kokį sprendimą panaikinti leidimą turi būti pranešta atitinkamam Europos Parlamento pareigūnui

ar kitam Parlamento darbuotojui, dirbančiam frakcijoje, kuris, prieš įsigaliojant sprendimui panaikinti leidimą, gali prašyti, kad generalinis sekretorius jį išklausytų, taip pat apie tai pranešama ir kompetentingai nacionalinei institucijai.

12.8. Asmens patikimumo patikrinimas generalinio sekretoriaus prašymu atliekamas padedant atitinkamam Europos Parlamento pareigūnui arba kitam Parlamento darbuotojui, dirbančiam frakcijose. Patikrinimą atlieka tos valstybės narės, kurios pilietis yra leidimo prašantis asmuo, kompetentinga nacionalinė institucija. Kai leidžiama pagal nacionalinius įstatymus ir teisės aktus, kompetentingos nacionalinės institucijos gali atlikti tyrimus, susijusius su užsienio piliečių reikalavimu susipažinti su slaptumo žymos CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ar TRÈS SECRET UE/EU TOP SECRET laipsniu pažymėta informacija.

12.9. Pagal tikrinimo tvarką reikalaujama, kad atitinkamas Europos Parlamento pareigūnas ar kitas Parlamento darbuotojas, dirbantis frakcijoje, užpildytų asmens informacijos anketą.

12.10. Generalinis sekretorius savo prašyme kompetentingai nacionalinei institucijai nurodo įslaptintos informacijos, su kuria atitinkamam Europos Parlamento pareigūnui arba kitam Parlamento darbuotojui, dirbančiam frakcijose, turėtų būti leista susipažinti, slaptumo žymos laipsnį, kad jis galėtų atlikti patikrinimą ir pateikti savo nuomonę dėl to, su kokio slaptumo žymos laipsnio informacija derėtų leisti susipažinti šiam asmeniui.

12.11. Visa kompetentingos nacionalinės institucijos atliekamo asmens patikimumo patikrinimo tvarka ir gauti rezultatai turi atitikti atitinkamoje valstybėje narėje galiojančias normas ir taisykles, įskaitant su apeliacijomis susijusias normas ir taisykles.

12.12. Gavęs kompetentingos nacionalinės institucijos teigiamą nuomonę, generalinis sekretorius gali atitinkamam Europos Parlamento pareigūnui arba kitam Parlamento darbuotojui, dirbančiam frakcijose, suteikti leidimą.

12.13. Apie neigiamą kompetentingos nacionalinės institucijos nuomonę pranešama atitinkamam Europos Parlamento pareigūnui ir kitam Parlamento darbuotojui, dirbančiam frakcijoje, o jis gali prašyti, kad generalinis sekretorius jį išklausytų. Jei generalinis sekretorius mano, kad tai tikslinga, jis gali paprašyti kompetentingos nacionalinės institucijos

papildomo paaiškinimo. Jei neigiama nuomonė patvirtinama, leidimas nesuteikiamas.

12.14. Visi Europos Parlamento pareigūnai ir kiti Parlamento darbuotojai, dirbantys frakcijose, kuriems leidimai suteikti pagal 12.4 ir 12.5 papunkčius, leidimo suteikimo metu ir reguliariai po to gauna visus būtinus nurodymus, susijusius su įslaptintos informacijos apsauga ir šios apsaugos užtikrinimo priemonėmis. Tokie pareigūnai ir darbuotojai pasirašo deklaracijas, kuriose patvirtina gavę nurodymus ir įsipareigoja jų laikytis.

12.15. Išimtiniais atvejais generalinis sekretorius, pranešęs kompetentingai nacionalinei institucijai ir per vieną mėnesį negavęs jos atsakymo, kol laukiama šios dalies 12.11 papunktyje nurodyto patikrinimo rezultatų, gali ne ilgiau kaip šešiems mėnesiams Europos Parlamento pareigūnui ar kitam Parlamento darbuotojui, dirbančiam frakcijoje, suteikti laikinąjį leidimą. Laikinieji leidimai nesuteikia teisės susipažinti su slaptumo žymos TRÈS SECRET UE/EU TOP SECRET laipsniu arba jam lygiaverčiu pažymėta informacija.

II PRIEDAS

ĮŽANGA

Šiomis nuostatomis apibrėžiami saugumo pranešimai, kuriais reglamentuojamas ir užtikrinamas Europos Parlamento atliekamas saugus konfidencialios informacijos tvarkymas ir valdymas. Tie saugumo pranešimai kartu su visais naudojimo nurodymais sudaro šio sprendimo 3 straipsnio 2 dalyje nurodytą Europos Parlamento informacijos saugumo valdymo sistemą (ISVS):

I SAUGUMO PRANEŠIMAS

Saugumo organizavimas Europos Parlamente siekiant apsaugoti konfidencialią informaciją

II SAUGUMO PRANEŠIMAS

Konfidencialios informacijos valdymas

III SAUGUMO PRANEŠIMAS

Konfidencialios informacijos tvarkymas naudojant automatines ryšių informacines sistemas (RIS)

IV SAUGUMO PRANEŠIMAS

Fizinis saugumas

V SAUGUMO PRANEŠIMAS

Pramoninis saugumas

VI SAUGUMO PRANEŠIMAS

Konfidencialios informacijos saugumo pažeidimai, praradimas arba neteisėtas atskleidimas

I SAUGUMO PRANEŠIMAS

SAUGUMO ORGANIZAVIMAS EUROPOS PARLAMENTE SIEKIANT APSAUGOTI KONFIDENCIALIĄ INFORMACIJĄ

1. Generalinis sekretorius atsakingas už visapusišką ir nuoseklų šio sprendimo įgyvendinimą.

Generalinis sekretorius imasi visų reikiamų priemonių, kad užtikrintų, jog konfidencialios informacijos tvarkymo ar saugojimo atveju Europos Parlamento nariai, Europos Parlamento pareigūnai, kiti Parlamento darbuotojai, dirbantys frakcijose, ir rangovai Parlamento patalpose taikytų šį sprendimą.

2. Generalinis sekretorius yra saugumo institucija (SĮ). Vykdydamas šias funkcijas generalinis sekretorius atsako už:

2.1. visų su Parlamento veikla susijusių saugumo klausimų koordinavimą konfidencialios informacijos apsaugos srityje;

2.2. leidimą įrengti saugią zoną, saugias skaityklas ir įdiegti saugią įrangą;

2.3. sprendimų, kuriais pagal šio sprendimo 6 straipsnį suteikiamas leidimas Parlamentui perduoti įslaptintą informaciją trečiosioms šalims, įgyvendinimą;

2.4. tyrimą ir nurodymą atlikti tyrimą dėl neteisėto konfidencialios informacijos atskleidimo, kuri *prima facie* buvo atskleista Parlamente, o jei su tuo susijęs Europos Parlamento narys – pasitarus su Europos Parlamento pirmininku;

2.5. glaudų bendradarbiavimą su Europos Sąjungos kitų institucijų saugumo tarnybomis ir valstybių narių nacionalinėmis saugumo institucijomis, siekiant užtikrinti geriausią su įslaptinta informacija susijusios saugumo politikos koordinavimą;

2.6. nuolatinį Parlamento saugumo politikos ir tvarkos tikrinimą ir atitinkamų deramų rekomendacijų teikimą;

2.7. nacionalinės saugumo institucijos (NSI), kuri pagal I priedo 2 dalies 11.3 papunktį atliko asmens patikimumo patikrinimą, informavimą tais atvejais, kai bet kokia neigiama informacija gali turėti poveikį tai institucijai.

3. Atvejais, kurie susiję su Europos Parlamento nariais, generali-

nis sekretorius savo pareigas vykdo glaudžiai bendradarbiaudamas su Europos Parlamento pirmininku.

4. Generaliniam sekretoriui atliekant savo pareigas pagal 2 ir 3 dalis padeda generalinio sekretoriaus pavaduotojas, Saugos ir rizikos vertinimo direktoratas, Informacinių technologijų direktoratas (ITD) ir Įslaptintos informacijos skyrius (ĮIS).

4.1.Saugos ir rizikos vertinimo direktoratas atsakingas už asmenines apsaugos priemones ir ypač už asmens patikimumo tikrinimą, kaip nustatyta I priedo 2 dalyje. Saugos ir rizikos vertinimo direktoratas taip pat:

a) yra Europos Sąjungos kitų institucijų saugumo tarnybų ir nacionalinių saugumo tarnybų kontaktinis centras klausimais, susijusiais su asmens patikimumo tikrinimu, atliekamu dėl Europos Parlamento narių, Europos Parlamento pareigūnų ir kitų Parlamento darbuotojų, dirbančių frakcijose;
b) rengia būtinus informavimo renginius bendro saugumo klausimais apie prievolę apsaugoti įslaptintą informaciją ir bet kokio šios prievolės pažeidimo pasekmes;
c) stebi, kaip naudojamasi saugia zona ir saugiomis skaityklomis Parlamento patalpose, jei reikia, bendradarbiaudamas su Europos Sąjungos kitų institucijų ir valstybių narių saugumo tarnybomis;
d) kontroliuoja, bendradarbiaudamas su kitų Europos Sąjungos institucijų ir valstybių narių saugumo tarnybomis, įslaptintos informacijos valdymą ir laikymą, saugią zoną ir saugias skaityklas Parlamento patalpose, kuriose tvarkoma įslaptinta informacija;
e) generaliniam sekretoriui teikia pasiūlymus dėl reikiamų naudojimo nurodymų.

4.2. ITD atsakingas už saugias IT sistemas, kurias Europos Parlamentas naudoja tvarkydamas konfidencialią informaciją.

4.3. ĮIS atsakingas už:

a) saugumo poreikių nustatymą siekiant veiksmingai apsaugoti konfidencialią informaciją, glaudžiai bendradarbiaujant su Saugos ir rizikos vertinimo direktoratu ir ITD ir kitų Europos Sąjungos institucijų saugumo tarnybomis;
b) konfidencialios informacijos valdymo ir laikymo Parlamente visų aspektų nustatymą, kaip nustatyta naudojimo nurodymuose;
c) saugios zonos naudojimą;

d) konfidencialios informacijos valdymą ir susipažinimą su ja saugioje zonoje arba ĮIS saugioje skaitykloje pagal šio sprendimo 7 straipsnio 2 ir 3 dalis;
e) ĮIS registro valdymą;
f) SI informavimą apie bet kokius įrodytus ar tariamus konfidencialios informacijos, pateikiamos ĮIS ir laikomos saugioje zonoje arba ĮIS saugioje skaitykloje, saugumo pažeidimus, praradimą arba neteisėtą atskleidimą.

5. Be to, generalinis sekretorius, kaip SI, skiria šias institucijas:
a) Saugumo akreditavimo instituciją (SAI);
b) Informacijos saugumo užtikrinimo operacinę instituciją (ISUOI);
c) Kriptografijos platinimo instituciją (KPLI);
d) TEMPEST instituciją (TEI);
e) Informacijos saugumo užtikrinimo instituciją (ISUI).

Šioms funkcijoms atlikti nereikia atskirų organizacinių vienetų. Šioms institucijoms suteikiami atskiri įgaliojimai. Tačiau šios funkcijos ir su jomis susijusi atsakomybė gali būti susietos arba integruotos viename organizaciniame vienete arba padalytos skirtingiems organizaciniams vienetams, jei išvengiama interesų konfliktų ir užduočių kartojimosi.

6. SAI konsultuoja visais saugumo klausimais, susijusiais su visų informacinių technologijų sistemų ir tinklų akreditavimu Parlamente:
6.1. užtikrindama, kad RIS atitiktų atitinkamą saugumo politiką ir saugumo gaires, pateikdama pareiškimą dėl RIS patvirtinimo, leidžiant ją naudoti įslaptintos informacijos tvarkymui iki nustatyto slaptumo žymos laipsnio informacijos operacinėje aplinkoje, ir nurodydama akreditavimo reikalavimus ir sąlygas bei kriterijus, kuriais remiantis reikalaujama, kad reikia iš naujo patvirtinti RIS;
6.2. nustatydama saugumo akreditavimo tvarką pagal atitinkamą politiką, aiškiai nurodydama patvirtinimo sąlygas, nustatytas jos priežiūrai pavestoms RIS;
6.3. parengdama saugumo akreditavimo strategiją, kurioje nustatytas akreditavimo tvarkos išsamumo lygis, atitinkantis reikiamą saugumo užtikrinimo lygį;
6.4. tikrindama ir patvirtindama su saugumu susijusius dokumentus, įskaitant pareiškimus dėl rizikos valdymo ir likutinės rizikos, saugumo įgyvendinimo patikrinimo dokumentus ir saugios eksploatacijos taisykles, taip pat užtikrindama, kad šie dokumentai atitiktų Parlamento saugumo taisykles ir politiką;

6.5. tikrindama su RIS susijusių saugumo priemonių įgyvendinimą vykdant saugumo įvertinimus, patikrinimus ar peržiūras arba juos finansuojant;

6.6. nustatydama saugumo reikalavimus (pavyzdžiui, susijusius su personalo patikimumo laipsniais), taikomus su RIS saugumo atžvilgiu susijusioms pareigybėms;

6.7. patvirtindama arba, jei reikia, dalyvaudama bendrame patvirtinime apie atitinkamos RIS sujungimą su kita RIS;

6.8. patvirtindama techninės įrangos, naudojamos saugiam įslaptintos informacijos tvarkymui ir apsaugai, saugumo standartus;

6.9. užtikrindama, kad Parlamente naudojamos šifravimo priemonės būtų įtrauktos į ES patvirtintų priemonių sąrašą;

6.10. konsultuodama sistemos tiekėją, saugumo srities subjektus ir vartotojų atstovus saugumo rizikos valdymo, visų pirma, likutinės rizikos ir pareiškimo dėl patvirtinimo reikalavimų ir sąlygų klausimais.

7. ISUOI atsakinga už:

7.1. saugumo dokumentų, atitinkančių saugumo politiką ir saugumo gaires, rengimą, ypač įskaitant pareiškimą dėl likutinės rizikos, saugios eksploatacijos taisykles ir šifravimo planą vykdant RIS akreditavimo procesą;

7.2. dalyvavimą atrenkant ir bandant konkrečioms sistemoms skirtas techninio saugumo priemones, prietaisus ir programinę įrangą, siekiant prižiūrėti, kaip jie taikomi, ir užtikrinti, kad jie būtų saugiai įdiegti, sukonfigūruoti ir eksploatuojami pagal atitinkamus saugumo dokumentus;

7.3. saugios eksploatacijos taisyklių įgyvendinimo ir taikymo stebėseną ir prireikus – atsakomybės už eksploatavimo saugumą delegavimą sistemos savininkui, būtent, ĮIS;

7.4. šifravimo priemonių valdymą ir tvarkymą užtikrinant šifravimo ir kontroliuojamų objektų saugojimą ir prireikus užtikrinant šifravimo kintamųjų generavimą;

7.5. saugumo analizės peržiūros ir bandymų atlikimą, visų pirma, siekiant parengti atitinkamas rizikos ataskaitas, kurių reikalauja SAI;

7.6. mokymo konkrečioms RIS skirto informacijos saugumo užtikrinimo (ISU) klausimais rengimą;

7.7. konkrečioms RIS skirtų apsaugos priemonių įgyvendinimą ir naudojimą.

8. KPLI atsako už:

8.1. ES šifravimo medžiagos valdymą ir apskaitą;

8.2. užtikrinimą, glaudžiai bendradarbiaujant su SAI, kad visos ES šifravimo medžiagos apskaitai, saugiam tvarkymui, laikymui ir platinimui būtų taikomos tinkamos procedūros ir nustatyti tinkami planai;

8.3. ES šifravimo medžiagos perdavimo ją naudojantiems asmenims ir tarnyboms arba priėmimo iš jų užtikrinimą.

9. TEI atsako už RIS atitikties TEMPEST politikai ir naudojimo nurodymams užtikrinimą. Ši institucija patvirtina TEMPEST atsakomąsias priemones, skirtas įrenginiams ir priemonėms, siekiant apsaugoti įslaptintą informaciją iki nustatyto slaptumo žymos laipsnio informacijos operacinėje aplinkoje.

10. ISUI atsako už visus konfidencialios informacijos valdymo ir tvarkymo Parlamente aspektus ir ypač už:

10.1 informacijos saugumo užtikrinimo saugumo politikos formavimą ir saugumo gairių rengimą bei jų veiksmingumo ir tinkamumo stebėseną;

10.2. su šifravimo priemonėmis susijusios techninės informacijos apsaugą ir administravimą;

10.3. užtikrinimą, kad įslaptintos informacijos apsaugai parinktos ISU priemonės atitiktų atitinkamą jų tinkamumo nustatymo ir atrankos politiką;

10.4. užtikrinimą, kad šifravimo priemonės būtų pasirenkamos laikantis jų tinkamumo nustatymo ir atrankos politikos;

10.5. konsultavimąsi su sistemos tiekėju, saugumo srities subjektais ir vartotojų atstovais ISU saugumo politikos klausimais.

II SAUGUMO PRANEŠIMAS

KONFIDENCIALIOS INFORMACIJOS VALDYMAS

A. ĮŽANGA

1. Šiuo saugumo pranešimu nustatytos Parlamento vykdomo konfidencialios informacijos valdymo nuostatos.

2. Rengėjas, rengdamas konfidencialią informaciją, įvertina konfidencialumo laipsnį ir priima sprendimą remdamasis šiuo saugumo pranešimu nustatytais principais dėl tokios informacijos žymėjimo slaptumo žymomis arba kitomis žymomis.

B. ESĮI ĮSLAPTINIMAS

3. Sprendimas įslaptinti dokumentą priimamas prieš jį rengiant. Tuo tikslu informacija nurodoma kaip ESĮI, informacijos rengėjui iš anksto įvertinus jos konfidencialumo laipsnį ir nusprendus, kad neteisėtas tokios informacijos atskleidimas galėtų tam tikru aspektu daryti poveikį Europos Sąjungos, vienos ar kelių valstybių narių arba asmenų interesams.

4. Priėmus sprendimą įslaptinti informaciją atliekamas antras išankstinis vertinimas, siekiant nustatyti tinkamą slaptumo žymos laipsnį. Dokumento įslaptinimo laipsnis nustatomas pagal dokumento turinio slaptumo laipsnį.

5. Atsakomybė už informacijos įslaptinimą tenka tik jos rengėjui. Parlamento pareigūnai informaciją įslaptina gavę generalinio sekretoriaus nurodymą arba remdamiesi jo suteiktais įgaliojimais.

6. Slaptumo žymos taikomos teisingai ir nuosaikiai. Įslaptinamo dokumento rengėjas vengia suteikti pernelyg aukštą ar pernelyg žemą slaptumo žymos laipsnį.

7. Informacijai paskirtas slaptumo žymos laipsnis nurodo apsaugos lygį, taikomą personalo patikimumo, fizinio saugumo, procedūrų saugumo ir informacijos saugumo užtikrinimo srityse.

8. Informacija, kurią reikia įslaptinti, žymima ir tvarkoma

kaip įslaptinta informacija nepriklausomai nuo jos fizinės formos. Informacijos gavėjai aiškiai informuojami apie jos įslaptinimą nurodant slaptumo žymą (jei informacija pateikiama rašytine – popieriuje arba RIS – forma) arba pateikiant pranešimą (jei informacija pateikiama žodine forma, pvz., pokalbyje arba uždarame posėdyje). Įslaptinta informacija fiziškai žymima, kad būtų galima paprastai nustatyti jos slaptumo žymą.

9. ESĮI elektronine forma rengiama tik naudojant akredituotą RIS. Pati įslaptinta informacija, rinkmenos pavadinimas ir laikmena (jei išorinė laikmena, pvz., pastoviosios atminties kompaktinis diskas arba USB atmintinė) žymimi atitinkama slaptumo žyma.

10. Informacija įslaptinama, kai tik įgauna formą. Pavyzdžiui, asmeninius užrašus, projektus arba el. pašto pranešimus, kuriuose yra informacijos, kurią reikia įslaptinti, iš pat pradžių reikia pažymėti kaip ESĮI. Tokia informacija rengiama ir tvarkoma pagal šį sprendimą ir jo nurodymus dėl fizinių ir techninių aspektų. Tokią informaciją galima naudoti oficialiame dokumente, kuris atitinkamai pažymimas ir tvarkomas. Rengiant oficialų dokumentą gali prireikti iš naujo jį įvertinti ir priskirti jam aukštesnį ar žemesnį už pradinį slaptumo žymos laipsnį.

11. Rengėjas gali nuspręsti skirti standartinį slaptumo žymos laipsnį tų kategorijų informacijai, kurią nuolat rengia. Tačiau rengėjas užtikrina, kad tokiu atveju atskiroms informacijos dalims jis sistemingai neskirs pernelyg aukšto arba pernelyg žemo slaptumo žymos laipsnio.

12. ESĮI visuomet žymima slaptumo žyma, atitinkančia jos slaptumo žymos laipsnį.

B.1. *Slaptumo žymų laipsniai*

13. ESĮI skiriamas vienas iš šių slaptumo žymų laipsnių:

– TRÈS SECRET UE/EU TOP SECRET, kaip apibrėžta šio sprendimo 2 straipsnio d punkte, jei neteisėtas tokios informacijos atskleidimas gali:

a) kelti tiesioginę grėsmę Europos Sąjungos, vienos ar kelių valstybių narių, trečiųjų valstybių arba tarptautinių organizacijų vidaus stabilumui;

b) daryti nepaprastai didelę žalą santykiams su trečiosiomis valstybėmis arba tarptautinėmis organizacijomis;

c) tiesiogiai lemti daugelio asmenų mirtį;

d) nepaprastai smarkiai pakenkti valstybių narių arba kitų partnerių dislokuotų darbuotojų veiklos veiksmingumui arba saugumui, arba ypač svarbių saugumo ar žvalgybos operacijų nuolatiniam veiksmingumui;

e) daryti didelę ilgalaikę žalą Europos Sąjungos arba valstybių narių ekonomikai;

– SECRET UE/EU SECRET, kaip apibrėžta šio sprendimo 2 straipsnio d punkte, jei neteisėtas tokios informacijos atskleidimas gali:

a) sukelti didelę tarptautinę įtampą;

b) padaryti didelę žalą santykiams su trečiosiomis valstybėmis ir tarptautinėmis organizacijomis;

c) sukelti tiesioginę arba didelę žalą viešajam ar asmenų saugumui arba laisvei;

d) kenkti svarbioms prekybos arba politinėms deryboms, taip sukeliant didelių veiklos sunkumų Europos Sąjungai arba valstybėms narėms;

e) stipriai kenkti valstybių narių veiklos saugumui arba ypač svarbių saugumo arba žvalgybos operacijų veiksmingumui;

f) daryti didelę materialinę žalą Europos Sąjungos arba valstybių narių finansiniams, pinigų politikos, ekonominiams ir prekybos interesams;

g) iš esmės pakenkti pagrindinių organizacijų arba partnerių finansiniam gyvybingumui;

h) stipriai trukdyti kurti Europos Sąjungos politiką arba ją vykdyti, taip sukeliant dideles ekonomines, prekybos arba finansines pasekmes;

– CONFIDENTIEL UE/EU CONFIDENTIAL, kaip apibrėžta šio sprendimo 2 straipsnio d punkte, jei neteisėtas tokios informacijos atskleidimas gali:

a) daryti didelę žalą diplomatiniams santykiams, jei tokie veiksmai sukeltų oficialų protestą arba kitas sankcijas;

b) kelti grėsmę asmens saugumui arba laisvei;

c) kelti didelę grėsmę prekybos arba politikos deryboms, taip sukeliant didelių veiklos sunkumų Europos Sąjungai arba valstybėms narėms;

d) kenkti valstybių narių veiklos saugumui arba ypač svarbių saugumo arba žvalgybos operacijų veiksmingumui;

e) iš esmės pakenkti pagrindinių organizacijų arba partnerių finansiniam gyvybingumui;

f) trukdyti tirti nusikaltimą ar terorizmo veiklą arba sudaryti palankesnes sąlygas įvykdyti nusikaltimą ar užsiimti tokia veikla;

g) atlikti esminius veiksmus, nukreiptus prieš Europos Sąjungos ar valstybių narių finansinius, pinigų politikos, ekonominius ar prekybos interesus;

h) stipriai trukdyti kurti Europos Sąjungos politiką arba ją vykdyti, sukeliant dideles ekonomines, prekybos arba finansines pasekmes;

– RESTREINT UE/EU RESTRICTED, kaip apibrėžta šio sprendimo 2 straipsnio d punkte, jei neteisėtas tokios informacijos atskleidimas gali:

a) būti nenaudingas bendriems Europos Sąjungoms interesams,

b) daryti neigiamą įtaką diplomatiniams santykiams;

c) labai pakenkti asmenims arba įmonėms;

d) būti nenaudingas Europos Sąjungai arba valstybėms narėms prekybos arba politikos derybose;

e) apsunkinti pastangas veiksmingai išlaikyti veiksmingą saugumą Europos Sąjungoje arba valstybėse narėse;

f) trukdyti veiksmingai kurti Europos Sąjungos politiką arba ją vykdyti;

g) trukdyti tinkamam Europos Sąjungos ir jos politikos administravimui;

h) pažeisti Parlamento įsipareigojimus išlaikyti trečiųjų šalių suteiktos informacijos įslaptinimo statusą;

i) pažeisti teisės aktais nustatytus informacijos atskleidimo apribojimus;

j) asmenims arba įmonėms padaryti finansinių nuostolių arba sudaryti palankesnes sąlygas jiems neteisėtai pasipelnyti ar įgyti pranašumo;

k) pakenkti tyrimui arba sudaryti palankesnes sąlygas nusikaltimui padaryti.

B.2. *Rinkinių, antraštinių puslapių ir ištraukų įslaptinimas*

14. Pridedamų dokumentų lydraščių arba pranešimų slaptumo žymos laipsnis atitinka priedų aukščiausio laipsnio slaptumo žymų laipsnį. Jei pranešimas arba lydraštis pateikiami atskirai nuo priedų, rengėjas aiškiai nurodo, koks slaptumo žymos laipsnis jiems suteikiamas. Jei nereikia įslaptinti pridedamo pranešimo (lydraščio), jame pateikiamas toks galutinis tekstas: „Šis pridedamas pranešimas (lydraštis) yra neįslaptintas, jei pateikiamas atskirai nuo priedų“.

15. Reikia sukurti tokią dokumentų arba rinkmenų, kurių dalys pažymėtos skirtingais slaptumo žymų laipsniais, struktūrą, kad būtų galima kuo paprasčiau nustatyti dalis, pažymėtas skirtingais slaptumo žymų laipsniais, ir prireikus jas atskirti. Dokumento ar dokumentų bylos bendras slaptumo žymos laipsnis atitinka aukščiausią slaptumo žymos laipsnį turinčią jo dalį.

16. Prireikus atitinkamo dokumento atskiriems lapams, dalims, skyriams, priedams, priedėliams ir pridedamiems dokumentams suteikti skirtingus slaptumo žymų laipsnius, jie yra atitinkamai įslaptinami. Dokumentuose, kuriuose yra ESĮI, galima naudoti standartines santrumpas, kuriomis nurodomas teksto skirsnių arba dalių, užimančių mažiau nei vieną puslapį, slaptumo žymos laipsnis.

17. Renkant informaciją iš įvairių šaltinių, galutinis dokumentas peržiūrimas siekiant nustatyti jo bendrą slaptumo žymos laipsnį, nes gali paaiškėti, kad jam turi būti suteiktas aukštesnis slaptumo žymos laipsnis nei jo sudėtinėms dalims.

C. KITA KONFIDENCIALI INFORMACIJA

18. Kita konfidenciali informacija žymima pagal šio saugumo pranešimo E punktą ir naudojimo nurodymus.

D. KONFIDENCIALIOS INFORMACIJOS RENGIMAS

19. Konfidencialią informaciją gali rengti tik tie asmenys, kuriems šiuo sprendimu suteikiama teisė tai daryti arba kuriems tokį leidimą suteikė SI.

20. Konfidenciali informacija neįkeliama į interneto arba intraneto dokumentų valdymo sistemas.

D.1. *ESĮI rengimas*

21. Siekiant rengti ESĮI, kuri žymima slaptumo žymų CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ar TRÈS SECRET UE/EU TOP SECRET laipsniais, atitinkamam asmeniui suteikiama teisė rengti tokią informaciją remiantis šiuo sprendimu arba toks asmuo pirmiausia turi gauti leidimą pagal šio sprendimo 4 straipsnio 1 dalį.

22. Slaptumo žymų CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ar TRÈS SECRET UE/EU TOP SECRET laipsniais žymima ESĮI rengiama tik saugioje zonoje.

23. ESĮI rengimui taikomos šios taisyklės:

a) kiekviename puslapyje aiškiai nurodomas atitinkamas slaptumo žymos laipsnis;
b) kiekvienas puslapis sunumeruojamas ir nurodomas bendras puslapių skaičius;
c) dokumento pirmame puslapyje nurodomas jo numeris ir dalykas, kurie nėra įslaptinta informacija, išskyrus tuos atvejus, kai jie pažymėti kaip įslaptinta informacija;
d) dokumento pirmame puslapyje nurodoma data;
e) bet kokio dokumento, pažymėto slaptumo žymų CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ar TRÈS SECRET UE/EU TOP SECRET laipsniais, pirmame puslapyje nurodomas visų priedų ir pridedamų dokumentų sąrašas;

f) jei platinamos kelios dokumentų, pažymėtų slaptumo žymų CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ar TRÈS SECRET UE/EU TOP SECRET laipsniais, kopijos, kiekvienos iš jų kiekviename puslapyje nurodomas kopijos numeris. Kiekvienos kopijos pirmame puslapyje taip pat nurodomas bendras kopijų ir puslapių skaičius;
g) jei dokumente pateikiamos nuorodos į iš kitų Europos Sąjungos institucijų gautus kitus dokumentus, kuriuose yra įslaptintos informacijos, arba jei dokumente yra šių dokumentų įslaptintos informacijos, dokumentas žymimas tokio paties laipsnio slaptumo žyma, kokia pažymėti šie dokumentai, ir be išankstinio raštiško jų rengėjo sutikimo negali būti platinami kitiems asmenims, kurių vardai ir pavardės nenurodytos originalaus dokumento arba dokumentų, kuriuose yra įslaptintos informacijos, platinimo sąraše.

24. Rengėjas vykdo ESĮI, kurią parengė, kontrolę. Prašoma suteikti išankstinį raštišką rengėjo sutikimą prieš:
a) sumažinant ESĮI slaptumo žymos laipsnį arba informaciją išslaptinant;
b) naudojant ESĮI kitiems, nei nustatė rengėjas, tikslams;
c) atskleidžiant ESĮI bet kokiai trečiajai valstybei arba tarptautinei organizacijai;
d) atskleidžiant ESĮI bet kokiam asmeniui, institucijai, šaliai arba tarptautinei organizacijai, kurie nenurodyti tarp gavėjų, kuriems rengėjas suteikė leidimą susipažinti su minima informacija;
e) atskleidžiant ESĮI rangovui arba numatomam rangovui, kuris yra trečiojoje valstybėje;
f) kopijuojant arba verčiant ESĮI, jeigu ji pažymėta slaptumo žymos TRES SECRET UE/EU TOP SECRET laipsniu;
g) sunaikinant ESĮI.

D.2. *Kitos konfidencialios informacijos rengimas*

25. Generalinis sekretorius, kaip SI, gali nuspręsti, ar suteikti leidimą rengti kitą konfidencialią informaciją atitinkamai pareigybei, tarnybai ir (arba) asmeniui.

26. Kita konfidenciali informacija žymima viena iš naudojimo nurodymuose nurodytų žymų.

27. Kitos konfidencialios informacijos rengimui taikomos šios taisyklės:

a) jos žymos nurodomos dokumento pirmo puslapio viršuje;
b) kiekvienas puslapis sunumeruojamas ir nurodomas bendras puslapių skaičius;
c) dokumento pirmame puslapyje nurodomas jo numeris ir dalykas;
d) dokumento pirmame puslapyje nurodoma data;
e) paskutiniame dokumento puslapyje pateikiamas visų priedų ir pridedamųjų dokumentų sąrašas.

28. Kitos konfidencialios informacijos rengimui taikomos naudojimo nurodymuose nustatytos specialios taisyklės ir tvarka.

E. SLAPTUMO ŽYMOS GALIOJIMO ŽYMOS IR KITOS ŽYMOS

29. Slaptumo žymų galiojimo žymos ir kitos žymos dokumentuose yra skirtos informacijos srautui kontroliuoti ir teisei susipažinti su konfidencialia informacija apriboti remiantis principu „būtina žinoti“.

30. Naudojant arba nurodant slaptumo žymų galiojimo žymas arba kitas žymas, būtina imtis veiksmų, kad jos nebūtų painiojamos su ESĮI žymėti naudojamomis slaptumo žymomis RESTREINT UE /EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET, TRES SECRET UE/EU TOP SECRET.

31. Naudojimo nurodymuose nustatomos specialios taisyklės dėl slaptumo žymų arba galiojimo žymos ir kitų žymų naudojimo, taip pat nustatomas patvirtintų Europos Parlamento slaptumo žymų sąrašas.

E.1. *Slaptumo žymos galiojimo žymos*

32. Slaptumo žymos galiojimo žymos gali būti naudojamos tik kartu su slaptumo žyma ir netaikomos atskirai dokumentams. Slaptumo žymos galiojimo žyma gali būti taikoma ESĮI siekiant:
a) nustatyti slaptumo žymos galiojimo terminus (įslaptintos informacijos, kuriai taikomas automatinis slaptumo laipsnio sumažinimas arba išslaptinimas, atveju);
b) riboti ESĮI platinimą;
c) nustatyti konkrečias papildomas tvarkymo priemones, kurios atitinka slaptumo žymos laipsnį.

33. Dokumentų, kuriuose yra ESĮI, tvarkymui ir laikymui taikoma papildoma kontrolė lemia papildomą naštą visiems susijusiems subjektams. Siekiant sumažinti šiuo atveju reikalingą darbą, rengiant tokį dokumentą

geroji patirtis yra nustatyti terminą arba įvykį, po kurio automatiškai nustoja galioti slaptumo žyma ir sumažinamas šiame dokumente pateiktos informacijos slaptumo žymos laipsnis arba informacija išslaptinama.

34. Jei dokumento sritis yra konkreti darbo sritis ir reikia apriboti dokumento platinimą ir (arba) taikyti jam konkrečias tvarkymo priemones, prie slaptumo žymos galima pridėti pareiškimą, kad būtų galima nustatyti dokumento tikslinę auditoriją.

E.2. *Kitos žymos*

35. Kitos žymos nėra slaptumo žymos. Kitos žymos naudojamos tik siekiant suteikti konkrečius nurodymus dėl dokumento tvarkymo ir nenaudojamos tokio dokumento turiniui aprašyti.

36. Kitos žymos gali būti naudojamos atskirai nuo dokumentų arba naudojamos kartu su slaptumo žyma.

37. Kitos žymos paprastai naudojamos informacijai, kuriai taikoma profesinė paslaptis, nurodyta SESV 339 straipsnyje ir Tarnybos nuostatų 17 straipsnyje, žymėti arba kurią Parlamentas turi apsaugoti dėl teisinių priežasčių, tačiau kurios nereikia arba negalima įslaptinti.

E.3. *Kitų žymų naudojimas RIS*

38. Kitų žymų naudojimo taisyklės taip pat taikomos akredituotoje RIS.

39. SAI nustato konkrečias kitų žymų akredituotoje RIS naudojimo taisykles.

F. INFORMACIJOS PRIĖMIMAS

40. Tik ĮIS turi teisę Parlamente iš trečiųjų šalių priimti slaptumo žymų CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ar TRÈS SECRET UE/EU TOP SECRET laipsniais arba jiems lygiaverčiais pažymėtą informaciją.

41. Jei informacija pažymėta slaptumo žymos RESTREINT UE/EU RESTRICTED ar jam lygiaverčiu laipsniu arba jei tai yra kita konfidenciali informacija, tiek ĮIS, tiek kompetentingas Parlamento organas ir (arba) atitinkamas pareigas einantis asmuo gali priimti šią informaciją iš trečiųjų šalių ir yra atsakingas už šiuo saugumo pranešimu nustatytų principų taikymą.

G. REGISTRAVIMAS

42. Registravimas – procedūrų, kuriomis naudojantis registruojamas konfidencialios informacijos gyvavimo ciklas, įskaitant jos platinimą, sunaikinimą ir susipažinimą su ja, taikymas.

43. Šiame saugumo pranešime registracijos knyga yra registras, kuriame registruojama data ir laikas, kai konfidenciali informacija:

a) patenka į atitinkamą Parlamento organo ir (arba) atitinkamas pareigas einančio asmens sekretoriatą ar ĮIS arba išsiunčiama (išgabenama);
b) kai su ja susipažįsta asmuo, kurio patikimumas patikrintas, arba kuriam ji persiunčiama;
c) sunaikinama.

44. Įslaptintos informacijos rengėjas atsakingas už pradinio pareiškimo žymėjimą, kai parengiamas dokumentas, kuriame yra tokios informacijos. Rengiant šį dokumentą ĮIS pranešama apie tą pareiškimą.

45. Slaptumo žyma CONFIDENTIEL UE/EU CONFIDENTIAL, aukštesnio laipsnio arba lygiaverte žyma pažymėtą informaciją dėl saugumo gali registruoti tik ĮIS. Iš trečiųjų šalių gautą slaptumo žyma RESTREINT UE/EU RESTRICTED arba lygiaverte žyma pažymėtą informaciją ar kitą konfidencialią informaciją administraciniais tikslais registruoja už oficialų dokumento priėmimą atsakinga tarnyba, kuri yra ĮIS, Parlamento organo arba atitinkamas pareigas einančio asmens sekretoriatas. Parlamente parengtą kitą konfidencialią informaciją administraciniais tikslais registruoja rengėjas.

46. Slaptumo žymos CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ar TRÈS SECRET UE/EU TOP SECRET laipsniu arba jam lygiaverčiu žymima informacija, visų pirma, registruojama, kai:

a) informacija rengiama;
b) informacija patenka į ĮIS ar iš jo išsiunčiama (išgabenama);
c) informacija patenka į RIS ar iš jos išsiunčiama.

47. Slaptumo žymos CONFIDENTIEL UE/EU CONFIDENTIAL laipsniu arba jam lygiaverčiu žymima informacija visų pirma registruojama, kai:

a) informacija rengiama;
b) informacija patenka atitinkamam Parlamento organo ir (arba) atitinkamas pareigas einančio asmens sekretoriatui arba ĮIS ar iš jų išsiunčiama (išgabenama);

c) informacija patenka į RIS ar iš jos išsiunčiama.

48. Konfidenciali informacija gali būti registruojama popierinėse arba elektroninėse registracijos knygose arba RIS.

49. Jei informacija žymima slaptumo žymos RESTREINT UE/EU RESTRICTED laipsniu ar jam lygiaverčiu arba jei ji yra kita konfidenciali informacija, registruojami bent šie duomenys:

a) data ir laikas, kai informacija patenka atitinkamam Parlamento organo ir (arba) atitinkamas pareigas einančio asmens sekretoriatui arba ĮIS ar iš jų išsiunčiama (išgabenama);
b) dokumento pavadinimas, įslaptinimo laipsnis arba kita žyma, įslaptinimo (arba kitos žymos) galiojimo pabaigos data ir dokumentui priskirti visi numeriai.

50. Jei informacija žymima slaptumo žymos CONFIDENTIEL UE /EU CONFIDENTIAL, SECRET UE/EU SECRET ar TRÈS SECRET UE/EU TOP SECRET laipsniu arba jam lygiaverčiu, registruojami bent šie duomenys:

a) data ir laikas, kai informacija patenka ĮIS arba yra iš jo išsiunčiama (išgabenama);
b) dokumento pavadinimas, įslaptinimo laipsnis arba kita žyma, dokumentui priskirti visi numeriai ir įslaptinimo (arba kitos žymos) galiojimo pabaigos data;
c) rengėjo rekvizitai;
d) įrašas apie asmens tapatybę, kuriam suteikta teisė susipažinti su dokumentu, ir data, kada tam asmeniui buvo leista su ja susipažinti;
e) įrašas apie padarytas dokumento kopijas arba vertimus;
f) data ir laikas, kada ĮIS išsiunčia (išgabena) arba gauna dokumento kopijas arba vertimus, ir informacija apie tai, kam jie buvo siųsti ir kas juos grąžino;
g) data ir laikas, kai dokumentas sunaikintas, ir duomenys apie tai, kas jį sunaikino, laikantis sunaikinimą reglamentuojančių Parlamento saugumo taisyklių;
h) duomenys apie dokumento išslaptinimą arba slaptumo laipsnio sumažinimą.

51. Atitinkamai įslaptinamos arba žymimos registracijos knygos. Registruojamoms informacijai skirtoms registracijos knygoms, pažymėtoms slaptumo žymos laipsniu TRES SECRET UE/EU TOP SECRET arba jam lygiaverčiu, suteikiama tokio paties laipsnio žyma.

52. Įslaptinta informacija gali būti registruojama:

a) vienoje registracijos knygoje;

b) atskirose registracijos knygose pagal informacijos slaptumo žymos laipsnį, pagal tai, ar informacija gaunama ar išsiunčiama, ir pagal tai, iš kur ji gauta ar kur išsiunčiama.

53. Jei informacija tvarkoma elektroniniu būdu RIS, registravimo procedūros gali būti atliekamos pasitelkiant tas RIS priemones, kurios atitinka minėtiems reikalavimams lygiaverčius reikalavimus. Kai ESĮI išsiunčiama iš RIS, taikoma nurodyta registravimo procedūra.

54. ĮIS registruoja visą įslaptintą informaciją, kurią Parlamentas suteikė trečiosioms šalims, ir iš trečiųjų šalių Parlamento gautą įslaptintą informaciją.

55. Užregistravus slaptumo žymos CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ar TRÈS SECRET UE/EU TOP SECRET laipsniu arba jam lygiaverčiu žymimą informaciją, ĮIS patikrina, ar gavėjas turi galiojantį saugumo leidimą. Jei toks leidimą turi, ĮIS informuoja gavėją. Susipažinti su įslaptinta informacija galima tik tuomet, kai užregistruojamas dokumentas, kuriame yra tokios informacijos.

H. PLATINIMAS

56. Rengėjas sudaro pradinę ESĮS, kurį parengė, platinimo sąrašą.

57. Slaptumo žymos RESTREINT UE/EU RESTRICTED laipsniu žymima informacija arba kita konfidenciali informacija, kurią parengė Parlamentas, rengėjo platinama Parlamente, laikantis atitinkamų naudojimo nurodymų ir pagal principą „būtina žinoti“. Jei informacija, žymima slaptumo žymos CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ar TRÈS SECRET UE/EU TOP SECRET laipsniu, yra parengta Parlamento saugioje zonoje, platinimo sąrašas (ir kiti nurodymai dėl platinimo) pateikiamas ĮIS, kuris yra atsakingas už šio sąrašo tvarkymą.

58. Parlamento parengtą ESĮI platinti trečiosioms šalims gali tik ĮIS pagal principą „būtina žinoti“.

59. Konfidenciali informacija, kurią gavo IĮS, bet koks Parlamento organas arba pareigas einantis asmuo, pateikęs atitinkamą prašymą, platinama laikantis informacijos rengėjo pateiktų nurodymų.

I. TVARKYMAS, LAIKYMAS IR SUSIPAŽINIMAS

60. Konfidenciali informacija tvarkoma, laikoma ir su ja susipažįstama laikantis IV saugumo pranešimo nuostatų ir naudojimo nurodymų.

J. ĮSLAPTINTOS INFORMACIJOS KOPIJAVIMAS, VERTIMAS RAŠTU IR ŽODŽIU

61. Dokumentai, kuriuose yra slaptumo žymos TRES SECRET UE/EU TOP SECRET arba jam lygiaverčiu laipsniu žymimos informacijos, kopijuojami arba verčiami tik gavus išankstinį raštišką informacijos rengėjo sutikimą. Dokumentai, kuriuose yra slaptumo žymos SECRET UE/EU SECRET arba jam lygiaverčiu laipsniu, arba slaptumo žymos CONFIDENTIEL UE/EU CONFIDENTIAL arba jam lygiaverčiu laipsniu žymimos informacijos, gali būti kopijuojami arba verčiami gavus turėtojo nurodymą, jeigu rengėjas neuždraudė to daryti.

62. Kiekviena dokumento, kuriame yra slaptumo žymos TRES SECRET UE/EU TOP SECRET, SECRET UE/EU SECRET EU arba CONFIDENTIEL UE/EU CONFIDENTIAL arba jam lygiaverčiu laipsniu žymimos informacijos, kopija dėl saugumo registruojama.

63. Dokumento kopijoms ir vertimams taikomos tos pačios saugumo priemonės, kaip ir dokumento, kuriame yra įslaptintos informacijos, originalui.

64. Iš Tarybos gaunami dokumentai turėtų būti parengti visomis oficialiomis kalbomis.

65. Rengėjas arba kopijos turėtojas gali paprašyti pateikti dokumento, kuriame yra įslaptintos informacijos, kopijas ir (arba) vertimus. Dokumentus, kuriuose yra slaptumo žymos CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ar TRÈS SECRET UE/EU TOP SECRET arba jam lygiaverčiu laipsniu žymimos informacijos, galima kopijuoti tik saugioje zonoje naudojantis kopijavimo aparatais, kurie priklauso akredituotai RIS. Dokumentai, kuriuose yra slaptumo žyma RESTREINT UE/EU RESTRICTED arba lygiaverte žyma žymimos informacijos, arba kitos konfidencialios informacijos, kopijuojami naudojantis akredituotais atgaminimo įrenginiais Parlamento patalpose.

66. Visos bet kokių dokumentų arba dokumentų dalių, kuriose yra įslaptintos informacijos, kopijos ir visi vertimai atitinkamai žymimi, sunumeruojami ir registruojami.

67. Nedaroma daugiau kopijų, nei būtinai reikia. Susipažinimo su informacija laikotarpio pabaigoje visos kopijos sunaikinamos laikantis naudojimo nurodymų.

68. Tik vertėjai žodžiu ir raštu, kurie yra Parlamento pareigūnai, gauna prieigą prie įslaptintos informacijos.

69. Prieigą prie dokumentų, kuriuose yra slaptumo žymos CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ar TRÈS SECRET UE/EU TOP SECRET arba jam lygiaverčiu laipsniu žymimos informacijos, turintys vertėjai žodžiu ir raštu yra atitinkamai tikrinami dėl patikimumo.

70. Vertėjai žodžiu ir raštu, dirbdami su dokumentais, kuriuose yra slaptumo žymos CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ar TRÈS SECRET UE/EU TOP SECRET arba jam lygiaverčiu laipsniu žymimos informacijos, dirba saugioje zonoje.

K. KONFIDENCIALIOS INFORMACIJOS SLAPTUMO ŽYMOS ARBA KITOS ŽYMOS LAIPSNIO SUMAŽINIMAS IR KONFIDENCIALIOS INFORMACIJOS IŠSLAPTINIMAS

K.1. *Bendrieji principai*

71. Konfidenciali informacija išslaptinama, sumažinamas jos slaptumo žymos ar kitos žymos laipsnis, jei nebereikia ilgiau apsaugoti šios informacijos arba jei nebereikia šios informacijos saugoti pirminiu lygiu.

72. Sprendimus dėl informacijos, esančios Parlamente parengtuose dokumentuose, slaptumo žymos ar kitos žymos laipsnio sumažinimo, informacijos išslaptinimo gali prireikti priimti ir pagal principą ad hoc, pvz., nagrinėjant viešosios arba Europos Sąjungos kitos institucijos prašymą leisti susipažinti su informacija, arba pareiškus iniciatyvą ĮIS, Parlamento organui ir (arba) atitinkamas pareigas einančiam asmeniui.

73. ESĮI rengėjas, rengdamas informaciją, jei įmanoma, nurodo, ar tam tikrą dieną arba po tam tikro įvykio galima sumažinti atitinkamos ESĮI slaptumo žymos laipsnį arba išslaptinti šią informaciją. Jei to nurodyti neįmanoma, informaciją turintis rengėjas, ĮIS, Parlamento organas ir (arba) atitinkamas pareigas einantis asmuo peržiūri ESĮI slaptumo žymos laipsnį bent kas penkerius metus. Bet kokiu atveju galima sumažin-

ti ESĮI slaptumo žymos laipsnį arba išslaptinti šią informaciją tik gavus išankstinį rašytinį informacijos rengėjo sutikimą.

74. Jei negalima nustatyti arba atsekti dokumentų, kurie parengti Parlamente, rengėjo SI peržiūri ESĮI slaptumo žymos laipsnį remdamasi informaciją turinčio Parlamento organo ir (arba) atitinkamas pareigas einančio asmens pasiūlymu, kuris šiuo klausimu gali pasikonsultuoti su ĮIS.

75. Informaciją turintis ĮIS, Parlamento organas ir (arba) atitinkamas pareigas einantis asmuo atsakingas už gavėjo (-ų) informavimą apie informacijos slaptumo žymos laipsnio sumažinimą arba informacijos išslaptinimą, o šis (-ie) gavėjas (-ai) atsako už kito (-ų) gavėjo (-ų), kuriam (-iems) nusiuntė arba kopijavo dokumentą, informavimą.

76. Registruojamas dokumente esančios informacijos išslaptinimas, slaptumo žymos arba kitos žymos laipsnio sumažinimas.

K.2. *Išslaptinimas*

77. ESĮI galima išslaptinti visą arba tik jos dalį. Gali būti išslaptinama ESĮI dalis, jei manoma, kad nebereikia ilgiau apsaugoti tam tikros dokumento dalies, kurioje yra šios informacijos, tačiau manoma, kad pagrįsta toliau apsaugoti likusią dokumento dalį.

78. Jei peržiūrint ESĮI, kuri yra Parlamente parengtame dokumente, nusprendžiama išslaptinti šią informaciją, atsižvelgiama į tai, ar dokumentą galima skelbti viešai, ar reikia jį pažymėti platinimo žyma (t. y., dokumentas neviešinamas).

79. Išslaptinus ESĮI, tai turi būti užfiksuojama registracijos knygoje nurodant šiuos duomenis: išslaptinimo datą, prašymą išslaptinti pateikusio asmens ir leidimą davusio asmens vardus ir pavardes, išslaptinto dokumento numerį ir jo galutinį gavėją.

80. Senos slaptumo žymos išslaptintame dokumente ir visose jo kopijose turi būti perbraukiamos. Dokumentai ir visos jų kopijos atitinkamai laikomi.

81. Išslaptinus dalį įslaptintos informacijos, parengiamas ir atitinkamai laikomas išslaptintos dalies išrašas. Kompetentinga tarnyba registruoja:

a) dalinio išslaptinimo datą;
b) asmenų, kurie pateikė prašymą išslaptinti informaciją, ir kurie suteikė leidimą, vardus ir pavardes;
c) išslaptinto išrašo numerį.

K.3. *Slaptumo žymos laipsnio sumažinimas*

82. Sumažinus įslaptintos informacijos slaptumo žymos laipsnį, dokumentas, kuriame ji yra, registruojamas registracijos knygose pagal seną ir naują slaptumo žymos laipsnį. Registruojama slaptumo žymos laipsnio sumažinimo data ir slaptumo žymos laipsnį sumažinti leidusio asmens vardas ir pavardė.

83. Dokumentui, kuriame yra informacijos, kurios slaptumo žymos laipsnis sumažintas, ir visoms jo kopijoms suteikiamas kitas slaptumo žymos laipsnis. Šis dokumentas ir visos jo kopijos atitinkamai laikomi.

L. KONFIDENCIALIOS INFORMACIJOS SUNAIKINIMAS

84. Konfidenciali informacija (spausdintine arba elektronine forma), kurios nebereikia, sunaikinama arba ištrinama laikantis naudojimo nurodymų ir atitinkamų archyvavimo taisyklių.

85. Slaptumo žymos TRES SECRET UE/EU TOP SECRET laipsniui lygiaverte žyma, slaptumo žyma SECRET UE/EU SECRET arba lygiaverte žyma žymimą informaciją sunaikina ĮIS, dalyvaujant asmeniui, kurio patikimumas patikrintas atitinkamai pagal žemiausią sunaikinamos informacijos slaptumo žymos laipsnį.

86. Slaptumo žymos TRES SECRET UE/EU TOP SECRET laipsniu arba lygiaverte žyma pažymėti dokumentai sunaikinami tik gavus išankstinį rašytinį dokumento rengėjo sutikimą.

87. Slaptumo žymos CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ar TRÈS SECRET UE/EU TOP SECRET arba jam lygiaverčiu laipsniu žymimą informaciją sunaikina ir šalina ĮIS, gavęs informacijos rengėjo arba kompetentingos institucijos nurodymą. Registracijos knygos ir kiti registrai atitinkamai atnaujinami. Slaptumo žymos RESTREINT UE/EU RESTRICTED arba jam lygiaverčiu laipsniu pažymėtą informaciją sunaikina ir šalina ĮIS, atitinkamas Parlamento organas arba pareigas einantis asmuo.

88. Už sunaikinimą atsakingas pareigūnas ir asmuo, esantis sunaikinimo liudininku, pasirašo sunaikinimo aktą, kuris registruojamas ir saugomas archyve ĮIS. ĮIS saugo slaptumo žymos TRES SECRET UE/EU TOP SECRET arba jam lygiaverčiu laipsniu pažymėtos informacijos sunaikinimo aktus kartu su platinimo formomis bent dešimt metų, o jei in-

formacija pažymėta SECRET UE/EU SECRET arba lygiaverte žyma, slaptumo žymos CONFIDENTIEL UE/EU CONFIDENTIAL arba jam lygiaverčiu laipsniu, – bent penkerius metus.

89. Dokumentas, kuriame yra įslaptintos informacijos, sunaikinamas naudojant atitinkamus Europos Sąjungos standartus arba jiems lygiaverčius standartus atitinkančius metodus, kad nebūtų galima atkurti visos šios informacijos arba jos dalies.

90. Įslaptintai informacijai saugoti naudotos kompiuterinių duomenų saugojimo laikmenos sunaikinamos laikantis atitinkamų naudojimo nurodymų.

91. Informacija apie įslaptintos informacijos sunaikinimą registruojama atitinkamoje registracijos knygoje nurodant šiuos duomenis:

a) sunaikinimo datą ir laiką;

b) už sunaikinimą atsakingo pareigūno vardą ir pavardę;

c) sunaikinto dokumento arba kopijų identifikacinį numerį;

d) pirminę sunaikintos ESĮI fizinę formą;

e) sunaikinimo priemonę;

f) sunaikinimo vietą.

M. ARCHYVAVIMAS

92. Įslaptinta informacija, įskaitant pridedamą pranešimą (lydraštį), priedus, pateikimo kvitą ir (ar) kitas rinkinio dalis, perduodama saugioje zonoje esančiam saugiam archyvui per šešis mėnesius nuo paskutinės susipažinimo su informacija datos, o vėliausiai – per vienerius metus nuo informacijos pateikimo. Išsamios įslaptintos informacijos archyvavimo taisyklės nustatomos naudojimo nurodymuose.

93. Kitos konfidencialios informacijos atveju bendrosios dokumento naudojimo taisyklės taikomos nedarant poveikio kitoms taisyklėms dėl dokumento tvarkymo.

III SAUGUMO PRANEŠIMAS

KONFIDENCIALIOS INFORMACIJOS TVARKYMAS NAUDOJANT AUTOMATINES RYŠIŲ INFORMACINES SISTEMAS (RIS)

A. INFORMACINĖSE SISTEMOSE TVARKOMOS ĮSLAPTINTOS INFORMACIJOS SAUGUMO UŽTIKRINIMAS

1. Informacijos saugumo užtikrinimas (ISU) informacinių sistemų srityje – užtikrinimas, kad tokiose sistemose tvarkoma įslaptinta informacija bus apsaugota ir kad, valdant teisėtiems naudotojams, jos veiks taip, kaip turi veikti, ir tada, kada turi veikti. Veiksmingas ISU užtikrina tinkamą konfidencialumo, vientisumo, prieinamumo, atsakomybės už veiksmus prisiėmimo ir autentiškumo lygį. ISU grindžiamas rizikos valdymo procesu.

2. Ryšių informacinė sistema (RIS), skirta įslaptintos informacijos tvarkymui, – sistema, sudaranti sąlygas tvarkyti informaciją elektroniniu būdu. Tokia informacinė sistema apima visas sistemos dalis, kurių reikia jos veikimui, įskaitant infrastruktūrą, organizavimą, personalą ir informacijos šaltinius.

3. Įslaptinta informacija pagal RIS tvarkoma laikantis ISU principo.

4. Visa RIS akredituojama. Akreditavimo tikslas – užtikrinti, kad įgyvendintos visos atitinkamos saugumo priemonės ir kad pasiektas pakankamas įslaptintos informacijos ir RIS apsaugos lygis, vadovaujantis šiuo saugumo pranešimu. Pareiškime dėl akreditavimo nurodomas aukščiausias informacijos, kuri gali būti tvarkoma RIS, slaptumo žymos laipsnis ir atitinkami reikalavimai bei sąlygos.

5. Toliau išdėstytos ISU savybės ir sąvokos yra būtinos saugumui ir tinkamam RIS operacijų vykdymui užtikrinti:

a) autentiškumas – užtikrinimas, kad informacija yra tikra ir kad ji gauta iš *bona fide* šaltinių;
b) prieinamumas – galimybė leidimą turinčiam subjektui pateikus prašymą gauti informaciją ir ja naudotis;

c) konfidencialumas – savybė, kuri reiškia, kad informacija nėra atskleidžiama neturintiems leidimo asmenims, subjektams ar procesams;
d) vientisumas – savybė, kuri reiškia, kad apsaugomas informacijos tikslumas ir išsamumas bei turtas;
e) atsakomybės už veiksmus prisiėmimas – galimybė įrodyti, kad veiksmas buvo atliktas ar įvykis įvyko, kad šio įvykio ar veiksmo po to negalima būtų išsižadėti.

B. INFORMACIJOS SAUGUMO UŽTIKRINIMO PRINCIPAI

6. Toliau išdėstytos nuostatos yra RIS, kurioje tvarkoma įslaptinta informacija, saugumo užtikrinimo pagrindas. Išsamūs šių nuostatų įgyvendinimo reikalavimai nustatyti ISU saugumo politikoje ir saugumo gairėse.

B.1. *Saugumo rizikos valdymas*

7. Saugumo rizikos valdymas yra neatsiejama RIS apibrėžties, kūrimo, veikimo ir priežiūros dalis. Rizikos valdymą (įvertinimą, traktavimą, pripažinimą ir informavimą), kaip kartotinį procesą, kartu vykdo sistemos savininkų, projekto institucijų, vykdančiųjų institucijų ir saugumo patvirtinimo institucijų atstovai, taikydami pavirtintą, skaidrų ir suprantamą rizikos įvertinimo procesą, o rizikos valdymas reglamentuojamas I saugumo pranešime. RIS ir jos turinio taikymo sritis aiškiai apibrėžiama rizikos valdymo proceso pradžioje.

8. Kompetentingos institucijos, kaip nurodyta I saugumo pranešime, peržiūri pavojus, kurie gali kilti RIS, ir nuolat vykdo naujausiais duomenimis grindžiamus ir tikslius pavojų įvertinimus, kurie atspindi esamą sistemos operacinę aplinką. Jos nuolat atnaujina savo žinias pažeidžiamumo klausimais ir reguliariai peržiūri pažeidžiamumo įvertinimą, neatsilikdamos nuo informacinių technologijų (IT) aplinkos pokyčių.

9. Valdant saugumo riziką siekiama taikyti apsaugos priemonių rinkinį, kuris užtikrina tinkamą vartotojų reikalavimų, sąnaudų ir likutinės rizikos, susijusios su saugumu, pusiausvyrą.

10. RIS akreditavimas apima atsakingos institucijos oficialų pareiškimą dėl likutinės rizikos ir likutinės rizikos pripažinimą. RIS akreditavimui taikomi konkretūs reikalavimai, reikalavimai dėl informacijos ap-

imties ir išsamumo, kuriuos nustato atitinkama SAI, turi atitikti įvertintą riziką, atsižvelgiant į visus svarbius veiksnius, įskaitant įslaptintos informacijos, kuri tvarkoma RIS, slaptumo žymos laipsnį.

B.2. *Saugumas viso RIS gyvavimo ciklo metu*

11. Saugumas turi būti užtikrintas viso RIS gyvavimo ciklo metu – nuo pradžios iki naudojimosi pabaigos.

12. Kiekvienu gyvavimo ciklo etapu nustatomas kiekvieno RIS dalyvio ir jo sąveikos su kitais dalyviais vaidmuo saugumo požiūriu.

13. RIS, įskaitant technines ir netechnines saugumo priemones, bandomos saugumo požiūriu akreditavimo proceso metu siekiant užtikrinti tinkamą saugumo užtikrinimo lygį ir patikrinti, ar RIS, įskaitant jų technines ir netechnines saugumo priemones, teisingai įdiegtos, integruotos ir sukonfigūruotos.

14. Saugumo įvertinimai, patikrinimai ir peržiūros atliekami reguliariai RIS veikimo ir techninės priežiūros metu bei susidarius išskirtinėms aplinkybėms.

15. RIS saugumo dokumentų atnaujinimas viso jos gyvavimo ciklo metu vykdomas kaip neatsiejama pakeitimų atlikimo ir konfigūracijos valdymo proceso dalis.

16. RIS atliekamos registravimo procedūros prireikus patikrinamos akreditavimo proceso metu.

B.3. *Geriausia patirtis*

17. ISUI parengia geriausios praktikos pavyzdžius, susijusius su RIS tvarkomos įslaptintos informacijos apsauga. Geriausios praktikos gairėse išdėstomos RIS skirtos techninės, fizinės, organizacinės ir procedūrinės saugumo priemonės, kurių veiksmingumas apsisaugant nuo konkrečių grėsmių ir pažeidžiamumo buvo įrodytas.

18. RIS tvarkomos įslaptintos informacijos apsauga užtikrinama, remiantis ISU dalyvaujančių subjektų įgyta patirtimi.

19. Geriausios praktikos pavyzdžių platinimu ir jų įgyvendinimu prisidedama prie siekio užtikrinti lygiavertį Parlamento sekretoriato naudojamų RIS, kuriose tvarkoma įslaptinta informacija, saugumo užtikrinimo lygį.

B.4. *Nuodugni apsauga*

20. Siekiant sušvelninti pavojų RIS, įgyvendinama daug techninių ir netechninių saugumo priemonių, kurios grupuojamos kaip kelios gynybinės linijos. Tos linijos apima:

a) atgrasymą – saugumo priemones, skirtas įtikinti nerengti priešiškų planų pulti RIS;
b) prevenciją – saugumo priemones, skirtas apsunkinti RIS puolimą arba jam sutrukdyti;
c) aptikimą – saugumo priemones, skirtas aptikti RIS puolimo atvejį;
d) atsparumą – saugumo priemones, skirtas apriboti puolimo poveikį iki mažiausio informacijos rinkinio ar RIS dalių grupės bei užkirsti kelią tolesnei žalai;
e) atstatymą – saugumo priemones, skirtas RIS saugiai padėčiai atkurti.

Tokių saugumo priemonių griežtumo lygis nustatomas atsižvelgiant į rizikos įvertinimą.

21. Kompetentingos institucijos, kaip tiksliai nurodyta I saugumo pranešime, užtikrina savo gebėjimus reaguoti į incidentus, kurie gali apimti kelias organizacijas, kad galėtų derinti reagavimo veiksmus ir dalytis informacija apie tuos incidentus bei susijusią riziką (kompiuterinių incidentų tyrimo gebėjimai).

B.5. *Minimalumo ir mažiausių privilegijų principas*

22. Įdiegiamos tik atsižvelgiant į operacinius reikalavimus būtinos funkcijos, prietaisai ir paslaugos, siekiant išvengti nereikalingos rizikos.

23. RIS naudotojams ir automatizuotiems procesams suteikiama tik tokia prieiga, privilegijos ar leidimai, kokių jiems reikia savo užduotims atlikti, siekiant apriboti žalą, kuri padaroma dėl avarijų, klaidų ar RIS išteklių naudojimo be leidimo.

B.6. *Informuotumas informacijos saugumo užtikrinimo srityje*

24. Informuotumas apie riziką ir turimas saugumo priemones yra pirmoji RIS saugumo gynybos linija. Visų pirma, visi personalo nariai, susiję su RIS gyvavimo ciklu, įskaitant naudotojus, suvokia:

a) kad naudojant įslaptintą informaciją saugumo spragos gali labai pakenkti RIS;

b) galimą žalą kitiems, kuri gali kilti dėl tarpusavio sujungimo ir tarpusavio priklausomybės;
c) savo asmeninę atsakomybę ir atsakingumą už RIS saugumą atsižvelgdami į savo vaidmenį naudojant sistemas ir procesus.

25. Siekiant užtikrinti, kad būtų suvokiama atsakomybė už saugumą, visam dalyvaujančiam personalui, įskaitant aukštesniąją vadovybę, Europos Parlamento narius ir RIS naudotojus, yra privalomi ISU švietimo ir informuotumo mokymai.

B.7. *IT saugumo priemonių vertinimas ir patvirtinimas*

26. RIS, kurioje tvarkoma slaptumo žymos CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ar TRÈS SECRET UE/EU TOP SECRET ar jam lygiaverčiu laipsniu, pažymėta informacija, apsaugoma tokiu būdu, kad informacija negalėtų būti neteisėtai atskleista dėl netyčinio elektromagnetinio spinduliavimo (TEMPEST apsaugos priemonės).

27. Kai įslaptinta informacija apsaugoma šifravimo priemonėmis, tas priemones patvirtina SAI kaip ES patvirtintas priemones.

28. Perduodant įslaptintą informaciją elektroninėmis priemonėmis naudojamos ES patvirtintos šifravimo priemonės. Nepaisant šio reikalavimo, esant nepaprastosios padėties sąlygoms arba specifinių techninių konfigūracijų atvejais, kaip nurodyta 41 ir 44 punktuose, gali būti taikomos specialios procedūros.

29. Reikiamas saugumo priemonių patikimumo lygis, apibrėžiamas kaip saugumo užtikrinimo lygis, nustatomas remiantis rizikos valdymo proceso rezultatais ir laikantis atitinkamos saugumo politikos bei gairių.

30. Saugumo užtikrinimo lygis patikrinamas naudojant tarptautiniu arba nacionaliniu lygiu patvirtintus procesus ir metodus. Tai apima pirminį įvertinimą, kontrolę ir auditą.

31. SAI patvirtina nešifravimo IT saugumo priemonių reikalavimų atitikimo ir patvirtinimo saugumo gaires.

B.8. *Perdavimas saugioje zonoje*

32. Kai įslaptintos informacijos perdavimas vykdomas saugioje zonoje, remiantis rizikos valdymo proceso rezultatais ir SAI pritarus, informacija gali būti platinama nešifruota arba šifruota žemesniu lygiu.

B.9. *Saugus RIS tarpusavio sujungimas*

33. Sistemų tarpusavio sujungimas reiškia tiesioginį dviejų ar daugiau IT sistemų sujungimą siekiant dalytis duomenimis ir kitais informacijos šaltiniais vienakrypčiu arba daugiakrypčiu būdu.

34. RIS kiekviena tarpusavyje sujungta IT sistema pirmiausia yra traktuojama kaip nepatikima ir sistemoje įdiegiamos apsaugos priemonės keitimuisi įslaptinta informacija su kita RIS kontroliuoti.

35. Bet kokio RIS ir kitos IT sistemos tarpusavio sujungimo atveju laikomasi toliau išdėstytų pagrindinių reikalavimų:

a) tokiems tarpusavio sujungimams taikomus veiklos arba operacinius reikalavimus nurodo ir patvirtina atsakingos institucijos;
b) tarpusavio sujungimui taikomas rizikos valdymas ir akreditavimo procesas, sujungimui reikalingas kompetentingų SAI pavirtinimas;
c) apsaugos priemonės (AP) įdiegiamos RIS perimetre.

36. Akredituota RIS ir neapsaugotas arba viešas tinklas negali būti tarpusavyje sujungiami, išskyrus atvejus, kai tarp RIS ir neapsaugoto arba viešo tinklo yra šiuo tikslu įdiegtos patvirtintos apsaugos priemonės. Tokiems tarpusavio sujungimams taikytinas saugumo priemones peržiūri kompetentinga ISUI ir patvirtina kompetentinga SAI.

37. Kai duomenys, perduodami neapsaugotu arba viešu tinklu, yra užšifruojami pagal 27 straipsnį patvirtinta ES šifravimo priemone. Toks sujungimas nelaikomas tarpusavio sujungimu.

38. Draudžiamas tiesioginis arba pakopinis RIS, akredituotos tvarkyti slaptumo žymos TRES SECRET UE/EU TOP SECRET ar jam lygiaverčiu laipsniu pažymėtą informaciją ar slaptumo žymos SECRET UE/EU SECRET arba jam lygiaverčiu laipsniu pažymėtą informaciją, ir neapsaugoto arba viešo tinklo tarpusavio sujungimas.

B.10. *Kompiuterinių duomenų saugojimo laikmenos*

39. Šifravimo priemonės sunaikinamos laikantis kompetentingos saugumo institucijos patvirtintų procedūrų.

40. Kompiuterinių duomenų saugojimo laikmenos pakartotinai naudojamos, jų slaptumo žymos laipsnis gali būti sumažintas arba laikmenos išslaptintos laikantis naudojimo nurodymų.

B.11. *Nepaprastosios padėties sąlygos*

41. Toliau aprašytos specialios procedūros gali būti taikomos, esant nepaprastajai padėčiai, pavyzdžiui, gresiant ar esant krizei, konfliktui ar karinei padėčiai, arba susidarius išskirtinėms su eksploatavimu susijusioms sąlygoms.

42. Įslaptinta informacija, pritarus kompetentingai institucijai, gali būti perduodama naudojant šifravimo priemones, kurios buvo patvirtintos žemesnio įslaptinimo laipsnio informacijai, arba nešifruota informacija, jei vėlavimas padarytų aiškiai didesnę žalą, negu įslaptintos medžiagos atskleidimas, ir jei:

a) siuntėjas ir gavėjas neturi reikiamos šifravimo įrangos arba jokios šifravimo įrangos;
b) įslaptinta medžiaga negali būti laiku perduota kitomis priemonėmis.

43. 41 dalyje išdėstytomis aplinkybėmis perduodama įslaptinta informacija nėra pažymėta jokiomis žymomis arba nuorodomis, kurios sudarytų sąlygas ją atskirti nuo neįslaptintos informacijos arba kurią galima apsaugoti naudojant turimas šifravimo priemones. Gavėjams kitomis priemonėmis nedelsiant pranešama apie informacijos slaptumo laipsnį.

44. Jeigu taikomos 41 ir 42 dalys, kompetentingai institucijai vėliau pateikiama ataskaita.

IV SAUGUMO PRANEŠIMAS

FIZINIS SAUGUMAS

A. ĮVADAS

Šiame saugumo pranešime nustatomi saugumo principai, kuriais siekiama sukurti saugią aplinką konfidencialios informacijos Europos Parlamente tvarkymui užtikrinti. Šiuos principus, įskaitant susijusius su techniniu saugumu, papildys naudojimo nurodymai.

B. SAUGUMO RIZIKOS VALDYMAS

1. Įslaptintai informacijai kylančios rizikos valdymas yra procesas. To proceso tikslas – nustatyti žinomą saugumo riziką, apibrėžti saugumo priemones tokiai rizikai sumažinti iki priimtino lygio pagal saugumo pranešime išdėstytus pagrindinius principus ir būtiniausius standartus ir taikyti tas priemones laikantis nuodugnios apsaugos sąvokos, kaip apibrėžta III saugumo pranešime. Reguliariai atliekamas tokių priemonių efektyvumo vertinimas.

2. Įslaptintos informacijos apsaugai užtikrinti skirtos saugumo priemonės visą savo gyvavimo ciklą turi atitikti jos slaptumo žymos laipsnį, susijusios informacijos ar medžiagos formą ir kiekį, patalpų, kuriose laikoma įslaptinta informacija, vietos ir konstrukcijos reikalavimus ir turi būti parenkamos, atsižvelgiant į vietos lygiu įvertintą piktavališkos ir (arba) nusikalstamos veiklos, įskaitant šnipinėjimą, sabotažą ar terorizmą, keliamą grėsmę.

3. Nenumatytų atvejų planuose turi būti atsižvelgiama į poreikį apsaugoti įslaptintą informaciją nepaprastosios padėties atvejais siekiant užkirsti kelią galimybei neteisėtai susipažinti su šia informacija, ją atskleisti ar prarasti jos vientisumą arba galimybę ja naudotis.

4. Veiklos tęstinumo planuose numatomos prevencinės ir atstatymo priemonės siekiant sumažinti didelių klaidų ar incidentų poveikį įslaptintos informacijos naudojimui ir saugojimui.

C. BENDRIEJI PRINCIPAI

5. Informacijai suteiktas slaptumo žymos laipsnis ar kitos žymos nulemia tai, kokio lygio apsauga informacijai bus taikoma fizinio saugumo srityse.

6. Informacija, kurią reikia įslaptinti, žymima ir tvarkoma kaip įslaptinta informacija nepriklausomai nuo jos fizinės formos. Apie jos įslaptinimą aiškiai nurodoma jos gavėjams nurodant slaptumo žymą (jeigu ji pateikiama rašytine forma – popieriuje ar RIS) arba apie tai pranešant (jeigu ji pateikiama žodine forma, pavyzdžiui, pokalbio metu arba darant pranešimą). Įslaptinta informacija fiziškai žymima, kad būtų galima paprastai nustatyti jos slaptumo žymą.

7. Konfidenciali informacija jokiomis aplinkybėmis neturi būti skaitoma viešose vietose, kur ją gali pamatyti asmenys, kurie neturėtų su ja susipažinti, pvz., traukiniuose, lėktuvuose, kavinėse, baruose ir t. t. Jos negalima palikti viešbučių seifuose ir kambariuose ar be priežiūros palikti viešose vietose.

D. ATSAKOMYBĖ

8. ĮIS atsako už fizinio saugumo užtikrinimą valdant konfidencialią informaciją, laikomą ĮIS saugiose patalpose. ĮIS taip pat atsako už saugių patalpų administravimą.

9. Už slaptumo žymos RESTREINT UE/EU RESTRICTED ar jam lygiaverčiu laipsniu pažymėtos informacijos arba kitos konfidencialios informacijos fizinį saugumą ją tvarkant atsako atitinkamas Parlamento organas ir (arba) atitinkamas pareigas einantis asmuo.

10. Saugos ir rizikos vertinimo direktoratas užtikrina reikiamą asmens saugumą ir asmens patikimumo patikrinimą, kad būtų užtikrintas saugus konfidencialios informacijos naudojimas Europos Parlamente.

11. ITD konsultuoja ir užtikrina, kad visos sukurtos ir naudojamos RIS visiškai atitiktų III saugumo pranešimą ir atitinkamus naudojimo nurodymus.

E. SAUGIOS PATALPOS

12. Saugios patalpos gali būti įrengtos laikantis techninių saugumo standartų ir atsižvelgiant į konfidencialiai informacijai suteiktą slaptumo laipsnį, kaip nurodyta 7 straipsnyje.

13. Saugias patalpas turi sertifikuoti SAI ir patvirtinti SI.

F. SUSIPAŽINIMAS SU KONFIDENCIALIA INFORMACIJA

14. Kai slaptumo žymos RESTREINT UE/EU RESTRICTED ar jam lygiaverčiu laipsniu žymima informacija arba kita konfidenciali informacija pateikiama ĮIS ir su ja turi būti susipažįstama už saugios zonos ribų, ĮIS perduoda kopiją atitinkamai tarnybai, gavusiai leidimą užtikrinti, kad susipažinimas su šia informacija ir naudojimasis ja atitiktų šio sprendimo 8 straipsnio 2 dalį ir 10 straipsnį bei atitinkamus naudojimo nurodymus.

15. Kai slaptumo žymos RESTREINT UE/EU RESTRICTED ar jam lygiaverčiu laipsniu žymima informacija arba kita konfidenciali informacija pateikiama Parlamento organui ir (arba) pareigas einančiam asmeniui, o ne ĮIS, to Parlamento organo sekretoriatas ir (arba) tas pareigas einantis asmuo užtikrina, kad susipažinimas su susijusia informacija ir naudojimasis ja atitiktų 7 straipsnio 3 dalį, 8 straipsnio 1, 2 ir 4 dalis, 9 straipsnio 3, 4 ir 5 dalis, 10 straipsnio 2 ir 6 dalis ir 11 straipsnį bei atitinkamus naudojimo nurodymus.

16. Kai su slaptumo žymos CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ar TRÈS SECRET UE/EU TOP SECRET ar jam lygiaverčiu žymima informacija reikia susipažinti saugioje zonoje, ĮIS užtikrina, kad susipažinimas su šia informacija ir naudojimasis ja atitiktų šio sprendimo 9 ir 10 straipsnius bei atitinkamus naudojimo nurodymus.

G. TECHNINIS SAUGUMAS

17. Už techninio saugumo priemones atsako SAI, ji nustato konkrečias techninio saugumo priemones, kurias reikia taikyti atitinkamuose naudojimo nurodymuose.

18. Saugios skaityklos, skirtos susipažinti su slaptumo žymos RESTREINT UE/EU RESTRICTED ar jam lygiaverčiu laipsniu pažymėta informacija arba kita konfidenciali informacija atitinka specifinius techninio saugumo reikalavimus, kaip nurodyta naudojimo nurodymuose.

19. Saugi zona apima šias patalpas:

a) saugios prieigos patikrinimo patalpą, kuri turi būti įrengta pagal techninio saugumo reikalavimus, kaip nustatyta naudojimo nurodymuose. Patekimas į šią patalpą turi būti registruojamas. Ši patalpa turi atitikti aukštus turinčių teisę į ją patekti asmenų tapatybės nustatymo ir vaizdo stebėjimo kameromis standartus, joje turi būti įrengta saugi zona, skirta pasidėti asmeninius daiktus, kurių neleidžiama įsinešti į saugias patalpas (telefonai, rašikliai ir t. t.);
b) ryšių patalpą, skirtą įslaptintai informacijai perduoti ar gauti, įskaitant koduotą įslaptintą informaciją, laikantis III saugumo pranešimo ir atitinkamų naudojimo nurodymų;
c) saugų archyvą, kuriame slaptumo žymos RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL ir SECRET UE/EU SECRET laipsniu arba ar jam lygiaverčiu pažymėtai informacijai atskirai naudojamos patvirtintos ir sertifikuotos talpyklos. Informacija, pažymėta slaptumo žymos TRES SECRET UE/EU TOP SECRET laipsniu arba jam lygiaverčiu laipsniu laikoma skirtingose patalpose specialiose sertifikuotose talpyklose. Vienintelė papildoma įranga, kurią leidžiama laikyti šioje patalpoje, yra pagalbinis stalelis, skirtas ĮIS tvarkyti archyvą;
d) registravimo patalpą, kurioje turi būti reikalingos priemonės, kad būtų galima vykdyti registraciją popieriuje ar elektroniniu būdu, ir todėl joje turi būti reikalingos saugios priemonės, skirtos atitinkamai RIS įdiegti. Tik registravimo patalpoje gali būti patvirtinti ir akredituoti dauginimo įrenginiai (popierinės ar elektroninės kopijos). Naudojimo nurodymuose nurodoma, kurie dauginimo įtaisai yra patvirtinti ir akredituoti. Registravimo patalpoje taip pat turi būti galimybė saugoti ir naudoti akredituotus įrenginius, reikalingus fiziniam įslaptintos informacijos žymėjimui, kopijavimui ir skirstymui pagal slaptumo žymos laipsnį. Visus akredituotus įrenginius apibrėžia ĮIS ir akredituoja SAI, vadovaudamasi Informacijos saugumo užtikrinimo operacinės institucijos patarimu. Registravimo patalpoje taip pat turi būti akredituotas dokumentų naikinimo prietaisas, patvirtintas aukščiausio laipsnio slaptumo žyma, kaip aprašyta naudojimo nurodymuose. Slaptumo žymos CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ar TRÈS SECRET UE/EU TOP SECRET laipsniu ar jam lygiaverčiu pažymėta informacija verčiama registravimo patalpoje, naudojantis:

i) patvirtinta ir akredituota sistema. Registravimo patalpoje turi būti dvi darbo vietos, kad du vertėjai vienu metu galėtų versti tą patį dokumentą. Verčiant turi dalyvauti ĮIS darbuotojas;

ii) skaitykla, kurioje tinkamą leidimą gavę asmenys gali individualiai susipažinti su įslaptinta informacija. Skaitykloje turi būti pakankamai vietos dviem asmenims, įskaitant ĮIS darbuotoją, kuris visąlaik turi būti kiekvieno susipažinimo su informacija metu. Šiai patalpai numatytas saugumo laipsnis yra CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ar TRÈS SECRET UE/EU TOP SECRET ar jam lygiavertis. Skaitykloje gali būti įdiegta TEMPEST įranga, skirta, kai reikia, susipažinti su informacija elektroniniu būdu, atsižvelgiant į slaptumo žymos laipsnį;

iii) posėdžių sale, kurioje turi tilpti iki 25 asmenų ir kurioje aptariama informacija, pažymėta slaptumo žymos CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET laipsniu arba jam lygiaverčiu. Posėdžių salėje turi būti techniškai saugi ir sertifikuota įranga, būtina vertimui žodžiu mažiausiai į dvi kalbas užtikrinti. Kai nenaudojama posėdžiams, ši posėdžių salė gali būti naudojama kaip papildoma skaitykla individualiai su informacija susipažįstantiems asmenims. Išimtiniais atvejais ĮIS gali leisti daugiau nei vienam leidimą turinčiam asmeniui susipažinti su įslaptinta informacija, jeigu visų salėje esančių asmenų patikimumo patikrinimo lygmuo yra vienodas ir visi asmenys atitinka principą „būtina žinoti“. Su įslaptinta informacija vienu metu gali susipažinti ne daugiau kaip keturi asmenys. Numatomas didesnis ĮIS darbuotojų skaičius;

iv) saugiomis techninėmis patalpomis, kuriose yra visa techninė įranga, susijusi su visos saugios zonos saugumu, ir apsaugoti IT serveriai;

20. Saugios zonos turi atitikti tarptautinius saugumo standartus ir turi būti sertifikuotos Saugos ir rizikos vertinimo direktorato. Saugi zona turi atitikti šiuos minimalius saugumo techninius reikalavimus:

a) įrengtos signalizacijos ir saugumo stebėsenos sistemos;
b) saugos įrangos ir avarinės sistemos (dvipusio įspėjimo sistema);
c) apsauginė vaizdo stebėjimo sistema (AVSS);
d) įsibrovimo aptikimo sistema;
e) patekimo kontrolė (įskaitant biometrinio saugumo sistemą);
f) talpyklos;
g) užrakinamos spintelės;
h) apsauga nuo elektromagnetinio lauko.

21. Glaudžiai bendradarbiaudama su ĮIS ir laikydamasi SI nurodymų, SAI gali pridėti papildomų reikalingų techninio saugumo priemonių.

22. Infrastruktūros įranga gali būti prijungta prie pastato, kuriame yra saugi zona, bendrųjų valdymo sistemų. Tačiau saugos įranga, skirta prieigos kontrolei ir RIS, turi būti nepriklausoma nuo visų kitų Europos Parlamente esamų sistemų.

H. SAUGIOS ZONOS TIKRINIMAI

23. SAI saugios zonos tikrinimus vykdo reguliariai ir paprašius ĮIS.

24. SAI sudaro ir atnaujina saugumo patikrinimo sąrašus, kuriuose nurodo, ką tikrinimų metu reikia patikrinti laikantis naudojimo nurodymų.

I. KONFIDENCIALIOS INFORMACIJOS TRANSPORTAVIMAS

25. Konfidenciali informacija gabenama taip, kad nebūtų matoma, ir nepateikiant jokios nuorodos į tai, kad jos turinys konfidencialaus pobūdžio, laikantis naudojimo nurodymų.

26. Tik pasiuntiniai ir darbuotojai, turintys leidimą dirbti su atitinkamo slaptumo žymos laipsnio informacija, gali gabenti informaciją su slaptumo žymos CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ar TRÈS SECRET UE/EU TOP SECRET laipsniu arba jam lygiaverčiu.

27. Konfidenciali informacija gali būti siunčiama išorės paštu ar nešama per pasiuntinį už pastato ribų tik laikantis sąlygų, nustatytų naudojimo nurodymuose.

28. Informacija su slaptumo žymos CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ar TRÈS SECRET UE/EU TOP SECRET laipsniu arba jam lygiaverčiu niekada nesiunčiama elektroniniu paštu ar faksu, net jei yra įrengta saugaus elektroninio pašto sistema ar koduojantis faksas. Slaptumo žymos RESTREINT UE/EU RESTRICTED laipsniu arba jam lygiaverčiu pažymėta informacija arba kita konfidenciali informacija gali būti siunčiama elektroniniu paštu, naudojant akredituotą kodavimo sistemą.

J. KONFIDENCIALIOS INFORMACIJOS LAIKYMAS

29. Konfidencialiai informacijai suteiktos slaptumo ar kitos žymos nulemia tai, kokio lygio apsauga jai bus taikoma numatant jos laikymą. Ji laikoma naudojant tam tikslui sertifikuotą įrangą pagal naudojimo nurodymus.

30. Slaptumo žymos RESTREINT UE/EU RESTRICTED laipsniu arba jam lygiaverčiu žymima informacija ir kita konfidenciali informacija:

a) laikoma standartinėje metalinėje užrakintoje spintoje kabinete ar darbo zonoje, kai ja nesinaudojama;
b) nepaliekama be priežiūros, nebent yra saugiai padėta ir užrakinta;
c) nepaliekama ant stalo ar darbo stalo ir pan. taip, kad bet koks neįgaliotas asmuo, pvz., lankytojai, valytojai, priežiūros darbuotojai ir t. t., galėtų ją perskaityti ar išsinešti;
d) nerodoma neįgaliotiems asmenims arba su jais neaptariama.

31. Informacija, pažymėta slaptumo žymos RESTREINT UE/EU RESTRICTED laipsniu arba jam lygiaverčiu ir kita konfidenciali informacija laikoma tik Parlamento organo ir (arba) atitinkamas pareigas einančių asmenų sekretoriatuose arba ĮIS, laikantis naudojimosi nurodymų.

32. Slaptumo žymos CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ar TRÈS SECRET UE/EU TOP SECRET laipsniu arba jam lygiaverčiu žymima informacija:

a) laikoma saugioje zonoje, apsauginėje talpykloje arba saugykloje. Išimtiniais atvejais, pavyzdžiui, jei ĮIS uždarytas, ji gali būti laikoma saugumo tarnybų patvirtintame ir sertifikuotame seife;
b) niekada negali būti palikta be priežiūros saugioje zonoje prieš tai jos neužrakinus patvirtintame seife (net ir trumpiausiam laikui);
c) nepaliekama ant stalo ar darbo stalo ir pan. taip, kad bet koks neįgaliotas asmuo galėtų ją perskaityti ar išsinešti, net jei atsakingas ĮIS darbuotojas yra patalpoje.

Kai dokumentas, kuriame yra įslaptintos informacijos, kuriamas elektronine forma saugioje zonoje, kompiuteris užrakinamas, o ekranas turi būti neprieinamas, jei autorius arba atsakingas ĮIS darbuotojas išeina iš patalpos (net ir trumpiausiam laikui). Automatinis apsauginis užraktas, suveikiantis po kelių minučių, negali būti laikomas pakankama priemone.

V SAUGUMO PRANEŠIMAS

PRAMONINIS SAUGUMAS

A. ĮVADAS

1. Šis saugumo pranešimas taikomas tik įslaptintai informacijai.

2. Jame išdėstomos šio sprendimo I priedo 1 dalyje nurodytų bendrųjų būtiniausių standartų įgyvendinimo nuostatos.

3. Pramoninis saugumas – priemonių, kurias rangovai arba subrangovai taiko derybų dėl sutarčių sudarymo metu ir visą įslaptintų sutarčių gyvavimo ciklą siekdami užtikrinti įslaptintos informacijos apsaugą, taikymas. Tokiose sutartyse nenumatoma galimybė susipažinti su slaptumo žymos TRES SECRET UE/EU TOP SECRET laipsniu pažymėta informacija.

4. Europos Parlamentas, kaip perkančioji institucija, užtikrina, kad skiriant įslaptintas sutartis su pramonės ar kitais subjektais būtų laikomasi šiame sprendime išdėstytų ir sutartyje nurodytų būtiniausių pramoninio saugumo standartų.

B. SAUGUMO ASPEKTAI ĮSLAPTINTOSE SUTARTYSE

B.1. *Slaptumo žymų vadovas (SŽV)*

5. Prieš paskelbdamas kvietimą teikti pasiūlymus įslaptintai sutarčiai sudaryti arba prieš sudarydamas įslaptintą sutartį, Europos Parlamentas, kaip perkančioji institucija, nustato visos informacijos, kuri turi būti suteikta konkurso dalyviams ir rangovams, slaptumo žymą, taip pat visos informacijos, kurią turi parengti rangovas, slaptumo žymą. Šiuo tikslu jis parengia slaptumo žymų vadovą (SŽV), kuris turi būti naudojamas vykdant sutartį.

6. Siekiant nustatyti skirtingų įslaptintos sutarties dalių slaptumo žymos laipsnį, taikomi toliau nurodyti principai:

a) rengdamas SŽV, Europos Parlamentas atsižvelgia į visus svarbius saugumo aspektus, įskaitant slaptumo žymą, priskirtą informacijai, kurią jos rengėjas pateikė ir patvirtino kaip naudotiną tai sutarčiai;
b) bendras sutarties slaptumo žymos laipsnis negali būti žemesnis nei aukščiausia bet kurios jos dalies slaptumo žyma;

B.2. *Saugumo aspektų paaiškinimas (SAP)*

7. Konkrečioms sutartims skirti saugumo reikalavimai aprašomi saugumo aspektų paaiškinime (SAP). Prireikus į SAP įtraukiamas SŽV; SAP yra neatsiejama įslaptintos sutarties ar subrangos sutarties dalis.

8. Į SAP įtraukiamos nuostatos, pagal kurias reikalaujama, kad rangovas ir (arba) subrangovas laikytųsi būtiniausių šiame sprendime nustatytų standartų. Tų būtiniausių standartų nesilaikymas gali būti pakankamas pagrindas sutarčiai nutraukti.

B.3. *Programos (projekto) saugumo instrukcijos (PSI)*

9. Atsižvelgiant į programų ar projektų, kuriuos vykdant reikia susipažinti su ESĮI arba ją tvarkyti ar saugoti, apimtį, programą ar projektą valdyti paskirta perkančioji institucija gali parengti konkrečios programos ar projekto saugumo instrukcijas (PSI).

C. ĮMONĖS PATIKIMUMĄ PATVIRTINANTIS PAŽYMĖJIMAS (ĮPPP)

10. ĮPPP išduoda valstybės narės NSI arba PSI ar kita kompetentinga saugumo institucija ir jame pagal nacionalinius įstatymus ir kitus teisės aktus nurodoma, kad pramonės arba kitas subjektas savo patalpose gali apsaugoti ESĮI slaptumo žymos CONFIDENTIEL UE/EU CONFIDENTIAL arba SECRET UE/EU SECRET laipsniu arba jam lygiaverčiu. Prieš rangovui ar subrangovui arba potencialiam rangovui ar subrangovui suteikiant ESĮI arba galimybę susipažinti su ESĮI, Europos Parlamentui, kaip perkančiajai institucijai, pateikiamas kaip įrodymas ĮPPP.

11. ĮPPP:
a) įvertina pramonės ar kitų subjektų patikimumą;
b) įvertina nuosavybę, kontrolę ir (arba) nederamos įtakos tikimybę, kurie gali būti laikomi saugumo rizika;

c) įsitikina, kad pramonės arba kitas subjektas patalpose yra sukūręs saugumo sistemą, kuri apima visas atitinkamas saugumo priemones, būtinas, kad būtų apsaugota informacija ar medžiaga, pažymėta slaptumo žymos laipsniu CONFIDENTIEL UE/EU CONFIDENTIAL arba SECRET UE/EU SECRET, laikantis šiame sprendime nustatytų reikalavimų;
d) įsitikina, kad vadovybės, savininkų ir darbuotojų, kurie turi turėti galimybę susipažinti su informacija, pažymėta slaptumo žymos laipsniu CONFIDENTIEL UE/EU CONFIDENTIAL arba SECRET UE/EU SECRET, asmens patikimumo statusas yra nustatytas laikantis šiame sprendime nustatytų reikalavimų;
e) įsitikina, kad pramonės arba kitas subjektas yra paskyręs patalpų saugumo pareigūną, kuris yra atsakingas vadovybei už saugumo įsipareigojimų tokiame subjekte vykdymo užtikrinimą.

12. Atitinkamais atvejais Europos Parlamentas, kaip perkančioji institucija, praneša atitinkamai NSI ar kitai kompetentingai saugumo institucijai, kad prieš sudarant sutartį arba sutarties vykdymui reikalingas ĮPPP. ĮPPP arba APP reikalaujama pateikti prieš sudarant sutartį tais atvejais, kai slaptumo žymos laipsniu CONFIDENTIEL UE/EU CONFIDENTIAL arba SECRET UE/EU SECRET pažymėta informacija turi būti suteikta paraiškų teikimo proceso metu.

13. Perkančioji institucija neskiria įslaptintos sutarties pasirinktam dalyviui prieš tai negavusi valstybės narės, kurioje yra registruotas atitinkamas rangovas ar subrangovas, NSI ar kitos kompetentingos saugumo institucijos patvirtinimo, kad reikiamais atvejais yra išduotas tinkamas ĮPPP.

14. ĮPPP išdavusi kompetentinga saugumo institucija praneša Europos Parlamentui, kaip perkančiajai institucijai, apie pasikeitimus, turinčius įtakos ĮPPP. Subrangos sutarties atveju atitinkamai informuojama kompetentinga saugumo institucija.

15. Jeigu atitinkama NSI ar kita kompetentinga saugumo institucija panaikina ĮPPP, tai yra pakankamas pagrindas Europos Parlamentui, kaip perkančiajai institucijai, nutraukti įslaptintą sutartį arba pašalinti dalyvį iš konkurso.

D. ĮSLAPTINTOS SUTARTYS IR SUBRANGOS SUTARTYS

16. Tais atvejais, kai įslaptinta informacija suteikiama dalyviui prieš sudarant sutartį, kvietime teikti paraiškas numatoma nuostata, pagal kurią paraiškos nepateikęs arba neatrinktas dalyvis įpareigojamas per nurodytą laiką grąžinti visus įslaptintus dokumentus.

17. Sudarius įslaptintą sutartį ar subrangos sutartį, Europos Parlamentas, kaip perkančioji institucija, praneša rangovo ir (arba) subrangovo NSI ar kitai kompetentingai saugumo institucijai tos įslaptintos sutarties saugumo nuostatas.

18. Nutraukus tokią sutartį, Europos Parlamentas, kaip perkančioji institucija ir (arba) atitinkamai kompetentinga saugumo institucija subrangos sutarties atveju), skubiai apie tai praneša valstybės narės, kurioje registruotas rangovas arba subrangovas, NSI ar kitai kompetentingai saugumo institucijai.

19. Paprastai reikalaujama, kad nutraukus įslaptintą sutartį ar subrangos sutartį rangovas arba subrangovas perkančiajai institucijai grąžintų visą turimą įslaptintą informaciją.

20. Konkrečios nuostatos dėl įslaptintos informacijos sunaikinimo vykdant sutartį arba ją nutraukus išdėstomos saugumo aspektų paaiškinime.

21. Tais atvejais, kai rangovui arba subrangovui duotas leidimas nutraukus sutartį pasilikti įslaptintą informaciją, šiame sprendime nustatyti būtiniausi standartai toliau galioja, o rangovas ir subrangovas užtikrina ESĮI konfidencialumą.

22. Sąlygos, kuriomis rangovas gali sudaryti subrangos sutartis, nurodomos kvietime teikti paraiškas ir sutartyje.

23. Prieš sudarydamas subrangos sutartis dėl įslaptintos sutarties dalių, rangovas turi gauti Europos Parlamento, kaip perkančiosios institucijos, leidimą. Su pramonės arba kitais subjektais, registruotais trečiojoje šalyje, kuri nėra sudariusi susitarimo dėl informacijos saugumo su Europos Sąjunga, subrangos sutartys negali būti sudaromos.

24. Rangovas atsako už tai, kad visa subrangos veikla būtų vykdoma, laikantis šiame sprendime nustatytų būtiniausių standartų, ir negali suteikti subrangovui ESĮI be išankstinio rašytinio perkančiosios institucijos sutikimo.

25. Įslaptintos informacijos, kurią parengė ar tvarko rangovas arba subrangovas, atžvilgiu perkančioji institucija naudojasi rengėjui priklausančiomis teisėmis.

E. VIZITAI, SUSIJĘ SU ĮSLAPTINTOMIS SUTARTIMIS

26. Jei Europos Parlamentui, rangovams ar subrangovams reikia susipažinti su slaptumo žymos laipsniu CONFIDENTIEL UE/EU CONFIDENTIAL arba SECRET UE/EU SECRET pažymėta informacija vieniems kitų patalpose, kad galėtų įvykdyti sutartį, dėl jų vizitų susitariama palaikant ryšius su nacionalinėmis saugumo institucijomis arba bet kokia kita atitinkama kompetentinga saugumo institucija. Tačiau tam tikrų projektų atveju nacionalinės saugumo institucijos gali taip pat susitarti dėl tvarkos, pagal kurią dėl tokių vizitų gali būti susitariama tiesiogiai.

27. Kad galėtų susipažinti su įslaptinta informacija, susijusia su Europos Parlamento sutartimi, visi lankytojai turi turėti atitinkamą APP ir turi būti vadovaujamasi principu „būtina žinoti“.

28. Lankytojams leidžiama susipažinti tik su ta įslaptinta informacija, kuri yra susijusi su vizito tikslu.

F. ĮSLAPTINTOS INFORMACIJOS PERDAVIMAS IR GABENIMAS

29. Perduodant įslaptintą informaciją elektroninėmis priemonėmis, taikomos atitinkamos III saugumo pranešimo nuostatos.

30. Įslaptintos informacijos pervežimui taikomos atitinkamos IV saugumo pranešimo nuostatos ir atitinkami naudojimo nurodymai.

31. Nustatant įslaptintos medžiagos (kaip krovinio) gabenimui taikomą saugumo tvarką taikomi toliau nurodyti principai:

a) saugumas užtikrinamas visuose gabenimo etapuose nuo gabenimo pradžios vietos iki galutinės paskirties vietos;
b) siuntai suteikiamas apsaugos lygis nustatomas pagal joje esančios medžiagos aukščiausią slaptumo žymos laipsnį;
c) gabenimą užtikrinančios bendrovės turi gauti atitinkamos slaptumo žymos ĮPPP. Tokiais atvejais laikantis I priedo turi būti patikrintas siuntą gabenančio personalo patikimumas;

d) prieš gabenant per valstybių sienas medžiagą, pažymėtą slaptumo žymos laipsniu CONFIDENTIEL UE/EU CONFIDENTIAL arba SECRET UE/EU SECRET ar jam lygiaverčiu, siuntėjas parengia, o generalinis sekretorius patvirtina gabenimo planą;
e) stengiamasi, kad kelionės vyktų be sustojimo ir būtų užbaigtos taip greitai, kaip leidžia aplinkybės;
f) kai tik įmanoma, pasirenkami maršrutai per valstybių narių teritoriją.

G. ĮSLAPTINTOS INFORMACIJOS PERDAVIMAS TREČIOSIOSE VALSTYBĖSE ĮSISTEIGUSIEMS RANGOVAMS

32. ESĮI Įslaptinta informacija perduodama trečiosiose valstybėse įsisteigusiems rangovams ir subrangovams, laikantis saugumo priemonių, dėl kurių susitarė Europos Parlamentas, kaip perkančioji institucija, ir atitinkama trečioji valstybė, kurioje registruotas rangovas.

H. SLAPTUMO ŽYMOS LAIPSNIU *RESTREINT UE/EU RESTRICTED* PAŽYMĖTOS INFORMACIJOS TVARKYMAS IR LAIKYMAS

33. Palaikydamas ryšius su valstybės narės NSI, Europos Parlamentas, kaip perkančioji institucija, prireikus turi teisę remdamasis sutarties nuostatomis rengti vizitus į rangovo (subrangovo) patalpas, kad patikrintų, ar įgyvendintos pagal sutartį reikalaujamos tinkamos saugumo priemonės, skirtos apsaugoti slaptumo žymos laipsniu RESTREINT UE/EU RESTRICTED pažymėtą ESĮI.

34. Kiek būtina pagal nacionalinius įstatymus ir kitus teisės aktus, nacionalinėms saugumo institucijoms (NSI) ar bet kokioms kitoms kompetentingoms saugumo institucijoms Europos Parlamentas, kaip perkančioji institucija, praneša apie sutartis arba subrangos sutartis, kuriose yra slaptumo žymos laipsniu RESTREINT UE/EU RESTRICTED pažymėtos informacijos.

35. Europos Parlamento sudarytų sutarčių, kuriose yra slaptumo žymos laipsniu RESTREINT UE/EU RESTRICTED pažymėtos informacijos, atveju rangovai ar subrangovai ir jų personalas neprivalo turėti ĮPPP ar APP.

36. Europos Parlamentas, kaip perkančioji institucija, išnagrinėja atsakymus į kvietimus dalyvauti konkursuose dėl sutarčių, pagal kurias turi būti suteikta galimybė susipažinti su slaptumo žymos laipsniu RESTREINT UE/EU RESTRICTED pažymėta informacija, neatsižvelgdamas į reikalavimus, susijusius su ĮPPP ar APP, kurie gali būti numatyti nacionaliniuose įstatymuose ir kituose teisės aktuose.

37. Sąlygos, kuriomis rangovas gali sudaryti subrangos sutartis, nurodomos kvietime teikti paraiškas ir sutartyje.

38. Kai pagal sutartį numatytas informacijos, pažymėtos slaptumo žymos laipsniu RESTREINT UE/EU RESTRICTED, tvarkymas rangovo naudojamoje ryšių ir informacijos sistemoje, Europos Parlamentas, kaip perkančioji institucija, užtikrina, kad sutartyje arba subrangos sutartyje būtų nustatyti su ryšio ir informacijos sistemos akreditavimu susiję būtini techniniai ir administraciniai reikalavimai, kurie atitiktų įvertintą riziką, ir atsižvelgia į visus svarbius veiksnius. Perkančioji institucija ir atitinkama NSI susitaria dėl tokio ryšių ir informacijos sistemų akreditavimo masto.

VI SAUGUMO PRANEŠIMAS

KONFINDENCIALIOS INFORMACIJOS SAUGUMO PAŽEIDIMAI, PRARADIMAS ARBA NETEISĖTAS ATSKLEIDIMAS

1. Saugumas pažeidžiamas dėl veiksmo ar neveikimo, prieštaraujančio sprendimui, dėl kurio gali kilti pavojus ar būti neteisėtai atskleista konfidenciali informacija.

2. Įslaptintos informacijos neteisėtu atskleidimu laikomas jos visos arba jos dalies patekimas į leidimo tam neturinčių asmenų rankas, t. y. į rankas tų asmenų, kurie neturi asmens patikimumo pažymėjimo arba neatitinka principo „būtina žinoti“, arba jei yra tikimybė, kad tai atsitiko.

3. Konfidenciali informacija gali būti neteisėtai atskleista dėl nerūpestingumo, neapdairumo ar neatsargumo, taip pat dėl tarnybų veiklos, nukreiptos apie ES, arba ardomąja veikla užsiimančių organizacijų veiklos.

4. Kai generalinis sekretorius sužino ar yra informuojamas apie įrodytus ar tariamus konfidencialios informacijos saugumo pažeidimus, praradimą arba neteisėtą atskleidimą, jis:

a) nustato faktus;
b) įvertina ir kuo labiau sumažina padarytą žalą;
c) imasi atitinkamų priemonių, kad pažeidimas nepasikartotų;
d) praneša trečiosios šalies kompetentingai institucijai ar valstybei narei, kuri sukūrė arba perdavė konfidencialią informaciją.

Jeigu su tokiu įvykiu yra susijęs Europos Parlamento narys, generalinis sekretorius veikia kartu su Europos Parlamento pirmininku.

Jei informacija gauta iš kitos Europos Sąjungos institucijos, generalinis sekretorius veikia vadovaudamasis atitinkamomis saugumo priemonėmis, nustatytomis įslaptintai informacijai, ir įsipareigojimais, nustatytais pagal Pagrindų susitarimą su Komisija ar Tarpinstitucinį susitarimą su Taryba.

5. Visi su konfidencialia informacija turintys dirbti asmenys tinkamai informuojami apie saugumo procedūras, neatsargių pokalbių ir ryšių su žiniasklaida keliamus pavojus ir, kai tikslinga, pasirašo pareiškimą, kad neatskleis konfidencialaus turinio informacijos tretiesiems asmenims, kad laikysis įsipareigojimo saugoti įslaptintą informaciją ir kad pri-

pažįsta ir suvokia padarinius, jei nesilaikys reikalavimų. Jei asmuo, kuris nebuvo informuotas ir nepasirašė atitinkamo pranešimo, turi prieigą prie įslaptintos informacijos ar ja naudojasi, tai laikoma saugumo pažeidimu.

6. Europos Parlamento nariai, Europos Parlamento pareigūnai ir kiti Parlamento darbuotojai, kurie dirba frakcijose arba yra laikinai samdomi, tučtuojau praneša generaliniam sekretoriui apie jų pastebėtus bet kokius saugumo pažeidimus, konfidencialios informacijos praradimą ar neteisėtą atskleidimą.

7. Asmuo, dėl kurio kaltės buvo neteisėtai atskleista konfidenciali informacija, baudžiamas drausmine nuobauda pagal atitinkamas teisės normas ir nuostatas. Toks veiksmas nedaro poveikio teisinėms priemonėms, kurių gali būti imamasi pagal atitinkamus taikomus teisės aktus.

8. Nedarant poveikio kitoms teisinėms priemonėms, jei pažeidimą padaro Parlamento pareigūnai ir kiti Parlamento darbuotojai, kurie dirba frakcijose, taikomos Tarnybos nuostatų VI Antraštinėje dalyje numatytos procedūros ir sankcijos.

9. Nedarant poveikio kitoms teisinėms priemonėms, jei pažeidimą padaro Europos Parlamento nariai, atitinkamai taikoma Parlamento Darbo tvarkos taisyklių 9 straipsnio 2 dalis ir 152, 153 ir 154 straipsniai.

2.2. DECISION OF THE BUREAU OF THE EUROPEAN PARLIAMENT OF 15 APRIL 2013 CONCERNING THE RULES GOVERNING THE TREATMENT OF CONFIDENTIAL INFORMATION BY THE EUROPEAN PARLIAMENT

DECISION OF THE BUREAU OF THE EUROPEAN PARLIAMENT

of 15 April 2013

concerning the rules governing the treatment of confidential information by the European Parliament

2014/C 96/01

THE BUREAU OF THE EUROPEAN PARLIAMENT,

Having regard to Rule 23(12) of the Rules of Procedure of the European Parliament,

Whereas:

(1) In the light of the Framework Agreement on relations between the European Parliament and the European Commission ([1]) signed on 20 October 2010 ('the Framework Agreement') and the Interinstitutional Agreement between the European Parliament and the Council concerning the forwarding to and handling by the European Parliament of classified information held by the Council on matters other than those in the area of the Common Foreign and Security Policy ([2]) signed on 12 March 2014 ('the Interinstitutional Agreement'), it is necessary to lay down specific rules on the treatment of confidential information by the European Parliament.

(2) The Lisbon Treaty assigns new tasks to the European Parliament and, in order to develop Parliament's activities in those areas which require a degree of confidentiality, it is necessary to lay down basic principles, minimum standards of security and appropriate procedures for the treatment by the European Parliament of confidential, including classified, information.

(3) The rules laid down in this Decision aim at ensuring equivalent standards of protection and compatibility with the rules adopted by other institutions, bodies, offices and agencies established by virtue or on the basis of the Treaties or by Member States, in order to facilitate the smooth functioning of the decision-making process of the European Union.

(4) The provisions of this Decision are without prejudice to current and future rules on access to documents adopted in accordance with Article 15 of the Treaty on the Functioning of the European Union (TFEU).

(5) The provisions of this Decision are without prejudice to current and future rules on the protection of personal data adopted in accordance with Article 16 TFEU,

HAS ADOPTED THIS DECISION:

Article 1

Objective

This Decision governs the management and handling of confidential information by the European Parliament, including the creation, reception, forwarding and storage of such information, with a view to the appropriate protection of its confidential nature. It implements, the Interinstitutional Agreement and the Framework Agreement, in particular Annex II thereto.

Article 2

Definitions

For the purposes of this Decision:

(a) **'information'** means any written or oral information, whatever the medium and whoever the author may be;

(b) **'confidential information'** means 'classified information', and non-classified 'other confidential information';

(c) **'classified information'** means 'EU classified information' and 'equivalent classified information';

(d) **'EU classified information' (EUCI)** means any information and material, classified as 'TRÈS SECRET UE/EU TOP SECRET', 'SECRET UE/EU SECRET', 'CONFIDENTIEL UE/EU CONFIDENTIAL' or 'RESTREINT UE/EU RESTRICTED', unauthorised disclosure of which could cause varying degrees of prejudice to Union interests or to those of one or more of its Member States, whether or not such information originates within the institutions, bodies, offices or agencies established by virtue or on the basis of the Treaties. In this regard, information and material classified at the level:

– **'TRÈS SECRET UE/EU TOP SECRET'** is information and material the unauthorised disclosure of which could cause exceptionally grave prejudice to the essential interests of the Union or of one or more of the Member States;

– **'SECRET UE/EU SECRET'** is information and material the unauthorised disclosure of which could seriously harm the essential interests of the Union or of one or more of the Member States;

– **'CONFIDENTIEL UE/EU CONFIDENTIAL'** is information and material the unauthorised disclosure of which could harm the essential interests of the Union or of one or more of the Member States;

– 'RESTREINT UE/EU RESTRICTED' is information and material the unauthorised disclosure of which could be disadvantageous to the interests of the Union or of one or more of the Member States;

(e) **'equivalent classified information'** means classified information issued by Member States, third States or international organisations which bears a security classification marking equivalent to one of the security classification markings used for EUCI and which has been forwarded to the European Parliament by the Council or the Commission;

(f) **'other confidential information'** means any other non-classified confidential information, including information covered by data protection rules or by the obligation of professional secrecy, created in the European Parliament or forwarded to the European Parliament by other institutions, bodies, offices and agencies established by virtue or on the basis of the Treaties or by Member States;

(g) **'document'** means any recorded information, regardless of its physical form or characteristics;

(h) **'material'** means any document or item of machinery or equipment, either manufactured or in the process of manufacture;

(i) **'need to know'** means the need of a person to have access to confidential information in order to be able to perform an official function or a task;

(j) **'authorisation'** means a decision adopted by the President, if it concerns Members of the European Parliament, or by the Secretary-General, if it concerns officials of the European Parliament and other European Parliament employees working for political groups, to grant an individual access to classified information up to a specific level, on the basis of a positive result of a security screening (vetting) carried out by a national authority under national law and pursuant to the provisions laid down in Annex I, Part 2;

(k) **'downgrading'** means a reduction in the level of classification;

(l) **'declassification'** means the removal of any classification;

(m) **'marking'** means a sign affixed to 'other confidential information' intended to identify predefined specific instructions about its handling or the field covered by a given document. It may also be affixed to classified information, in order to impose additional requirements for its handling;

(n) **'unmarking'** means the removal of any marking;

(o) **'originator'** means the duly authorised author of confidential information;

(p) **'security notices'** means the implementing measures laid down in Annex II;

(q) **'handling instructions'** means technical instructions issued to the European Parliament's services concerning the management of confidential information.

Article 3

Basic principles and minimum standards

1. The treatment of confidential information by the European Parliament shall follow the basic principles and minimum standards laid down in Annex I, Part 1.

2. The European Parliament shall set up an information security management system (ISMS) in accordance with those basic principles and minimum standards. The ISMS shall consist of the security notices, the handling instructions and the relevant Rules of Procedure. It shall aim at facilitating parliamentary and administrative work, while ensuring the protection of any confidential information processed by the European Parliament, in full respect of the rules established by the originator of such information as laid down in the security notices.

The processing of confidential information by means of automated communication and information systems (CIS) of the European Parliament shall be implemented in accordance with the concept of information assurance (IA), as provided for in security notice 3.

3. Members of the European Parliament may consult classified information up to and including the level RESTREINT UE/EU RESTRICTED without security clearance.

4. Where the information concerned is classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL or its equivalent, access shall be granted to those Members of the European Parliament who have been authorised by the President pursuant to paragraph 5 or after having signed a solemn declaration of non-disclosure of the content of that information to third persons, of compliance with the obligation to protect information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL and of acknowledgement of the consequences of any failure to do so.

5. Where the information concerned is classified at the level SECRET UE/EU SECRET or TRÈS SECRET/EU TOP SECRET or its equivalent, access shall be granted to those Members of the European Parliament who are authorised by the President after:

(a) they have been security-cleared in accordance with Annex I, Part 2, of this Decision, or

(b) a notification has been received from a competent national authority that the Members concerned are duly authorised by virtue of their functions in accordance with national law.

6. Before being granted access to classified information, Members of the European Parliament shall be briefed on, and shall acknowledge, their responsibilities regarding the protection of such information in accordance with Annex I. They shall also be briefed on the means of ensuring such protection.

7. Officials of the European Parliament and other European Parliament employees working for political groups may consult confidential information if they have an established 'need to know', and may consult classified information above the level RESTREINT UE/EU RESTRICTED if they hold the appropriate level of security clearance. Access to classified information shall be granted only if they have been briefed on, and received written instructions concerning, their responsibilities regarding the protection of such information, as well as the means of ensuring such protection, and if they have signed a declaration acknowledging receipt of those instructions and undertaking to comply with them in accordance with the current rules.

Article 4

Creation of confidential information and administrative handling by the European Parliament

1. The President of the European Parliament, the chairs of the parliamentary committees concerned and the Secretary-General and/or any person duly authorised by him/her in writing may originate confidential information and/or classify information as provided for in the security notices.

2. When creating classified information, the originator shall apply the appropriate level of classification in line with the international standards and definitions set out in Annex I. The originator shall also determine, as a general rule, the addressees who are to be authorised to consult the information commensurate to the level of classification. This information shall be communicated to the Classified Information Unit (CIU) when the document is deposited with the CIU.

3. 'Other confidential information' covered by professional secrecy

shall be dealt with in accordance with Annexes I and II and the handling instructions.

Article 5

Reception of confidential information by the European Parliament

1. Confidential information received by the European Parliament shall be communicated as follows:

(a) information classified at the level RESTREINT UE/EU RESTRICTED or its equivalent and 'other confidential information': to the secretariat of the parliamentary body/office-holder which submitted the request therefor, or directly to the CIU;

(b) information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET or its equivalent: to the CIU.

2. The registration, storage and traceability of confidential information shall be dealt with, as the case may be, either by the secretariat of the parliamentary body/office-holder who received the information or by the CIU.

3. The agreed arrangements to be established by common accord with a view to preserving the confidentiality of the information, in the case of confidential information communicated by the Commission pursuant to point 3.2 of Annex II to the Framework Agreement, or in the case of classified information forwarded by the Council pursuant to Article 5(4) of the Interinstitutional Agreement, shall be deposited, together with the confidential information, at the secretariat of the parliamentary body/office-holder or at the CIU, as the case may be.

4. The arrangements referred to in paragraph 3 may also be applied mutatis mutandis for the communication of confidential information by other institutions, bodies, offices and agencies established by virtue or on the basis of the Treaties or by Member States.

5. In order to ensure a level of protection commensurate with the level of classification TRÈS SECRET UE/EU TOP SECRET or its equivalent, the Conference of Presidents shall set up an oversight committee. Information classified at the level TRÈS SECRET UE/EU TOP SECRET or its equivalent shall be communicated to the European Parliament

subject to further arrangements, to be agreed between the European Parliament and the Union Institution from whom the information is received.

Article 6

Communication of classified information by the European Parliament to third parties

The European Parliament may, subject to the prior written consent of the originator or the Union Institution, which has communicated the classified information to the European Parliament, as the case may be, forward such classified information to third parties, on condition that they ensure that, when such information is handled, rules equivalent to those laid down in this Decision are respected within their services and premises.

Article 7

Secure facilities

1. For the purposes of the management of confidential information, the European Parliament shall establish a Secure Area and Secure Reading Rooms.

2. The Secure Area shall provide facilities for the registration, consultation, archiving, transmission and handling of classified information. It shall comprise, inter alia, a reading room and a meeting room for the consultation of classified information and shall be managed by the CIU.

3. Outside the Secure Area, Secure Reading Rooms may be created, in order to allow for the consultation of information classified at the level RESTREINT UE/EU RESTRICTED or its equivalent, and of 'other confidential information'. Those Secure Reading Rooms shall be managed by the competent services of the secretariat of the parliamentary body/office-holder or by the CIU, as the case may be. They shall not contain photocopying machines, telephones, fax facilities, scanners or any other technical equipment for the reproduction or transmission of documents.

Article 8

Registration, handling and storage of confidential information

1. Information classified at the level RESTREINT UE/EU RESTRICTED or its equivalent and 'other confidential information' shall be registered and stored by the competent services of the secretariat of the parliamentary body/office-holder or by the CIU, depending on who received the information.

2. The following conditions shall apply to the handling of information classified at the level RESTREINT EU/EU RESTRICTED or its equivalent and 'other confidential information':

(a) documents shall be handed over in person to the head of the secretariat, who shall register them and provide an acknowledgement of receipt;

(b) when not actually being used, such documents shall be kept in a locked location, under the responsibility of the secretariat;

(c) in no case may the information be saved on another medium or transmitted to any person. Such documents may only be duplicated by means of appropriately accredited equipment as defined in the security notices;

(d) access to such information shall be restricted to those designated by the originator or by the Union Institution which communicated the information to the European Parliament, in accordance with the arrangements referred to in Article 4(2) or Article 5(3), (4) and (5);

(e) the secretariat of the parliamentary body/office-holder shall keep a record of the persons who have consulted the information, and of the date and time of such consultation, and shall transmit the record to the CIU at the time when the information is deposited with the CIU.

3. Information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET, or its equivalent shall be registered, handled and stored by the CIU in the Secure Area, in accordance with the specific level of classification and as defined in the security notices.

4. In the event of a breach of the rules set out in paragraghs 1 to 3, the responsible official of the secretariat of the parliamentary body/office-holder or of the CIU, as the case may be, shall inform the Secretary-General, who shall refer the matter to the President if a Member of the European Parliament is concerned.

Article 9

Access to secure facilities

1. Only the following persons shall have access to the Secure Area:
(a) persons who, pursuant to Article 3(4) to (7), are authorised to consult the information held there and who have submitted an application pursuant to Article 10(1);
(b) persons who, pursuant to Article 4(1), are authorised to create classified information and who have submitted an application pursuant to Article 10(1);
(c) the European Parliament's officials of the CIU;
(d) the European Parliament officials responsible for managing the CIS;
(e) European Parliament officials responsible for security and fire safety, when necessary;
(f) cleaning staff, but only in the presence of, and under close surveillance by, an official of the CIU.

2. The CIU may deny access to the Secure Area to any person not authorised to enter. Any objection challenging such a denial of access shall be submitted to the President, in the case of a request for access by a Member of the European Parliament, and to the Secretary-General in other cases.

3. The Secretary-General may authorise a meeting for a limited number of persons in the meeting room located within the Secure Area.

4. Only the following persons shall have access to a Secure Reading Room:
(a) Members of the European Parliament, officials of the European Parliament and other European Parliament employees working for political groups, duly identified for the purposes of consultation or creation of confidential information;
(b) the European Parliament officials responsible for managing the CIS, officials of the secretariat of the parliamentary body/office-holder which received the information, and officials of the CIU;
(c) where necessary, European Parliament officials responsible for security and fire safety;
(d) cleaning staff, but only in the presence of, and under close surveillance by, an official working in the secretariat of the parliamentary body/office-holder or in the CIU, as the case may be.

5. The competent secretariat of the parliamentary body/office-holder or the CIU, as the case may be, may deny access to a Secure Reading

Room to any person not authorised to enter. Any objection challenging such a denial of access shall be submitted to the President, in the case of a request for access by a Member of the European Parliament, and to the Secretary-General in other cases.

Article 10

Consultation or creation of confidential information in secure facilities

1. Any person wishing to consult or create confidential information in the Secure Area shall communicate his or her name in advance to the CIU. The CIU shall check the identity of that person and verify whether he or she is permitted, in accordance with Article 3(3) to (7), Article 4(1) or Article 5(3), (4) and (5) to consult or create confidential information.

2. Any person wishing, in accordance with Article 3(3) and (7), to consult confidential information classified at the level RESTREINT EU/EU RESTRICTED or its equivalent or 'other confidential information' in a Secure Reading Room shall communicate his or her name in advance to the competent services of the secretariat of the parliamentary body/office-holder or to the CIU.

3. Save in exceptional circumstances (e.g. where numerous requests for consultation are submitted within a short period of time), only one person at a time shall be authorised to consult confidential information in a secure facility, in the presence of an official of the secretariat of the parliamentary body/office-holder or of the CIU.

4. During the consultation process, contact with the exterior (including by means of telephones or other technological devices), the taking of notes and the photocopying or photographing of the confidential information consulted shall be prohibited.

5. Before authorising a person to leave the secure facility, the official of the secretariat of the parliamentary body/office-holder or of CIU shall check that the confidential information consulted is still present, intact and complete.

6. In the event of a breach of the rules set out above, the official of the secretariat of the parliamentary body/office-holder or of the CIU shall inform the Secretary-General, who shall refer the matter to the President where a Member of the European Parliament is concerned.

Article 11

Minimum standards for consultation of confidential information at a meeting in camera outside secure facilities

1. Information classified at the level RESTREINT UE/EU RESTRICTED or its equivalent and 'other confidential information' may be consulted by members of parliamentary committees or of other political and administrative bodies of the European Parliament at a meeting in camera outside the secure facilities.

2. In the circumstances provided for in paragraph 1, the secretariat of the parliamentary body/office-holder responsible for the meeting shall ensure that the following conditions are complied with:

(a) only the persons designated by the chair of the competent committee or body to participate in the meeting are allowed to enter the meeting room;
(b) all documents are numbered, distributed at the beginning of the meeting and collected again at the end, and no notes of those documents and no photocopies or photographs thereof are taken;
(c) the minutes of the meeting make no mention of the content of the discussion of the information considered. Only the relevant decision, if any, may be recorded;
(d) confidential information provided orally to recipients in the European Parliament is subject to a level of protection equivalent to that applied to confidential information in written form;
(e) no additional stock of documents is held in meeting rooms;
(f) copies of documents are distributed only in the requisite numbers to participants and interpreters at the start of the meeting;
(g) the classification/marking status of the documents is made clear by the chair of the meeting at the start of the meeting;
(h) participants do not remove documents from the meeting room;
(i) all copies of documents are collected and accounted for at the end of the meeting by the secretariat of the parliamentary body/office-holder; and
(j) no electronic communication devices or other electronic devices are taken into the meeting room where the confidential information in question is consulted or discussed.

3. Where, in accordance with the exceptions laid down in point 3.2.2 of Annex II to the Framework Agreement and in Article 6(5) of

the Interinstitutional Agreement, information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL or its equivalent is discussed at a meeting held in camera, the secretariat of the parliamentary body/office-holder responsible for the meeting shall, in addition to ensuring compliance with the provisions laid down in paragraph 2, ensure that the persons designated to participate in the meeting comply with the requirements of Article 3(4) and (7).

4. In the case provided for in paragraph 3, the CIU shall provide to the secretariat of the parliamentary body/office-holder-responsible for the meeting in camera the requisite number of copies of the documents to be discussed, which shall be returned to the CIU after the meeting.

Article 12

Archiving of confidential information

1. Secure archiving facilities shall be provided within the Secure Area. The CIU shall be responsible for managing the secure archive in accordance with standard archiving criteria.

2. Classified information definitively deposited with the CIU, and information classified at the level RESTREINT UE/EU RESTRICTED or its equivalent which is deposited with the secretariat of the parliamentary body/office-holder, shall be transferred to the secure archive in the Secure Area six months after it was last consulted and, at the latest, one year after it was deposited. 'Other confidential information' shall be archived, unless deposited with the CIU, by the secretariat of the parliamentary body/office-holder concerned, in accordance with the general rules on document management.

3. Confidential information held in the secure archive may be consulted subject to the following conditions:

(a) only those persons identified by name, by function or by office in the accompanying document drawn up when the confidential information was deposited shall be authorised to consult that information;

(b) the application to consult confidential information shall be submitted to the CIU, which shall transfer the document in question to the Secure Reading Room; and

(c) the procedures and conditions governing the consultation of confidential information set out in Article 10 shall apply.

Article 13

Downgrading, declassification and unmarking of confidential information

1. Confidential information may be downgraded, declassified or unmarked only with the prior consent of the originator, and, if necessary, after discussion with other interested parties.

2. Downgrading or declassification shall be confirmed in writing. The originator shall be responsible for informing its addressees of the change, and they in turn shall be responsible for informing any subsequent addressees to whom they have sent or copied the document, of the change. If possible, originators shall specify on classified documents a date, period or event when the contents may be downgraded or declassified. Otherwise, they shall keep the documents under review every five years, at the latest, in order to ensure that the original classification is necessary.

3. Confidential information held in the secure archives shall be examined in good time, and by no later than the 25th anniversary of its creation, in order to determine whether or not it should be declassified, downgraded or unmarked. The examination and publication of such information shall take place in accordance with the provisions of Council Regulation (EEC, Euratom) No 354/83 of 1 February 1983 concerning the opening to the public of the historical archives of the European Economic Community and the European Atomic Energy Community ([3]). Declassification shall be effected by the originator of the classified information or the service currently responsible in accordance with Annex I, Part 1, Section 10.

4. Following declassification, formerly classified information held in the secure archive shall be transferred to the historical archives of the European Parliament for permanent preservation and further treatment under the applicable rules.

5. Following unmarking, formerly ‘other confidential information’ shall be subject to the European Parliament rules on document management.

Article 14

Breaches of security, loss or compromise of confidential information

1. A breach of confidentiality in general, and of this Decision in particular, shall in the case of Members of the European Parliament entail the application of the relevant provisions concerning penalties set out in the European Parliament's Rules of Procedure.

2. A breach committed by a member of staff of the European Parliament shall lead to the application of the procedures and penalties provided for by, respectively, the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Union, laid down in Regulation (EEC, Euratom, ECSC) No 259/68 ([4]) ('the Staff Regulations').

3. The President and/or the Secretary-General, as the case may be, shall organise any necessary investigations in the event of a breach as defined in security notice 6.

4. If the confidential information was communicated to the European Parliament by a Union Institution or by a Member State, the President and/or the Secretary-General, as the case may be, shall inform the Union Institution or Member State concerned of any proven or suspected loss or compromise of classified information, of the results of the investigation and of the measures taken to prevent a recurrence.

Article 15

Adaptation of this Decision and its implementing rules and annual reporting on the application of this Decision

1. The Secretary-General shall propose any necessary adaptation of this Decision and the annexes implementing it and shall forward those proposals to the Bureau for decision.

2. The Secretary-General shall be responsible for the implementation of this Decision by the European Parliament's services and shall issue the handling instructions on matters covered by the ISMS in accordance with the principles laid down by this Decision.

3. The Secretary-General shall submit an annual report to the Bureau

on the application of this Decision.

Article 16

Transitional and final provisions

1. Non-classified information held in the CIU or in any other archive of the European Parliament which is considered as confidential and dated before 1 April 2014 shall be deemed, for the purpose of this Decision, to constitute 'other confidential information'. Its originator may at any time reconsider the level of its confidentiality.

2. By way of derogation from point (a) of Article 5(1) and from Article 8(1) of this Decision, for a period of twelve months from 1 April 2014, information provided by the Council pursuant to the Interinstitutional Agreement which is classified at the level RESTREINT UE/EU RESTRICTED or its equivalent shall be deposited with, registered by and stored in the CIU. Such information may be consulted in accordance with points (a) and (c) of Article 4(2) and with Article 5(4) of the Interinstitutional Agreement.

3. The decision of the Bureau of 6 June 2011 concerning the rules governing the treatment of confidential information by the European Parliament is repealed.

Article 17

Entry into force

This Decision shall enter into force on the day of its publication in the *Official Journal of the European Union*.

([1]) OJ L 304, 20.11.2010, p. 47.

([2]) OJ C 95, 1.4.2014, p. 1.

([3]) OJ L 43, 15.2.1983, p. 1.

([4]) OJ L 56, 4.3.1968, p. 1.

ANNEX I

Part 1

BASIC PRINCIPLES AND MINIMUM STANDARDS OF SECURITY FOR THE PROTECTION OF CONFIDENTIAL INFORMATION

1. INTRODUCTION

These provisions set out the basic principles and minimum standards of security for the protection of confidential information to be respected and/or complied with by the European Parliament in all its places of employment, including by all recipients of, classified information and 'other confidential information' so that security is safeguarded and all persons concerned may be assured that a common standard of protection is established. These provisions are supplemented by the security notices contained in Annex II and by other provisions governing the treatment of confidential information by parliamentary committees and other parliamentary bodies/office-holders.

2. BASIC PRINCIPLES

The European Parliament's security policy forms an integral part of its general internal management policy and is thus based on the principles governing that general policy. Those principles include legality, transparency, accountability, subsidiarity and proportionality.

Legality entails the need to remain strictly within the legal framework in the performance of security functions, and to conform to the applicable legal requirements. Furthermore, responsibilities in the field of security must be based on proper legal provisions. The provisions of the Staff Regulations, in particular Article 17 thereof on the obligation of staff to refrain from any unauthorised disclosure of information received in the line of duty and Title VI thereof on disciplinary measures, are fully applicable. Finally, breaches of security within the responsibility of the European Parliament shall be dealt with in a manner consistent with its

Rules of Procedure and its policy on disciplinary measures.

Transparency entails the need for clarity regarding all security rules and provisions, for a balance between the different services and the different domains (physical security as compared to the protection of information, etc.), and for a consistent and structured security awareness policy. Moreover, clear written guidelines are necessary for the implementation of security measures.

Accountability means that responsibilities in the field of security must be clearly defined. Moreover, it entails the need regularly to monitor whether those responsibilities have been properly fulfilled.

Subsidiarity means that security must be organised at the lowest possible level and as closely as possible to the European Parliament's Directorates-General and services.

Proportionality means that security activities must be strictly limited to those which are absolutely necessary and that security measures must be proportional to the interests to be protected as well as to the actual or potential threat to those interests, so as to enable those interests to be defended in a manner ensuring the least possible disruption.

3. FOUNDATIONS OF INFORMATION SECURITY

The foundations of sound information security are:

(a) proper communication and information systems (CIS). These fall within the responsibility of the European Parliament's Security Authority (as defined in security notice 1);

(b) within the European Parliament, the Information Assurance Authority (as defined in security notice 1) responsible for working with the Security Authority to provide information and advice on technical threats to CIS and the means of protecting against those threats;

(c) close cooperation between the European Parliament's responsible services and the security services of the other Union institutions;

4. PRINCIPLES OF INFORMATION SECURITY

4.1. *Objectives*

The principle objectives of information security are as follows:

(a) to safeguard confidential information against espionage, compromise or unauthorised disclosure;

(b) to safeguard classified information handled in communications and information systems and networks against threats to its confidentiality, integrity and availability;

(c) to safeguard European Parliament premises housing classified information against sabotage and malicious wilful damage;

(d) in the event of a security failure, to assess the damage caused, limit the consequences, conduct security investigations and adopt any necessary remedial measures.

4.2. *Classification*

4.2.1. Where confidentiality is concerned, care and experience are needed in the selection of the information and material to be protected as well as in assessing the degree of protection required. It is essential that the degree of protection should correspond to the sensitivity, in terms of security, of the individual item of information or material to be safeguarded. In order to ensure the smooth flow of information, both over-classification and under-classification shall be avoided.

4.2.2. The classification system is the instrument for putting into effect the principles set out in this section. A similar classification system shall be followed in planning and organising ways to counter espionage, sabotage, terrorism and other threats, in order to ensure maximum protection for the most important premises housing classified information and the most sensitive points within those premises.

4.2.3. Responsibility for classifying information lies solely with the originator of the information concerned.

4.2.4. The level of classification may be based solely on the content of the information concerned.

4.2.5. Where several items of information are grouped together, their classification shall be at least as high as the highest classification level assigned to one of its individual items. However, a collection of

information may be assigned a higher classification than its constituent parts.

4.2.6. Classifications shall be assigned only when necessary and for as long as necessary.

4.3. *Aims of security measures*

The security measures shall:

(a) extend to all persons having access to classified information, media carrying classified information and 'other confidential information', as well as all premises containing such information and important installations;

(b) be designed in such a way as to identify persons whose position (in terms of access, relationships or otherwise) might jeopardise the security of such information and of important installations housing such information, and provide for their exclusion or removal;

(c) prevent unauthorised persons from having access to such information or to installations containing it;

(d) ensure that such information is disseminated solely on the basis of the need-to-know principle, which is fundamental to all aspects of security;

(e) ensure the integrity (by preventing corruption, unauthorised alteration or unauthorised deletion) and the availability (to those needing and authorised to have access thereto) of confidential information, especially where it is stored, processed or transmitted in electromagnetic form.

5. COMMON MINIMUM STANDARDS

The European Parliament shall ensure that common minimum standards of security are observed by all recipients of classified information, both inside the institution and under its competence, namely all its services and contractors, so that such information can be passed on in the confidence that it will be handled with equal care. Such minimum standards shall include criteria for the security clearance of officials of the European Parliament and other Parliament employees working for political groups, and procedures for the protection of confidential information.

The European Parliament shall allow third parties access to such information only when such third parties guarantee that it is handled in

accordance with provisions that are at least strictly equivalent to these common minimum standards.

Such common minimum standards shall also be applied when, pursuant to a contract or grant, the European Parliament entrusts to industrial or other entities tasks involving confidential information.

6. SECURITY AS REGARDS OFFICIALS OF THE EUROPEAN PARLIAMENT AND OTHER PARLIAMENT EMPLOYEES WORKING FOR POLITICAL GROUPS

6.1. *Security instructions as regards officials of the European Parliament and other Parliament employees working for political groups*

Officials of the European Parliament and other Parliament employees working for political groups in positions where they could have access to classified information shall be given thorough instructions, both on taking up their duties and at regular intervals thereafter, on the need for security and the procedures involved. Such persons shall be required to confirm in writing that they have read and fully understand the applicable security provisions.

6.2. *Management responsibilities*

It must be part of the duties of managers to know which of their staff are engaged in work on classified information or have access to secure communication or information systems, and to record and report any incidents or apparent vulnerabilities which are likely to affect security.

6.3. *Security status of officials of the European Parliament and other Parliament employees working for political groups*

Procedures shall be established to ensure that, when adverse information becomes known concerning an official of the European Parliament or other Parliament employee working for a political group,

steps are taken to determine whether that individual's work brings him or her into contact with classified information or whether he or she has access to secure communication or information systems, and that the European Parliament's responsible service is informed. If the competent National Security Authority indicates that such an individual constitutes a security risk, he or she shall be barred or removed from assignments where he or she might endanger security.

7. PHYSICAL SECURITY

'Physical security' means the application of physical and technical protective measures to prevent unauthorised access to classified information.

7.1. *Need for protection*

The degree of physical security measures to be applied to ensure the protection of classified information shall be proportionate to the classification and volume of, and the threat to, the information and material held. All holders of classified information shall follow uniform practices regarding classification of such information and must meet common standards of protection regarding the custody, transmission and disposal of information and material requiring protection.

7.2. *Checking*

Before leaving areas containing classified information unattended, persons having custody thereof shall ensure that it is securely stored and that all security devices have been activated (locks, alarms, etc.). Further independent checks shall be carried out after working hours.

7.3. *Security of buildings*

Buildings housing classified information or secure communication and information systems shall be protected against unauthorised access.

The nature of the protection afforded to classified information, e.g. barring of windows, locks for doors, guards at entrances, automated access control systems, security checks and patrols, alarm systems,

intrusion detection systems and guard dogs, shall depend on:

(a) the classification, volume and location within the building of the information and material to be protected;

(b) the quality of the security containers for the information and material concerned; and

(c) the physical nature and location of the building.

The nature of the protection afforded to communication and information systems shall depend on an assessment of the value of the assets at stake and of the potential damage if security were to be compromised, on the physical nature and location of the building in which the system is housed, and on the location of that system within the building.

7.4. *Contingency plans*

Detailed plans shall be in place in advance to ensure the protection of classified information in the event of an emergency.

8. SECURITY DESIGNATORS, MARKINGS, AFFIXING AND CLASSIFICATION MANAGEMENT

8.1. *Security designators*

No classifications other than those defined in point (d) of Article 2 of this Decision are permitted.

An agreed security designator may be used to set limits to the validity of a classification (for classified information signifying automatic downgrading or declassification).

Security designators shall only be used in combination with a classification.

Security designators are further regulated in security notice 2 and defined in the handling instructions.

8.2. *Markings*

A marking is used to specify predefined specific instructions about the handling of confidential information. Markings may also indicate the

field covered by a given document, a particular distribution on a need-to-know basis, or (for non-classified information) to signify the end of an embargo.

A marking is not a classification and shall not be used in lieu of one.

Markings are further regulated in security notice 2 and defined in the handling instructions.

8.3. *Affixing of classifications and of security designators*

Affixing of classifications and security designators and markings shall be done in accordance with security notice 2, section E, and the handling instructions.

8.4. *Classification management*

8.4.1 *General*

Information shall be classified only when necessary. The classification shall be clearly and correctly indicated, and shall be maintained only as long as the information requires protection.

The responsibility for classifying information and for any subsequent downgrading or declassification rests solely with the originator.

Officials of the European Parliament shall classify, downgrade or declassify information on instructions from, or pursuant to a delegation from, the Secretary-General.

The detailed procedures for the treatment of classified documents shall be so framed as to ensure that they are afforded protection appropriate to the information which they contain.

The number of persons authorised to originate information classified at the level TRÈS SECRET UE/EU TOP SECRET shall be kept to a minimum, and their names shall be recorded on a list drawn up by the CIU.

8.4.2 *Application of classification*

The classification of a document shall be determined by the level of

sensitivity of its contents in accordance with the definitions contained in point (d) of Article 2. It is important that classifications be assigned correctly and used sparingly.

The classification of a letter or note containing enclosures shall be at least as high as the highest classification assigned to one of its enclosures. The originator shall indicate clearly the level at which the letter or note should be classified when detached from its enclosures.

The originator of a document that is to be given a classification shall follow the rules set out above and shall avoid over-classification or under-classification.

Individual pages, paragraphs, sections, annexes, appendices, attachments and enclosures of a given document may require different classifications and shall be classified accordingly. The classification of the document as a whole shall be that of its most highly classified part.

9. INSPECTIONS

Periodic internal inspections of security arrangements for the protection of classified information shall be carried out by the European Parliament's Directorate for Security and Risk Assessment, which may request assistance from the Security Authorities of the Council or of the Commission.

The Security Authorities and competent services of the Union Institutions may carry out, as part of an agreed process initiated by either side, peer evaluations of the security arrangements for the protection of classified information exchanged under the relevant interinstitutional agreements.

10. DECLASSIFICATION AND UNMARKING PROCEDURES

10.1. The CIU shall examine confidential information contained in its Register and seek the consent of the originator to the declassification or unmarking of a document by no later than the 25th anniversary of its creation. Documents not declassified or unmarked at the first examination shall be re-examined periodically and at least every five years. In addition to being applied to documents actually located in the secure archives in the Secure Area and duly classified, the unmarking

process may also cover other confidential information held either in the parliamentary body/office or in the service in charge of the Parliament's historical archives.

10.2. The decision with regard to the declassification or unmarking of a document shall, as a general rule, be taken solely by the originator or, exceptionally, in cooperation with the parliamentary body/office-holder of such information, before the information which it contains is transferred to the service in charge of the Parliament's historical archives. Classified information may only be declassified or unmarked with the prior written consent of the originator. In the case of 'other confidential information', the secretariat of the parliamentary body/office-holder of such information shall, in cooperation with the originator, decide whether the document can be unmarked.

10.3. On behalf of the originator, the CIU shall be responsible for informing the addressees of the document of the change to the classification or marking, and they in turn shall be responsible for informing any subsequent addressees to whom they have sent or copied the document.

10.4. Declassification shall not affect any security designators or markings which may appear on the document.

10.5. In the case of declassification, the original classification at the top and bottom of every page shall be crossed out. The first (cover) page of the document shall be stamped and completed with the reference of the CIU. In the case of unmarking, the original marking at the top of every page shall be crossed out.

10.6. The text of the declassified or unmarked document shall be attached to the electronic fiche or equivalent system where it has been registered.

10.7. In the case of documents covered by the exception relating to privacy and the integrity of the individual or commercial interests of a natural or legal person, and in the case of sensitive documents, Article 2 of Regulation (EEC, Euratom) No 354/83 shall apply.

10.8. In addition to the provisions of points 10.1 to 10.7, the following rules shall apply:

(a) as regards third-party documents, the CIU shall consult the third party concerned before proceeding to carry out the declassification or unmarking;

(b) as regards the exception relating to privacy and the integrity of the individual, the declassification or unmarking procedure shall take into account, in particular, the agreement of the person concerned or, as the case may be, the impossibility of identifying the person concerned;

(c) as regards the exception relating to commercial interests of a natural or legal person, the person concerned may be notified via publication in the *Official Journal of the European Union* and given four weeks from the date of that publication in which to submit remarks.

Part 2

SECURITY CLEARANCE PROCEDURE

11. SECURITY CLEARANCE PROCEDURE FOR MEMBERS OF THE EUROPEAN PARLIAMENT

11.1. In order to have access to information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL or its equivalent, Members of the European Parliament shall have been authorised either in accordance with the procedure referred to in points 11.3 and 11.4 of this Annex or on the basis of a solemn declaration of non-disclosure pursuant to Article 3(4) of this Decision.

11.2. In order to have access to information classified at the level SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET or its equivalent, Members of the European Parliament shall have been authorised in accordance with the procedure referred to in points 11.3 and 11.14.

11.3. Authorisation shall be granted only to Members of the European Parliament who have undergone security screening by the competent national authorities of the Member States in accordance with the procedure referred to in points 11.9 to 11.14. The President shall be responsible for granting the authorisation for Members.

11.4. The President may grant written authorisation after obtaining the opinion of the competent national authorities of the Member States on the basis of security screening carried out in accordance with points

11.8 to 11.13.

11.5. The European Parliament's Directorate for Security and Risk Assessment shall maintain an up-to-date list of all Members of the European Parliament who have been granted authorisation, including provisional authorisation within the meaning of point 11.15.

11.6. Authorisation shall be valid for a period of five years or for the duration of the tasks in respect of which it was granted, whichever is the shorter. It may be renewed in accordance with the procedure laid down in point 11.4.

11.7. Authorisation shall be withdrawn by the President where he/she considers that there are justified grounds for such withdrawal. Any decision to withdraw authorisation shall be notified to the Member of the European Parliament concerned, who may ask to be heard by the President before the withdrawal takes effect, and to the competent national authority.

11.8. Security screening shall be carried out with the assistance of the Member of the European Parliament concerned and at the request of the President. The competent national authority for screening shall be that of the Member State of which the Member concerned is a national.

11.9. As part of the screening procedure, the Member of the European Parliament concerned shall be required to complete a personal information form.

11.10. The President shall specify in his/her request to the competent national authority the level of classified information to be made available to the Member of the European Parliament concerned, so that it may carry out the screening process.

11.11. The entire security-screening process carried out by the competent national authority, together with the results obtained, shall be in accordance with the relevant rules and regulations in force in the Member State concerned, including those concerning appeals.

11.12. Where the competent national authority gives a positive opinion, the President may grant the Member of the European Parliament concerned authorisation.

11.13. A negative opinion by the competent national authority shall be notified to the Member of the European Parliament concerned, who may ask to be heard by the President. Should he/she consider it

necessary, the President may ask the competent national authority for further clarification. If the negative opinion is confirmed, authorisation shall not be granted.

11.14. All Members of the European Parliament who are granted authorisation within the meaning of point 11.3 shall, at the time when the authorisation is granted and at regular intervals thereafter, receive any necessary guidelines concerning the protection of classified information and the means of ensuring such protection. Such Members shall sign a declaration acknowledging receipt of those guidelines.

11.15. In exceptional circumstances, the President may, after notifying the competent national authority and provided that no reaction is received from that authority within one month, grant provisional authorisation to a Member of the European Parliament for a period not exceeding six months, pending the outcome of the screening referred to in point 11.11. Provisional authorisations thus granted shall not give access to information classified at the level TRÈS SECRET UE/EU TOP SECRET or its equivalent.

12. SECURITY CLEARANCE PROCEDURE FOR OFFICIALS OF THE EUROPEAN PARLIAMENT AND OTHER PARLIAMENT EMPLOYEES WORKING FOR POLITICAL GROUPS

12.1. Only officials of the European Parliament and other Parliament employees working for political groups who, by reason of their duties and the requirements of the service, need to have knowledge of, or to use, classified information may have access thereto.

12.2. In order to have access to information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET, or TRÈS SECRET UE/EU TOP SECRET, or its equivalent, the officials of the European Parliament and other Parliament employees working for political groups concerned shall have been authorised in accordance with the procedure laid down in points 12.3 and 12.4.

12.3. Authorisation shall be granted only to the persons referred to in point 12.1 who have undergone security screening by the competent national authorities of the Member States in accordance with the procedure referred to in points 12.9 to 12.14. The Secretary-General shall

be responsible for granting the authorisation for officials of the European Parliament and other Parliament employees working for political groups.

12.4. The Secretary-General may grant written authorisation after obtaining the opinion of the competent national authorities of the Member States on the basis of security screening carried out in accordance with points 12.8 to 12.13.

12.5. The European Parliament's Directorate for Security and Risk Assessment shall maintain an up-to-date list of all posts requiring a security clearance, as provided by the relevant European Parliament services, and of all persons who have been granted authorisation, including provisional authorisation within the meaning of point 12.15.

12.6. Authorisation shall be valid for a period of five years or for the duration of the tasks in respect of which it was granted, whichever is the shorter. It may be renewed in accordance with the procedure referred to in point 12.4.

12.7. Authorisation shall be withdrawn by the Secretary-General where he/she considers that there are justifiable grounds for such withdrawal. Any decision to withdraw authorisation shall be notified to the official of the European Parliament or other Parliament employee working for a political group concerned, who may ask to be heard by the Secretary-General before the withdrawal takes effect, and to the competent national authority.

12.8. Security screening shall be carried out with the assistance of the official of the European Parliament or other Parliament employee working for political groups concerned and at the request of the Secretary-General. The competent national authority for screening shall be that of the Member State of which the person concerned is a national. Where permissible under national laws and regulations, the competent national authorities may conduct investigations in respect of non-nationals who require access to information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET.

12.9. As part of the screening procedure, the official of the European Parliament or other Parliament employee working for a political group concerned shall be required to complete a personal information form.

12.10. The Secretary-General shall specify in his/her request to the competent national authority the level of classified information to

be made available to the official of the European Parliament or other Parliament employee working for political groups concerned, so that it may carry out the screening process and give its opinion as to the level of authorisation appropriate to be granted to that person.

12.11. The entire security-screening process carried out by the competent national authority, together with the results obtained, shall be in accordance with the relevant rules and regulations in force in the Member State concerned, including those concerning appeals.

12.12. Where the competent national authority gives a positive opinion, the Secretary-General may grant the official of the European Parliament or other Parliament employee working for political groups concerned authorisation.

12.13. A negative opinion by the competent national authority shall be notified to the official of the European Parliament or other Parliament employee working for a political group concerned, who may ask to be heard by the Secretary-General. Should he/she consider it necessary, the Secretary-General may ask the competent national authority for further clarification. If the negative opinion is confirmed, authorisation shall not be granted.

12.14. All officials of the European Parliament and other Parliament employees working for political groups who are granted authorisation within the meaning of points 12.4 and 12.5 shall, at the time when the authorisation is granted and at regular intervals thereafter, receive any necessary instructions concerning the protection of classified information and the means of ensuring such protection. Such officials and employees shall sign a declaration acknowledging receipt of those instructions and give an undertaking to obey them.

12.15. In exceptional circumstances, the Secretary-General may, after notifying the competent national authority and provided that no reaction is received from that authority within one month, grant provisional authorisation to an official of the European Parliament or other Parliament employee working for a political group for a period not exceeding six months, pending the outcome of the screening referred to in point 12.11. Provisional authorisations thus granted shall not give access to information classified at the level TRÈS SECRET UE/EU TOP SECRET or its equivalent.

ANNEX II

INTRODUCTION

These provisions lay down the security notices governing and ensuring the secure treatment and management of confidential information by the European Parliament. Those security notices, together with the handling instructions, constitute the European Parliament's information security management system (ISMS) referred to in Article 3(2) of this Decision:

SECURITY NOTICE 1

The organisation of security in the European Parliament for the protection of confidential information

SECURITY NOTICE 2

Management of confidential information

SECURITY NOTICE 3

The processing of confidential information by means of automated communication information systems (CIS)

SECURITY NOTICE 4

Physical security

SECURITY NOTICE 5

Industrial security

SECURITY NOTICE 6

Breaches of security, loss or compromise of confidential information

SECURITY NOTICE 1

THE ORGANISATION OF SECURITY IN THE EUROPEAN PARLIAMENT FOR THE PROTECTION OF CONFIDENTIAL INFORMATION

1. The Secretary-General shall be responsible for the overall and consistent implementation of this Decision.

The Secretary-General shall take all necessary measures to ensure that, for the purposes of handling or storing confidential information, this Decision is applied in Parliament's premises, by Members of the European Parliament, by officials of the European Parliament, by other Parliament employees working for political groups and by contractors.

2. The Secretary-General is the Security Authority (SA). In this capacity, the Secretary-General shall be responsible for:

2.1. coordinating all matters of security relating to Parliament's activities in relation to the protection of confidential information;

2.2. approving the installation of a Secure Area, Secure Reading Rooms and secure equipment;

2.3. implementing decisions authorising, pursuant to Article 6 of this Decision, the transmission of classified information by Parliament to third parties;

2.4. investigating or ordering an investigation into any leakage of confidential information which prima facie has occurred within Parliament, in liaison with the President of the European Parliament, where a Member of the European Parliament is concerned;

2.5. maintaining close contact with the security authorities of other Union Institutions and with National Security Authorities in the Member States with a view to ensuring optimal coordination of security policy related to classified information;

2.6. keeping Parliament's security policy and procedures constantly under review and issuing appropriate recommendations resulting therefrom;

2.7. reporting to the National Security Authority (NSA) which has carried out the security screening procedure, in accordance with Annex I, Part 2, point 11.3, in cases involving any adverse information which may affect that authority.

3. Where a Member of the European Parliament is concerned, the Secretary-General shall discharge his/her responsibilities in close liaison with the President of the European Parliament.

4. In fulfilling his/her responsibilities under paragraphs 2 and 3, the Secretary-General shall be assisted by the Deputy Secretary-General, the Directorate for Security and Risk Assessment, the Directorate for Information Technologies (DIT) and the Classified Information Unit (CIU).

4.1. The Directorate for Security and Risk Assessment shall be responsible for personal protection measures and, in particular, for the security clearance procedure, as laid down in Annex I, Part 2. The Directorate for Security and Risk Assessment shall also:

(a) be the point of contact for the security authorities of the other Union Institutions and for the NSAs, in matters relating to security clearance procedures for Members of the European Parliament, officials of the European Parliament and other Parliament employees working for political groups;
(b) provide the necessary general security briefing on the obligation to protect classified information and on the consequences of any failure to do so;
(c) monitor the operation of the Secure Area and the Secure Reading Rooms within Parliament's premises, in cooperation, where appropriate, with the security services of the other Union Institutions and the NSAs;
(d) audit, in cooperation with the security authorities of the other Union Institutions and the NSAs, the procedures for the management and storage of classified information, the Secure Area and the Secure Reading Rooms within Parliament's premises where classified information is handled;
(e) propose the appropriate handling instructions to the Secretary-General.

4.2. The DIT shall be responsible for handling of confidential information by secure IT systems at the European Parliament.

4.3. The CIU shall be responsible for:

(a) identifying the security needs for the effective protection of confidential information, in close cooperation with the Directorate for Security and Risk Assessment and DIT and with the Security Authorities of the other Union Institutions;

(b) identifying all aspects of the management and storage of confidential information within Parliament, as laid down in the handling instructions;
(c) the operation of the Secure Area;
(d) the management or consultation of confidential information in the Secure Area or in the CIU's Secure Reading Room, in accordance with paragraphs (2) and (3) of Article 7 of this Decision;
(e) the management of the CIU Register;
(f) reporting to the SA any proven or suspected breach of security, loss or compromise relating to confidential information deposited at the CIU and held in the Secure Area or in the CIU Secure Reading Room.

5. Furthermore, the Secretary-General, as SA, shall appoint the following authorities:
(a) a Security Accreditation Authority (SAA);
(b) an Information Assurance Operational Authority (IAOA);
(c) a Crypto Distribution Authority (CDA);
(d) a TEMPEST Authority (TA);
(e) an Information Assurance Authority (IAA).

The exercise of those functions does not require single organisational entities. They shall have separate mandates. However, those functions, and their accompanying responsibilities, may be combined or integrated in the same organisational entity or split into different organisational entities, provided that conflicts of interest and duplication of tasks are avoided.

6. The SAA shall advise on all security matters related to the accreditation of each information technology system and network within Parliament by:
6.1. ensuring that the CIS comply with the relevant security policies and security guidelines, providing a statement of approval for the handling by the CIS of classified information to a defined level of classification in its operational environment and stating the terms and conditions of the accreditation and the criteria under which re-approval is required;
6.2. setting up a security accreditation process, in accordance with the relevant policies, clearly stating the approval conditions for the CIS under its authority;
6.3. drawing up a security accreditation strategy which sets out the degree of detail for the accreditation process commensurate with the level of assurance required;

6.4. examining and approving security-related documentation, including risk management and residual risk statements, security implementation verification documentation and security operating procedures, and ensuring that it complies with Parliament's security rules and policies;

6.5. verifying the implementation of security measures in relation to the CIS by carrying out or sponsoring security assessments, inspections or reviews;

6.6. identifying security requirements (e.g. personnel clearance levels) for sensitive positions in relation to the CIS;

6.7. approving, or where relevant, participating in, the joint approval of the interconnection of a given CIS to other CIS;

6.8. approving the security standards of technical equipment envisaged for the secure handling and protection of classified information;

6.9. ensuring that cryptographic products used within Parliament are included in the list of EU approved products; and

6.10. consulting the system provider, the security actors and representatives of the users with respect to security risk management, in particular the residual risk, and the terms and conditions of the approval statement.

7. The IAOA shall be responsible for:

7.1. developing security documentation in line with security policies and security guidelines, in particular including the residual risk statement, the security operating procedures and the crypto plan within the CIS accreditation process;

7.2. participating in the selection and testing of the system-specific technical security measures, devices and software, in order to supervise their implementation and to ensure that they are securely installed, configured and maintained in accordance with the relevant security documentation;

7.3. monitoring the implementation and application of the security operating procedures and, where appropriate, delegating operational security responsibilities to the system owner, namely the CIU;

7.4. managing and handling cryptographic products, ensuring the custody of crypto items and controlled items and, if so required, ensuring the generation of cryptographic variables;

7.5. conducting security analysis reviews and tests, in particular for the purposes of producing the relevant risk reports, as required by the SAA;

7.6. providing CIS-specific information assurance training;
7.7. implementing and operating CIS-specific security measures.

8. The CDA shall be responsible for:
8.1. managing and accounting for EU crypto material;
8.2. ensuring, in close cooperation with the SAA, that appropriate procedures are enforced and that plans are in place for accounting, secure handling, storage and distribution of all EU crypto material; and
8.3. ensuring the transfer of EU crypto material to or from individuals or services using it.

9. The TA shall be responsible for ensuring compliance by the CIS with TEMPEST policies and handling instructions. It shall approve TEMPEST countermeasures for installations and products to protect classified information to a defined level of classification in its operational environment.

10. The IAA shall be responsible for all aspects of the management and handling of confidential information within Parliament and, in particular, for:
10.1 developing information assurance security and its security guidelines, and monitoring their effectiveness and pertinence;
10.2. safeguarding and administering technical information related to cryptographic products;
10.3. ensuring that information assurance measures selected for protecting classified information comply with the relevant policies governing their eligibility and selection;
10.4. ensuring that cryptographic products are selected in compliance with policies governing their eligibility and selection;
10.5. consulting with the system provider, the security actors and representatives of users with regard to information assurance security.

SECURITY NOTICE 2

MANAGEMENT OF CONFIDENTIAL INFORMATION

A. INTRODUCTION

1. This security notice sets out the provisions for the management by Parliament of confidential information.

2. When creating confidential information, the originator shall assess the level of confidentiality and take a decision based on the principles set out in this security notice as to the classification or marking of that information.

B. EUCI CLASSIFICATION

3. The decision to classify a document shall be made before its creation. To that end, classifying information as EUCI involves a prior assessment of its level of confidentiality and a decision by the originator that unauthorised disclosure of such information would cause some degree of prejudice to the interests of the European Union or of one or more of its Member States or individuals.

4. Once the decision to classify the information is taken, a second prior assessment shall follow in order to determine the appropriate classification level. The classification of a document shall be determined by the level of sensitivity of its contents.

5. Responsibility for classifying information shall lie solely with the originator. Parliament officials shall classify information on instructions from, or pursuant to a delegation by, the Secretary-General.

6. Classification shall be correctly and sparingly used. The originator of a document that is to be given a classification shall curb any tendency to over-classify or under-classify.

7. The classification level assigned to the information shall determine the level of protection afforded to it in the areas of personnel security, physical security, procedural security and information assurance.

8. Information which warrants classification shall be marked and handled as such, regardless of its physical form. Its classification shall be clearly communicated to its recipients, either by a security classification marking (if it is delivered in written form, be it on paper or within a CIS) or by an announcement (if it is delivered in oral form, such as in the course of a conversation or a meeting held in camera). Classified material shall be physically marked so as to enable its security classification to be easily identified.

9. EUCI in electronic form may only be created within an accredited CIS. The classified information itself, as well as the file name and storage device (if external, such as a CD-ROM or USB stick), shall bear the relevant security classification marking.

10. Information shall be classified as soon as it takes form. For example, personal notes, drafts or e-mail messages containing information which warrants classification are to be marked as EUCI from the outset and shall be produced and handled in accordance with this Decision and its handling instructions in physical and technical terms. Such information may then evolve into an official document which will in turn be appropriately marked and handled. During the drafting process, an official document may need to be re-evaluated and assigned a higher or lower classification level as it evolves.

11. The originator may decide to assign a standard classification level to categories of information which he/she creates on a regular basis. However, the originator shall ensure that, in so doing, he/she does not systematically over-classify or under-classify individual pieces of information.

12. EUCI shall always bear a security classification marking corresponding to its security classification level.

B.1. *Levels of classification*

13. EUCI shall be classified at one of the following levels:

– 'TRÈS SECRET UE/EU TOP SECRET', as defined in point (d) of Article 2 of this Decision, where its compromise would be likely to:

(a) threaten directly the internal stability of the Union or of one or more of its Member States or third States or international organisations;

(b) cause exceptionally grave damage to relations with third States or international organisations;

(c) lead directly to widespread loss of life;

(d) cause exceptionally grave damage to the operational effectiveness or security of Member States' or other contributors' deployed personnel, or to the continuing effectiveness of extremely valuable security or intelligence operations; or

(e) cause severe long-term damage to the Union's or Member States' economy;

– 'SECRET UE/EU SECRET', as defined in point (d) of Article 2 of this Decision, where its compromise would be likely to:

(a) raise international tensions to a significant degree;

(b) seriously damage relations with third States and international organisations;

(c) threaten life directly or seriously prejudice public order or individual security or liberty;

(d) damage major commercial or policy negotiations, causing significant operational problems for the Union or Member States;

(e) cause serious damage to the operational security of Member States, or to the effectiveness of highly valuable security or intelligence operations;

(f) cause substantial material damage to Union or Member State financial, monetary, economic and commercial interests;

(g) substantially undermine the financial viability of major organisations or operators; or

(h) seriously impede the development or operation of Union policies with major economic, trade or financial consequences;

– 'CONFIDENTIEL UE/EU CONFIDENTIAL', as defined in point (d) of Article 2 of this Decision, where its compromise would be likely to:

(a) significantly damage diplomatic relations, e.g. where it would lead to a formal protest or other sanctions;

(b) put individual security or liberty at risk;

(c) put the outcome of commercial or policy negotiations at serious risk; cause operational problems for the Union or Member States;

(d) cause damage to the operational security of Member States, or to the effectiveness of security or intelligence operations;

(e) substantially undermine the financial viability of major organisations or operators;

(f) impede the investigation or facilitate the commission of crime or terrorist activities;

(g) work substantially against Union or Member State financial, monetary, economic and commercial interests; or

(h) seriously impede the development or operation of Union policies with major economic, trade or financial consequences;

– 'RESTREINT UE/EU RESTRICTED', as defined in point (d) of Article 2 of this Decision, where its compromise would be likely to:

(a) be disadvantageous to the general interests of the Union;

(b) adversely affect diplomatic relations;

(c) cause substantial distress to individuals or companies;

(d) be disadvantageous to the Union or Member States in commercial or policy negotiations;

(e) make it more difficult to maintain effective security within the Union or Member States;

(f) impede the effective development or operation of Union policies;

(g) undermine the proper management of the Union and its operations;

(h) breach undertakings given by Parliament to maintain the classified status of information provided by third parties;

(i) breach statutory restrictions on disclosure of information;

(j) cause financial loss or facilitate improper gain or advantage for individuals or companies; or

(k) prejudice the investigation or facilitate the commission of crime.

B.2. *Classification of compilations, cover pages and excerpts*

14. The classification of a letter or note containing enclosures shall be as high as the highest classification level assigned to one of its enclosures. The originator shall indicate clearly the level at which the letter or note should be classified when detached from its enclosures. Where the cover note/letter does not need to be classified, it shall include the following final wording: 'When detached from its enclosures, this note/letter is unclassified.'.

15. Documents or files containing components with different classification levels are whenever possible to be structured in such a way that components with a different classification level may be easily identified and detached if necessary. The overall classification level of a document or file shall be at least as high as that of its most highly classified component.

16. Individual pages, paragraphs, sections, annexes, appendices, attachments and enclosures of a given document may require different classification levels and shall be classified accordingly. Standard abbreviations may be used within documents containing EUCI to indicate the classification level of sections or blocks of text of less than a single page.

17. When information from various sources is collated, the final product shall be reviewed to determine its overall security classification level, since it may warrant a higher classification level than its component parts.

C. OTHER CONFIDENTIAL INFORMATION

18. 'Other confidential information' shall be marked in accordance with point E of this security notice and the handling instructions.

D. CREATION OF CONFIDENTIAL INFORMATION

19. Only persons duly empowered by this Decision or authorised by the SA may create confidential information.

20. Confidential information shall not be added to internet or intranet document management systems.

D.1. *Creation of EUCI*

21. In order to create EUCI classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET, the individual concerned shall be empowered by this Decision or shall first be in possession of an authorisation granted pursuant to Article 4(1) of this Decision.

22. EUCI classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET shall be created only within the Secure Area.

23. The following rules shall apply to the creation of EUCI:

(a) each page shall be marked clearly with the applicable classification level;
(b) each page shall be numbered and shall state the total number of pages;
(c) the document shall bear a reference number on the first page and an indication of its subject-matter, which shall not itself constitute classified information, unless it is affixed as such;
(d) the document shall bear a date on the first page;
(e) the first page of any document classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET shall contain a list of all annexes and enclosures;
(f) documents classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET shall bear a copy number on every page, if they are to be distributed in several copies. Each copy shall also bear on the first page the total number of copies and of pages, and
(g) if the document makes reference to other documents containing classified information received from other Union Institutions, or if it contains classified information emanating from those documents, it shall bear the same classification level as those documents and may not, without the prior written consent of its originator, be distributed to any persons other than those named in the distribution list in respect of the original document or documents containing classified information.

24. The originator shall retain control of EUCI which he/she has created. His/her prior written consent shall be sought before that EUCI is:

(a) downgraded or declassified;

(b) used for purposes other than those established by the originator;
(c) disclosed to any third State or international organisation;
(d) disclosed to any person, institution, country or international organisation other than the addressees originally authorised by the originator to consult the information in question;
(e) disclosed to a contractor or prospective contractor located in a third State;
(f) copied or translated, if the information is classified at the level TRES SECRET UE/EU TOP SECRET;
(g) destroyed.

D.2. *Creation of other confidential information*

25. The Secretary-General, acting as SA, may decide whether or not to authorise the creation of 'other confidential information' by a given function, service and/or individual.

26. 'other confidential information' shall bear one of the markings defined in the handling instructions.

27. The following rules shall apply to the creation of 'other confidential information':
(a) its marking shall be indicated at the top of the first page of the document;
(b) each page shall be numbered within the total number of pages;
(c) the document shall bear a reference number on the first page and an indication of its subject-matter;
(d) the document shall bear a date on the first page and;
(e) the last page of the document shall contain a list of all annexes and enclosures.

28. Creation of 'other confidential information' is subject to specific rules and procedures laid down in the handling instructions.

E. SECURITY DESIGNATORS AND MARKINGS

29. Security designators and markings on documents are intended to control the flow of information and to restrict access to confidential information on the basis of the 'need to know' principle.

30. When security designators and/or markings are being used or affixed, care shall be taken to avoid confusion with security classifications for EUCI: RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/

EU CONFIDENTIAL, SECRET UE/EU SECRET, TRES SECRET UE/EU TOP SECRET.

31. Specific rules concerning the use of security designators and markings, along with the list of approved European Parliament security markings, shall be laid down in the handling instructions.

E.1. *Security designators*

32. Security designators may only be used in conjunction with a security classification and shall not be applied separately to documents. A security designator may be applied to EUCI in order to:

(a) set limits to the validity of a classification (for classified information signifying automatic downgrading or declassification);
(b) limit the distribution of the EUCI in question;
(c) establish special handling arrangements in addition to those corresponding to the security classification level.

33. The extra controls applicable to the handling and storage of documents containing EUCI impose additional burdens on all involved. In order to minimise the work required in this connection, it is good practice, when creating such a document, to establish a time limit or event after which the classification is to automatically expire and the information contained in the document is to be downgraded or declassified.

34. Where a document deals with a specific area of work and its distribution needs to be limited and/or it is to be subject to special handling arrangements, a statement to that effect may be added to its classification to help to identify its target audience.

E.2. *Markings*

35. Markings do not constitute a security classification. They are intended to serve only to provide concrete instructions about the handling of a document, and shall not be used to describe the contents of such document.

36. Markings may be applied separately to documents or used in conjunction with a security classification.

37. As a general rule, markings shall be applied to information which is covered by the professional secrecy referred to in Article 339 TFEU and

Article 17 of the Staff Regulations, or which has to be protected for legal reasons by Parliament but does not need to be, or cannot be, classified.

E.3. *Use of markings in the CIS*

38. The rules on the use of the markings are also applicable within the accredited CIS.

39. The SAA shall establish specific rules on the use of markings in the accredited CIS.

F. RECEPTION OF INFORMATION

40. Only the CIU shall be entitled within Parliament to receive information classified as CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET, or its equivalent from third parties.

41. As to information classified at the level RESTREINT UE/EU RESTRICTED or its equivalent and 'other confidential information', both the CIU or the competent parliamentary body/office-holder may be responsible for receiving it from third parties, and for applying the principles set out in this security notice.

G. REGISTRATION

42. Registration means the application of procedures for recording the life-cycle of confidential information, including its dissemination, consultation and destruction.

43. For the purposes of this security notice, 'logbook' means a register which records in particular the dates and times when confidential information:

(a) enters or exits the respective secretariat of the parliamentary body/office-holder or, as the case may be, the CIU;
(b) is accessed by or transmitted to a security-cleared person; and
(c) is destroyed.

44. The originator of classified information shall be responsible for marking the initial declaration upon the creation of a document containing such information. That declaration shall be communicated to the CIU when the document is created.

45. Information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET, or its equivalent may only be registered by the CIU for security purposes. Information classified at the level RESTREINT UE/EU RESTRICTED or its equivalent and 'other confidential information' received from third parties shall be registered by the service responsible for the official reception of the document, being either the CIU or the secretariat of the parliamentary body/office-holder, for administrative purposes. 'Other confidential information' produced within Parliament shall be registered by the originator, for administrative purposes.

46. Information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET, or its equivalent shall be registered especially when:

(a) it is produced;

(b) it arrives at or leaves the CIU; and

(c) it arrives at or leaves the CIS.

47. Information classified at the level RESTREINT UE/EU RESTRICTED or its equivalent shall be registered especially when:

(a) it is produced;

(b) it arrives at or leaves the respective secretariat of the parliamentary body/office-holder or the CIU; and

(c) it arrives at or leaves the CIS.

48. Registration of confidential information may be carried out on paper or in electronic logbooks/CIS.

49. For information classified at the level RESTREINT UE/EU RESTRICTED or its equivalent and 'other confidential information', at least the following shall be recorded:

(a) the date and time when it enters or leaves the respective secretariat of the parliamentary body/office-holder or the CIU, as the case may be;

(b) the document title, the classification level or marking, the expiry date of the classification/marking and any reference number assigned to the document.

50. For information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET, or its equivalent, at least the following shall be recorded:

(a) the date and time when it enters or leaves the CIU;

(b) the document title, classification level or marking, any reference number assigned to the document and the expiry date of the classification/marking;
(c) details of the originator;
(d) a record of the identity of any person who is given access to the document, and of the date when it was accessed by that person;
(e) a record of any copies or translations made of the document;
(f) the date and time when any copies or translations of the document leave or return to the CIU, and details of where they have been sent and who has returned them;
(g) the date and time when the document is destroyed, and by whom, in accordance with Parliament's security rules on destruction; and
(h) the declassification or downgrading of the document.

51. Logbooks shall be classified or marked as appropriate. Logbooks for information classified at the level TRES SECRET UE/EU TOP SECRET or its equivalent shall be registered at the same level.

52. Classified information may be registered:
(a) in a single logbook; or
(b) in separate logbooks according to its classification level, its status as incoming or outgoing information and its origin or destination.

53. In the case of electronic handling within the CIS, registration procedures may be carried out by those means within the CIS itself which meet requirements equivalent to those specified above. Whenever EUCI leaves the perimeter of the CIS, the registration procedure described above shall apply.

54. The CIU shall keep a record of all classified information released by Parliament to third parties and of classified information received by Parliament from third parties.

55. Once registration of information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET or its equivalent is complete, the CIU shall check whether the addressee has a valid security authorisation. Where this is the case, the addressee shall be notified by the CIU. The consultation of classified information may only take place once the document containing it has been registered.

H. DISTRIBUTION

56. The originator shall establish the initial distribution list for the EUCI which he/she has created.

57. Information classified at the level RESTREINT UE/EU RESTRICTED and 'other confidential information' produced by Parliament shall be distributed within Parliament by the originator, in accordance with the relevant handling instructions and on the basis of the 'need-to-know' principle. For information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET created by Parliament within the Secure Area, the distribution list (and any further instructions concerning distribution) shall be provided to the CIU, which shall be responsible for its management.

58. EUCI produced by Parliament may be distributed to third parties only by the CIU, on the basis of the 'need to know' principle.

59. Confidential information received either by the CIU or by any parliamentary body/office-holder who submitted the request therefor shall be distributed in accordance with the instructions received from the originator.

I. HANDLING, STORAGE AND CONSULTATION

60. Handling, storage and consultation of confidential information shall be carried out in accordance with security notice 4 and the handling instructions.

J. COPYING/TRANSLATING/INTERPRETING CLASSIFIED INFORMATION

61. Documents containing information classified at the level TRES SECRET UE/EU TOP SECRET or its equivalent shall not be copied or translated without the prior written consent of the originator. Documents containing information classified at the level SECRET UE/EU SECRET or its equivalent or at the level CONFIDENTIEL UE/EU CONFIDENTIAL or its equivalent may be copied or translated on instruction from the holder, provided the originator has not prohibited this.

62. Each copy of a document containing information classified at the level TRES SECRET UE/EU TOP SECRET, SECRET UE/EU SECRET

or CONFIDENTIEL UE/EU CONFIDENTIAL or its equivalent shall be registered for security purposes.

63. The security measures applicable to the original document containing classified information shall apply to copies and translations thereof.

64. Documents received from the Council should be received in all official languages.

65. Copies and/or translations of documents containing classified information may be requested by the originator or copy holder. Copies of documents containing information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET, or its equivalent may only be produced in the Secure Area and on copiers which are part of an accredited CIS. Copies of documents containing information classified at the level RESTREINT UE/EU RESTRICTED or its equivalent and 'other confidential information' shall be made using an accredited reproduction device within Parliament's premises.

66. All copies and translations of any document or parts of copies of documents containing confidential information shall be appropriately marked, numbered and registered.

67. No more copies shall be made than are strictly necessary. All copies shall be destroyed in accordance with the handling instructions at the end of the consultation period.

68. Only interpreters and translators who are Parliament officials shall ge given access to classified information.

69. Interpreters and translators with access to documents containing information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET, or its equivalent shall have the appropriate security clearance.

70. When working on documents containing information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET, or its equivalent, interpreters and translators shall work in the Secure Area.

K. DOWNGRADING, DECLASSIFYING AND UNMARKING OF CONFIDENTIAL INFORMATION

K.1. *General principles*

71. Confidential information shall be declassified, downgraded or unmarked when protection is no longer necessary or is no longer needed at the original level.

72. Decisions to downgrade, declassify or unmark information contained in documents produced within Parliament may also have to be made on an ad hoc basis, for example in response to a request for access from the public or from another Union Institution, or at the initiative of the CIU or parliamentary body/office-holder.

73. At the time of its creation, the originator of EUCI shall indicate, where possible, whether the EUCI in question can be downgraded or declassified on a given date or following a specific event. When it is not practicable to give such an indication, the originator, the CIU or the parliamentary body/office-holder holding the information shall review the classification level of EUCI at least once every five years. In all instances, EUCI may be downgraded or declassified only with the prior written consent of the originator.

74. In the event that the originator of EUCI cannot be established or traced in respect of documents produced within Parliament, the SA shall review the classification level of the EUCI in question on the basis of a proposal from the parliamentary body/office-holder holding the information, which may consult the CIU in that regard.

75. The CIU or the parliamentary body/office-holder holding the information shall be responsible for notifying the addressee(s) that the information has been declassified or downgraded, and the addressee(s) shall in turn be responsible for notifying any subsequent addressee(s) to whom they have sent or copied the document.

76. The declassification, downgrading or unmarking of information contained in a document shall be recorded.

K.2. *Declassification*

77. EUCI may be declassified in full or in part. It may be declassified in part when protection is no longer deemed necessary for a specific part of the document containing it but continues to be justified for the rest of the document.

78. When the review of EUCI contained in a document created within Parliament results in a decision to declassify it, consideration shall be given to the question whether the document may be made public or whether it is to bear a distribution marking (i.e. not be made public).

79. When EUCI is declassified, its declassification shall be recorded in the logbook with the following data: date of the declassification, names of the persons who requested and who authorised the declassification, reference number of the declassified document and its final destination.

80. The old classification markings in the declassified document and in all copies thereof shall be struck through. The documents and all copies thereof shall be stored accordingly.

81. Upon partial declassification of classified information, the part that has been declassified shall be produced in the form of an extract and stored appropriately. The competent service shall register:
(a) the date of the partial declassification;
(b) the names of the persons who requested and who authorised the declassification; and
(c) the reference number of the declassified extract.

K.3. *Downgrading*

82. Following the downgrading of classified information, the document containing it shall be registered in the logbooks corresponding to both the old and the new classification level. The date of downgrading shall be recorded, as well as the name of the person who authorised it.

83. The document containing the downgraded information and all copies thereof shall be classified with the new classification level and stored appropriately.

L. DESTRUCTION OF CONFIDENTIAL INFORMATION

84. Confidential information (in either hard copy or electronic form) which is no longer required shall be destroyed or deleted, in accordance with the handling instructions and relevant rules on archiving.

85. Information classified at the level TRES SECRET UE/EU TOP SECRET or SECRET UE/EU SECRET or its equivalent, shall be destroyed by the CIU. Its destruction shall be witnessed by a person holding security clearance corresponding to at least the classification level of the information being destroyed.

86. Information classified at the level TRES SECRET UE/EU TOP SECRET or its equivalent shall be destroyed only with the prior written consent of the originator.

87. Information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET, or its equivalent shall be destroyed and disposed of by the CIU on instruction from the originator or from a competent authority. The logbooks and other registers shall be updated accordingly. Information classified at the level RESTREINT UE/EU RESTRICTED or its equivalent shall be destroyed and disposed of either by the CIU or by the relevant parliamentary body/office-holder.

88. The official responsible for the destruction and the person witnessing the destruction shall sign a destruction certificate, to be filed and archived in the CIU. The CIU shall keep, together with the distribution forms, destruction certificates relating to information classified at the level TRES SECRET UE/EU TOP SECRET or its equivalent for a period of at least ten years, and, in the case of information classified at the level SECRET UE/EU SECRET or its equivalent and CONFIDENTIEL UE/EU CONFIDENTIAL or its equivalent, for a period of at least five years.

89. Documents containing classified information shall be destroyed by methods which meet the relevant Union standards or equivalent standards so as to prevent them from being reconstructed in whole or in part.

90. The destruction of computer storage media used for classified information shall be carried out in accordance with the relevant handling instructions.

91. Destruction of classified information shall be recorded in the relevant logbook with the following data:

(a) date and time of destruction;

(b) name of the official responsible for destruction;

(c) identification of the document or copies destroyed;

(d) original physical form of the destroyed EUCI;

(e) means of destruction; and

(f) place of destruction.

M. ARCHIVING

92. Classified information, including any cover note/letter, annexes, deposit slip and/or other parts of the dossier, shall be transferred to the secure archive in the Secure Area six months after it was last consulted and, at the latest, one year after it was deposited. Detailed rules on the archiving of classified information shall be laid down in the handling instructions.

93. For 'other confidential information', the general rules on document management shall apply without prejudice to any other specific provisions on its handling.

SECURITY NOTICE 3

THE PROCESSING OF CONFIDENTIAL INFORMATION BY MEANS OF AUTOMATED COMMUNICATION INFORMATION SYSTEMS (CIS)

A. INFORMATION ASSURANCE OF CLASSIFIED INFORMATION HANDLED IN INFORMATION SYSTEMS

1. 'Information assurance' (IA) in the field of information systems is the confidence that such systems will protect the classified information they handle and will function as they need to and when they need to, under the control of legitimate users. Effective IA shall ensure appropriate levels of confidentiality, integrity, availability, non-repudiation and authenticity. IA shall be based on a risk management process.

2. 'Communication Information System' (CIS) for the handling of classified information means a system enabling information to be handled in electronic form. Such an information system shall comprise the entire assets required for it to operate, including the infrastructure, organisation, personnel and information resources.

3. CIS shall handle classified information in accordance with the concept of IA.

4. CIS shall undergo an accreditation process. Accreditation shall aim at obtaining assurance that all appropriate security measures have been implemented and that a sufficient level of protection of the classified information and of the CIS has been achieved in accordance with this security notice. The accreditation statement shall determine the maximum classification level of the information that may be handled in the CIS as well as the corresponding terms and conditions.

5. The following IA properties and concepts are essential for the security and correct functioning of CIS operations:

(a) authenticity: the guarantee that information is genuine and that it emanates from bona fide sources;
b) availability: the property of being accessible and usable upon request by an authorised entity;
(c) confidentiality: the property that information is not to be disclosed to unauthorised individuals, entities or processes;
(d) integrity: the property of safeguarding the accuracy and completeness of information and assets;
(e) non-repudiation: the ability to prove that an action or event has taken place, so as to preclude the possibility of any subsequent denial of that event or action.

B. INFORMATION ASSURANCE PRINCIPLES

6. The provisions set out below shall form the baseline for the security of any CIS handling classified information. Detailed requirements for implementing these provisions shall be defined in IA security policies and security guidelines.

B.1. *Security risk management*

7. Security risk management shall be an integral part of defining, developing, operating and maintaining CIS. Risk management (assessment, treatment, acceptance and communication) shall be conducted as an iterative process jointly by representatives of the system owners, project authorities, operating authorities and security approval authorities, as laid down in security notice 1, using a proven, transparent and understandable risk assessment process. The scope of the CIS and its assets shall be clearly defined at the outset of the risk management process.

8. The competent authorities, as laid down in security notice 1, shall review the potential threats to CIS and shall maintain up-to-date and accurate threat assessments which reflect the current operational environment. They shall constantly update their knowledge of vulnerability issues and periodically review the vulnerability assessment to keep up with the changing information technology (IT) environment.

9. The aim of security risk treatment shall be to apply a set of security measures which results in a satisfactory balance between user

requirements, cost and residual security risk.

10. Accreditation of a CIS shall include a formal residual risk statement and acceptance of the residual risk by a responsible authority. The specific requirements, scale and degree of detail determined by the relevant SAA for accrediting a CIS shall be commensurate with the risk assessed, taking account of all relevant factors, including the classification level of the classified information handled in the CIS.

B.2. *Security throughout the CIS life cycle*

11. Ensuring security shall be a requirement throughout the entire CIS life cycle, from initiation to withdrawal from service.

12. The role and interaction of each actor involved in CIS with regard to its security shall be identified for each phase of the life cycle.

13. CIS, including its technical and non-technical security measures, shall be subject to security testing during the accreditation process to ensure that the appropriate level of assurance is obtained and to verify that the CIS, including its technical and non-technical security measures, are correctly implemented, integrated and configured.

14. Security assessments, inspections and reviews shall be performed periodically during the operation and maintenance of CIS and when exceptional circumstances arise.

15. Security documentation for CIS shall evolve over its life cycle as an integral part of the process of change management.

16. Registration procedures performed by a CIS, where required, shall be verified as part of the accreditation process.

B.3. *Best practice*

17. The IAA shall develop best practice for protecting classified information handled by the CIS. Best practice guidelines shall set out technical, physical, organisational and procedural security measures for CIS with proven effectiveness in countering given threats and vulnerabilities.

18. The protection of classified information handled by the CIS shall draw on lessons learned by entities involved in IA.

19. The dissemination and subsequent implementation of best practice

shall help to achieve an equivalent level of assurance for the CIS operated by the Parliament secretariat which handles classified information.

B.4. *Defence in depth*

20. In order to mitigate risk to CIS, a range of technical and non-technical security measures, organised as multiple layers of defence, shall be implemented. Those layers shall include:

(a) deterrence: security measures aimed at dissuading any adversary planning to attack the CIS;
(b) prevention: security measures aimed at impeding or blocking an attack on the CIS;
(c) detection: security measures aimed at discovering the occurrence of an attack on the CIS;
(d) resilience: security measures aimed at limiting the impact of an attack to a minimum set of information or CIS assets and preventing further damage; and
(e) recovery: security measures aimed at regaining a secure situation for the CIS.

The degree of stringency of such security measures shall be determined following a risk assessment.

21. The competent authorities, as specified in security notice 1, shall ensure that they can respond to incidents which may transcend organisational boundaries in such a way as to coordinate responses and share information about those incidents and the related risks (computer emergency response capabilities).

B.5. *Principle of minimalist and least privilege*

22. In order to avoid unnecessary risk, only the essential functionalities, devices and services needed to meet operational requirements shall be implemented.

23. CIS users and automated processes shall be given only the access, privileges or authorisations they require in order to perform their tasks, so as to limit any damage resulting from accidents, errors, or unauthorised use of CIS resources.

B.6. *Information assurance awareness*

24. Awareness of the risks and available security measures is the first line of defence for the security of CIS. In particular, all personnel involved in the life cycle of CIS, including users, shall understand:

(a) that security failures may significantly harm the CIS handling classified information;

(b) the potential harm to others which may arise from interconnectivity and interdependency; and

(c) their individual responsibility and accountability for the security of CIS according to their roles within the systems and processes.

25. In order to ensure that security responsibilities are understood, IA education and awareness training shall be mandatory for all personal involved, including senior management, Members of the European Parliament and CIS users.

B.7. *Evaluation and approval of IT-security products*

26. CIS handling information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET, or its equivalent shall be protected in such a way that the information cannot be compromised by unintentional electromagnetic emanations (‘TEMPEST security measures’).

27. Where the protection of classified information is provided by cryptographic products, such products shall be certified by the SAA as EU-approved cryptographic products.

28. During transmission of classified information by electronic means, EU-approved cryptographic products shall be used. Notwithstanding this requirement, specific procedures or specific technical configurations may be applied in emergency circumstances as specified in points 41 to 44.

29. The requisite degree of confidence in the security measures, defined as a level of assurance, shall be determined following the outcome of the risk management process and in line with the relevant security policies and guidelines.

30. The level of assurance shall be verified by using internationally recognised or nationally approved processes and methodologies. This includes primarily evaluation, controls and auditing.

31. The SAA shall approve security guidelines on the qualification and approval of non-cryptographic IT security products.

B.8. *Transmission within the Secure Area*

32. When transmission of classified information is confined within the Secure Area, unencrypted distribution or encryption at a lower level may be used, based on the outcome of a risk management process and subject to the approval of the SAA.

B.9. *Secure interconnection of CIS*

33. Interconnection shall mean the direct connection of two or more IT systems for the purpose of sharing data and other information resources in a unidirectional or multidirectional way.

34. CIS shall treat any interconnected IT system as untrustworthy and shall implement protective measures to control the exchange of classified information with any other CIS.

35. For all interconnections of CIS with another IT system the following basic requirements shall be met:

(a) business or operational requirements for such interconnections shall be stated and approved by the competent authorities;

(b) the interconnection in question shall undergo a risk management and accreditation process and shall require the approval of the competent SAA;

(c) protection services (PS) shall be implemented at the perimeter of CIS.

36. There shall be no interconnection between an accredited CIS and an unprotected or public network, except where the CIS has approved PSs installed for such a purpose between the CIS and the unprotected or public network. The security measures for such interconnections shall be reviewed by the competent IAA and approved by the competent SAA.

37. When the unprotected or public network is used solely as a carrier and the data is encrypted by an EU cryptographic product certified in accordance with paragraph 27, such a connection shall not be deemed to be an interconnection.

38. The direct or cascaded interconnection to an unprotected or public network of a CIS accredited to handle information classified at the level TRES SECRET UE/EU TOP SECRET or its equivalent or SECRET UE/

EU SECRET or its equivalent shall be prohibited.

B.10. *Computer storage media*

39. Computer storage media shall be destroyed in accordance with procedures approved by the competent security authority.

40. Computer storage media shall be reused, downgraded or declassified in accordance with the handling instructions.

B.11. *Emergency circumstances*

41. The specific procedures described below may be applied in an emergency, such as during situations of impending or actual crisis, conflict or war, or in exceptional operational circumstances.

42. Classified information may, with the consent of the competent authority, be transmitted using cryptographic products which have been approved for a lower classification level or without encryption if any delay would cause harm clearly outweighing the harm entailed by any disclosure of the classified material and if:

(a) the sender and the recipient do not have the required encryption facility or have no encryption facility; and

(b) the classified material cannot be conveyed in sufficient time by other means.

43. Classified information transmitted under the circumstances set out in paragraph 41 shall not bear any markings or indications distinguishing it from information which is unclassified or which can be protected by an available cryptographic product. Recipients shall be notified of the classification level, without delay, by other means.

44. Should recourse be had to paragraph 41 or 42 a subsequent report shall be made to the competent authority.

SECURITY NOTICE 4

PHYSICAL SECURITY

A. INTRODUCTION

This security notice sets out the security principles for creating a secure environment for ensuring the correct treatment of confidential information in the European Parliament. These principles, including those relating to technical security, will be supplemented by the handling instructions.

B. SECURITY RISK MANAGEMENT

1. Risk to classified information shall be managed as a process. That process shall be aimed at determining known security risks, at defining security measures to reduce such risks to an acceptable level in accordance with the basic principles and minimum standards set out in this security notice, and at applying those measures in line with the concept of defence in depth as defined in security notice 3. The effectiveness of such measures shall be continuously evaluated.

2. Security measures for protecting classified information throughout its life cycle shall be commensurate with, in particular, its security classification, the form and volume of the information or material concerned, the location and construction of facilities housing classified information and the locally assessed threat of malicious and/or criminal activities, including espionage, sabotage and terrorism.

3. Contingency plans shall take account of the need to protect classified information during emergency situations in order to prevent unauthorised access, disclosure or loss of integrity or availability.

4. Preventive and recovery measures to minimise the impact of major failures or incidents on the handling and storage of classified information shall be included in business continuity plans.

C. GENERAL PRINCIPLES

5. The classification or marking level assigned to the information shall determine the level of protection afforded to it in the areas of physical security.

6. Information which warrants classification shall be marked and handled as such regardless of its physical form. Its classification shall be clearly communicated to its recipients, either by a classification marking (if it is delivered in written form, be it on paper or in CIS) or by an announcement (if it is delivered in oral form, such as in a conversation or a presentation). Classified material shall be physically marked so as to enable its security classification to be easily identified.

7. Confidential information shall not, under any circumstances, be read in public places where it might be seen by an individual without a need to know, e.g. on trains or in planes, cafes, bars etc. It shall not be left in hotel safes or rooms, or left unattended in public places.

D. RESPONSIBILITIES

8. The CIU is responsible for ensuring physical security in the management of confidential information deposited in its secure facilities. The CIU is also responsible for the management of its secure facilities.

9. Physical security in the management of information classified at the level RESTREINT UE/EU RESTRICTED or its equivalent and of 'other confidential information' is the responsibility of the respective parliamentary body/office-holder.

10. The Directorate for Security and Risk Assessment shall ensure the personal security and security clearance needed to ensure the secure handling of confidential information in the European Parliament.

11. The DIT shall advise and ensure that any created or used CIS is fully in compliance with security notice 3 and the respective handling instructions.

E. SECURE FACILITIES

12. Secure facilities may be installed under the technical security standards and in accordance with the level assigned to the confidential information as defined in Article 7.

13. The secure facilities shall be certified by the SAA and validated by the SA.

F. CONSULTATION OF CONFIDENTIAL INFORMATION

14. When information classified at the level RESTREINT UE/EU RESTRICTED or its equivalent and 'other confidential information' is deposited with the CIU and has to be consulted outside the Secure Area, the CIU shall transmit a copy to the appropriate authorised service which shall ensure that consultation and handling of the information in question complies with Article 8(2) and Article 10 of this Decision and the appropriate handling instructions.

15. When information classified at the level RESTREINT UE/EU RESTRICTED or its equivalent and 'other confidential information' is deposited with a parliamentary body/office-holder other than the CIU, the secretariat of that parliamentary body/office-holder shall ensure that consultation and handling of the information in question complies with Article 7(3), Article 8(1), (2) and (4), Article 9(3), (4) and (5), Article 10(2) to (6), and Article 11 of this Decision and the appropriate handling instructions.

16. When information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET, or its equivalent has to be consulted in the Secure Area, the CIU shall ensure that consultation and handling of the information in question complies with Articles 9 and 10 of this Decision and the appropriate handling instructions.

G. TECHNICAL SECURITY

17. Technical security measures are the responsibility of the SAA, who shall determine in the appropriate handling instructions the specific technical security measures which are to apply.

18. Secure Reading Rooms for consultation of information classified at the level RESTREINT UE/EU RESTRICTED or its equivalent and of 'other confidential information' shall comply with specific technical security measures, as provided for in the handling instructions.

19. The Secure Area shall comprise the following facilities:

(a) a Security Access Screening Room (SAS), to be installed in accordance with the technical security measures laid down in the handling instructions. Access to this facility shall be registered. The SAS shall meet high standards in terms of identification of persons with access, video registering, and secure space in which to deposit personal elements that are not allowed in the secured rooms (telephones, pens, etc.);

(b) a communication room for transmission and receipt of classified information, including encrypted classified information, in accordance with security notice 3 and the respective handling instructions;

(c) a secure archive, in which approved and certified containers shall be used separately for information classified at the level RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL and/or SECRET EU/EU SECRET or its equivalent. Information classified at the level TRES SECRET UE/EU TOP SECRET or its equivalent shall be placed in a separate room in a specific certified container. The only additional material available in that separate room shall be the support desk for handling the archive by the CIU;

(d) a registry room, which shall provide the tools needed to ensure that registration can be done on paper or electronically and shall thus be equipped with the secure facilities needed for the installation of the appropriate CIS. Only the registry room may contain approved and accredited reproduction devices (for making copies in paper or electronic form). The handling instructions shall specify which reproduction devices are approved and accredited. The registry room shall also provide the space needed in order for accredited material to be stored and handled so as to allow for the marking, copying and dispatching of classified information in physical form, by level of classification. All accredited material shall be defined by the CIU and accredited by the SAA, in accordance with the advice received from the IAOA. The registry room shall also be equipped with the accredited destruction device approved for the highest level of classification, as described in the handling instructions. Translation of information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL EU, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET or its equivalent shall be done in the registry room, in the appropriate and

accredited system. The registry room shall provide work stations for up to two translators at a time and for the same document. One staff member of the CIU shall be present;

(e) a reading room, for individual consultation of classified information by duly authorised persons. The reading room shall have enough space for two persons, including a staff member of the CIU who shall be present throughout each consultation. The security level of this room shall be adequate for the consultation of information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET or its equivalent. The reading room may be equipped with TEMPEST equipment so as to allow for electronic consultation, when needed, in accordance with the level of classification of the information concerned;

(f) a meeting room, which shall be able to accommodate up to 25 persons for the purposes of discussing information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET EU/EU SECRET or its equivalent. The meeting room shall provide the necessary technical secure and certified facilities for interpretation into and out of up to two languages. When not used for meetings, the meeting room may also be used as an additional reading room for individual consultation. In exceptional cases, the CIU may allow more than one authorised person to consult classified information, as long as the level of clearance and the need to know is the same for all persons in the room. No more than four persons shall be allowed to consult classified information at the same time. The presence of CIU officials shall be reinforced;

(g) technical secured rooms for lodging all technical equipment, linked to the security of the entire Secure Area, and the secured IT servers.

20. The Secure Area shall comply with the applicable international security standards and shall be certified by the Directorate for Security and Risk Assessment. The Secure Area shall contain the following minimum security technical equipment:

(a) alarm and monitoring security systems;
(b) safety equipment and emergency systems (two-way warning system);
(c) a CCTV system;
(d) an intrusion detection system;
(e) access control (including a biometric security system);
(f) containers;
(g) lockers;

(h) anti-electromagnetic protection.

21. Where additional technical security measures are needed, these may be added by the SAA, acting in close cooperation with the CIU and with the approval of the SA.

22. The infrastructure equipment may be connected to the general management systems of the building in which the Secure Area is located. However, the security equipment dedicated to access control and to the CIS shall be independent from any other such systems existing within the European Parliament.

H. INSPECTIONS OF THE SECURE AREA

23. Inspections of the Secure Area shall be carried out regularly by the SAA and at the request of the CIU.

24. The SAA shall draw up and keep updated the security inspection checklist of items to be verified in the course of an inspection, in line with handling instructions.

I. TRANSPORTATION OF CONFIDENTIAL INFORMATION

25. When carried, confidential information shall be concealed from view and shall give no indication of the confidential nature of its content, in accordance with the handling instructions.

26. Only messengers or staff with the appropriate level of security authorisation may carry information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET or its equivalent.

27. Confidential information may only be despatched by external mail or carried by hand outside a building in accordance with the conditions laid down in the handling instructions.

28. Information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET or its equivalent shall never be sent by e-mail or fax, even via a ‘secure’ e-mail system or a crypto-fax machine. Information classified at the level RESTREINT UE/EU RESTRICTED or its equivalent and other confidential information may be send by e-mail using an accredited encryption system.

J. STORAGE OF CONFIDENTIAL INFORMATION

29. The classification or marking level assigned to confidential information shall determine the level of protection afforded to it with a view to its storage. It shall be stored in the equipment certified for that purpose, in accordance with the handling instructions.

30. Information classified at the level RESTREINT UE/EU RESTRICTED or its equivalent and 'other confidential information' shall:

(a) be stored in a standard-issue, steel, locked, cupboard, either within an office or in a working area, when it is not actually being used;
(b) not be left unattended, unless properly locked and stored;
(c) not be left on a desk, table, etc. in such a way that it may be read or removed by any non-authorised individuals, e.g. visitors, cleaners, maintenance personnel, etc.;
(d) not be shown to, or discussed with, any non-authorised individual.

31. Information classified at the level RESTREINT UE/EU RESTRICTED or its equivalent and 'other confidential information' shall be stored only within the secretariats of the parliamentary bodies/office-holders, or in the CIU, in accordance with the handling instructions.

32. Information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET or its equivalent shall:

(a) be stored in the Secure Area, in a security container or in a strongroom. Exceptionally, for example if the CIU is closed, it may be stored in an approved and certified safe deposit within the security services;
(b) not be left unattended within the Secure Area at any time, without first having been locked in an approved safe (even for the briefest of absences);
(c) not be left on a desk, table etc in such a way that it may be read or removed by a non-authorised person, even if the responsible staff member of the CIU remains in the room.

Where a document containing classified information is being produced in electronic form within the Secure Area, the computer shall be locked, and the screen rendered inaccessible if the originator or the responsible staff member of the CIU leaves the room (even for the briefest of absences). An automatic security lock cutting in after a few minutes shall not be considered a sufficient measure.

SECURITY NOTICE 5

INDUSTRIAL SECURITY

A. INTRODUCTION

1. This security notice concerns classified information only.

2. It sets out provisions for implementing the common minimum standards of Part 1 of Annex I to this Decision.

3. 'Industrial security' is the application of measures to ensure the protection of classified information by contractors or subcontractors in pre-contract negotiations and throughout the life cycle of classified contracts. Such contracts shall not involve access to information classified at the level TRÈS SECRET UE/EU TOP SECRET.

4. The European Parliament, as contracting authority, shall ensure that the minimum standards on industrial security set out in this Decision, and referred to in the contract, are complied with when awarding classified contracts to industrial or other entities.

B. SECURITY ELEMENTS IN A CLASSIFIED CONTRACT

B.1. *Security Classification Guide (SCG)*

5. Prior to launching a call for tenders or awarding a classified contract, the European Parliament, as the contracting authority, shall determine the security classification of any information to be provided to bidders and contractors, as well as the security classification of any information to be created by the contractor. For that purpose, it shall prepare a Security Classification Guide (SCG) to be used for the performance of the contract.

6. In order to determine the level of security classification of the various elements of a classified contract, the following principles shall apply:

(a) in preparing an SCG, the European Parliament shall take into account all relevant security aspects, including the security classification assigned to information which is provided and approved by the originator of the information for use in respect of the contract;
(b) the overall level of classification of the contract may not be lower than the highest level of classification of any of its elements.

B.2. *Security Aspects Letter (SAL)*

7. The contract-specific security requirements shall be described in a Security Aspects Letter (SAL). The SAL shall, where appropriate, contain the SCG and shall be an integral part of a classified contract or sub-contract.

8. The SAL shall contain the provisions requiring the contractor and/or subcontractor to comply with the minimum standards laid down in this Decision. Non-compliance with those minimum standards may constitute grounds for termination of the contract.

B.3. *Programme/Project Security Instructions (PSI)*

9. Depending on the scope of programmes or projects involving access to or the handling or storage of EUCI, specific Programme/Project Security Instructions (PSI) may be prepared by the contracting authority designated to manage the programme or project concerned.

C. FACILITY SECURITY CLEARANCE (FSC)

10. An FSC shall be granted by the NSA or any other competent security authority of a Member State to indicate, in accordance with national laws and regulations, that an industrial or other entity is capable of protecting EUCI at the level CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET or its equivalent within its facilities. Evidence of the grant of the FSC shall be presented to the European Parliament, as the contracting authority, before a contractor or subcontractor or potential contractor or subcontractor is provided with, or granted access to, EUCI.

11. An FSC shall:
(a) evaluate the integrity of the industrial or other entity;

(b) evaluate ownership, control, and/or any potential for undue influence that may be considered a security risk;

(c) verify that the industrial or any other entity has established a security system at its facility which covers all appropriate security measures necessary for the protection of information or material classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET in accordance with the requirements laid down in this Decision;

(d) verify that the personnel security status of management, owners and employees who are required to have access to information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET has been established in accordance with the requirements laid down in this Decision; and

(e) verify that the industrial or any other entity has appointed a Facility Security Officer who is responsible to its management for enforcing the security obligations within such an entity.

12. Where relevant, the European Parliament, as the contracting authority, shall notify the appropriate NSA or other competent security authority that an FSC is required at the pre-contractual stage or for the performance of the contract. An FSC or Personal Security Clearance (PSC) shall be required at the pre-contractual stage where information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET has to be provided in the course of the bidding process.

13. The contracting authority shall not award a classified contract to a preferred bidder until it has received confirmation from an NSA or other competent security authority of the Member State in which the contractor or subcontractor concerned is registered that, where required, an appropriate FSC has been issued.

14. Any competent security authority which has issued an FSC shall notify the European Parliament, as contracting authority, about any changes affecting that FSC. In the case of a sub-contract, the competent security authority shall be informed accordingly.

15. Withdrawal of an FSC by the relevant NSA or other competent security authority shall constitute sufficient grounds for the European Parliament, as the contracting authority, to terminate a classified contract or exclude a bidder from the competition.

D. CLASSIFIED CONTRACTS AND SUBCONTRACTS

16. Where classified information is provided to potential bidders at the pre-contractual stage, the invitation to bid shall contain a provision obliging any of them that fail to submit a bid or that are not selected to return all classified documents within a specified period.

17. Once a classified contract or subcontract has been awarded, the European Parliament, as the contracting authority, shall notify the NSA of the contractor or subcontractor and/or any other competent security authority about the security provisions of the classified contract.

18. Upon the termination of such a contract, the European Parliament, as the contracting authority (and/or the competent security authority, as appropriate, in the case of a subcontract) shall promptly notify the NSA or any other competent security authority of the Member State in which the contractor or subcontractor is registered.

19. As a general rule, the contractor or subcontractor shall be required, upon termination of the classified contract or subcontract, to return to the contracting authority any classified information held by it.

20. Specific provisions for the disposal of classified information during the performance of the contract or upon its termination shall be laid down in the SAL.

21. Where the contractor or subcontractor is authorised to retain classified information after termination of a contract, the minimum standards contained in this Decision shall continue to apply and the confidentiality of EUCI shall be protected by the contractor or subcontractor.

22. The conditions under which the contractor may subcontract shall be defined in the call for tenders and in the contract.

23. A contractor shall obtain permission from the European Parliament, as the contracting authority, before subcontracting any parts of a classified contract. No subcontract may be awarded to industrial or other entities registered in a third State which has not concluded a security of information agreement with the Union.

24. The contractor shall be responsible for ensuring that all subcontracting activities are undertaken in accordance with the minimum standards laid down in this Decision and shall not provide EUCI to a subcontractor without the prior written consent of the contracting

authority.

25. With regard to classified information created or handled by the contractor or subcontractor, the rights vested in the originator shall be exercised by the contracting authority.

E. VISITS IN CONNECTION WITH CLASSIFIED CONTRACTS

26. Where the European Parliament, contractors or subcontractors require access to information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET in each other's premises for the performance of a classified contract, visits shall be arranged in liaison with the NSAs or any other competent security authority concerned. However, in the context of specific projects, the NSAs may also agree on a procedure whereby such visits can be arranged directly.

27. All visitors shall hold an appropriate PSC and have a 'need to know' for access to the classified information related to the European Parliament contract.

28. Visitors shall be given access only to classified information which relates to the purpose of the visit.

F. TRANSMISSION AND CARRIAGE OF CLASSIFIED INFORMATION

29. With regard to the transmission of classified information by electronic means, the relevant provisions of security notice 3 shall apply.

30. With regard to the transport of classified information, the relevant provisions of security notice 4 and the relevant handling instructions shall apply.

31. For the transport of classified material as freight, the following principles shall be applied when determining security arrangements:

(a) security shall be assured at all stages during transportation from the point of origin to the final destination;

(b) the degree of protection afforded to a consignment shall be determined by the highest classification level of material contained within it;

(c) an FSC at the appropriate level shall be obtained for companies providing transportation. In such cases, personnel handling the consignment shall be security cleared in accordance with Annex I;

(d) prior to any cross-border movement of material classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL or as SECRET UE/EU SECRET or its equivalent, a transportation plan shall be drawn up by the consignor and approved by the Secretary-General;

(e) journeys shall as far as possible be undertaken from a given point of departure to a given destination point, and shall be completed as quickly as circumstances permit;

(f) the route taken shall wherever possible pass through the territory of Member States.

G. TRANSFER OF CLASSIFIED INFORMATION TO CONTRACTORS LOCATED IN THIRD STATES

32. Classified information shall be transferred to contractors and subcontractors located in third States in accordance with security measures agreed between the European Parliament, as the contracting authority, and the third State concerned in which the contractor is registered.

H. HANDLING AND STORAGE OF INFORMATION CLASSIFIED AT THE LEVEL RESTREINT UE/EU RESTRICTED

33. In liaison, as appropriate, with the NSA of the Member State concerned, the European Parliament, as the contracting authority, shall be entitled to conduct visits to contractors'/subcontractors' facilities on the basis of contractual provisions in order to verify that the relevant security measures for the protection of EUCI at the level RESTREINT UE/EU RESTRICTED, as required under the contract, have been put in place.

34. To the extent necessary under national laws and regulations, NSAs or any other competent security authorities shall be notified by the European Parliament, as the contracting authority, of contracts or subcontracts containing information classified at the level RESTREINT UE/EU RESTRICTED.

35. An FSC or a PSC for contractors or subcontractors and their personnel shall not be required in the case of contracts awarded by the European Parliament which contain information classified at the level RESTREINT UE/EU RESTRICTED.

36. The European Parliament, as the contracting authority, shall examine the responses to invitations to tender for contracts which require access to information classified at the level RESTREINT UE/EU RESTRICTED, notwithstanding any requirements relating to FSCs or PSCs which may exist under national laws and regulations.

37. The conditions under which the contractor may subcontract shall be defined in the call for tenders and in the contract.

38. Where a contract involves the handling of information classified at the level RESTREINT UE/EU RESTRICTED in communication and information systems operated by a contractor, the European Parliament, as contracting authority, shall ensure that the contract or any subcontract specifies the necessary technical and administrative requirements regarding accreditation of the communication and information systems commensurate with the assessed risk, taking account of all relevant factors. The scope of accreditation of such communication and information systems shall be agreed between the contracting authority and the relevant NSA.

SECURITY NOTICE 6

BREACHES OF SECURITY, LOSS OR COMPROMISE OF CONFIDENTIAL INFORMATION

1. A breach of security occurs as the result of an act or omission contrary to this Decision which might endanger or compromise confidential information.

2. Compromise of confidential information occurs when it has fallen, wholly or in part, into the hands of unauthorised persons, i.e. persons having neither the appropriate security clearance or the necessary need-to-know, or if the likelihood exists of such an event having occurred.

3. Confidential information may be compromised as a result of carelessness, negligence or indiscretion, as well as by the activities of services which target the Union or of subversive organisations.

4. In the event that the Secretary-General discovers or is informed of a proven or suspected breach of security, loss or compromise relating to confidential information, he/she shall:

(a) establish the facts;
(b) assess and minimise the damage done;
(c) take action to prevent a recurrence;
(d) notify the competent authority of the third party or Member State that originated or forwarded the confidential information.

Where the case concerns a Member of the European Parliament, the Secretary-General shall act in liaison with the President of Parliament.

If the information is received from another Union Institution, the Secretary-General shall act in conformity with the appropriate security measures for classified information and the established arrangements laid down pursuant to the Framework Agreement with the Commission or the Interinstitutional Agreement with the Council.

5. All persons required to handle confidential information shall be thoroughly briefed on security procedures, the dangers of indiscreet conversation and their relationships with the media, and shall, where appropriate, sign a declaration that they will not disclose the contents of confidential information to third persons, that they will respect the

obligation to protect classified information and that they acknowledge the consequences of any failure to do so. The access to or use of classified information by a person who has not been briefed and signed the corresponding declaration shall be considered a breach of security.

6. Members of the European Parliament, Parliament officials and other Parliament employees working for political groups or contractors shall immediately report to the Secretary-General any breach of security, loss or compromise of confidential information which may come to their notice.

7. Any person responsible for compromising confidential information shall be subject to disciplinary action in accordance with the relevant rules and regulations. Such action shall be without prejudice to any legal action that may be brought pursuant to the applicable law.

8. Without prejudice to other legal action, breaches committed by Parliament officials and other Parliament employees working for political groups shall entail the application of the procedures and penalties provided for in Title VI of the Staff Regulations.

9. Without prejudice to other legal action, breaches committed by Members of the European Parliament shall be dealt with in accordance with Rule 9(2) and Rules 152, 153 and 154 of Parliament's Rules of Procedure.

2.3. TARYBOJE POSĖDŽIAVUSIŲ EUROPOS SĄJUNGOS VALSTYBIŲ NARIŲ SUSITARIMAS DĖL ĮSLAPTINTOS INFORMACIJOS, KURIA KEIČIAMASI EUROPOS SĄJUNGOS INTERESAIS, APSAUGOS

Taryboje posėdžiavusių Europos Sąjungos valstybių narių

SUSITARIMAS

dėl įslaptintos informacijos, kuria keičiamasi Europos Sąjungos interesais, apsaugos

2011/C 202/05

TARYBOJE POSĖDŽIAVĘ EUROPOS SĄJUNGOS VALSTYBIŲ NARIŲ VYRIAUSYBIŲ ATSTOVAI,

kadangi:

(1) Europos Sąjungos valstybės narės (toliau – Šalys) pripažįsta, jog siekiant visapusiškai ir veiksmingai konsultuotis ir bendradarbiauti, gali prireikti tarpusavyje ir su Europos Sąjungos institucijomis ar Europos Sąjungos įsteigtomis agentūromis, įstaigomis ar biurais keistis įslaptinta informacija Europos Sąjungos interesais.

(2) Šalys turi bendrą norą – prisidėti prie nuoseklios ir išsamios bendros sistemos, skirtos įslaptintos informacijos, gaunamos iš Šalių, iš Europos Sąjungos institucijų ar Europos Sąjungos įsteigtų agentūrų, įstaigų arba biurų bei iš trečiųjų šalių ar tarptautinių organizacijų apsaugai Europos Sąjungos interesais, įdiegimo.

(3) Šalys supranta, kad būtina nustatyti tinkamas prieigos prie tokios įslaptintos informacijos ir keitimosi ja saugumo priemones, siekiant tą informaciją apsaugoti,

SUSITARĖ:

1 straipsnis

Šio Susitarimo tikslas – užtikrinti, kad Šalys apsaugotų įslaptintą informaciją:

a) kuri yra gaunama iš Europos Sąjungos institucijų ar Europos Sąjungos įsteigtų agentūrų, įstaigų ar biurų ir kuri pateikiama Šalims arba kuria su Šalimis keičiamasi;
b) kuri yra gaunama iš Šalių ir pateikiama Europos Sąjungos institucijoms ar Europos Sąjungos įsteigtoms agentūroms, įstaigoms ar biurams arba kuria su jomis keičiamasi;
c) kuri yra gaunama iš Šalių, siekiant pateikti ją kitoms Šalims arba su Šalimis ja keistis Europos Sąjungos interesais, ir kuri yra pažymėta, siekiant nurodyti, kad jai taikomas šis Susitarimas;
d) kurią iš trečiųjų valstybių ar tarptautinių organizacijų yra gavusios Europos Sąjungos institucijos ar Europos Sąjungos įsteigtos agentūros, įstaigos ar biurai ir kuri yra pateikiama Šalims arba kuria su Šalimis keičiamasi.

2 straipsnis

Šiame Susitarime „įslaptinta informacija“ – bet kokia forma esanti informacija ir medžiaga, kurios neteisėtas atskleidimas padarytų įvairaus dydžio žalos Europos Sąjungos arba vienos ar kelių valstybių narių interesams ir kuri pažymėta viena iš ES slaptumo žymų arba priede nurodyta ją atitinkančia slaptumo žyma:

– TRÈS SECRET UE/EU TOP SECRET. Šia žyma žymima informacija ir medžiaga, kurios neteisėtas atskleidimas padarytų ypatingai didelės žalos esminiams Europos Sąjungos arba vienos ar kelių valstybių narių interesams;
– SECRET UE/EU SECRET. Šia žyma žymima informacija ir medžiaga, kurios neteisėtas atskleidimas rimtai pakenktų esminiams Europos Sąjungos arba vienos ar kelių valstybių narių interesams;
– CONFIDENTIEL UE/EU CONFIDENTIAL. Šia žyma žymima informacija ir medžiaga, kurios neteisėtas atskleidimas pakenktų esminiams Europos Sąjungos arba vienos ar kelių valstybių narių interesams;
– RESTREINT UE/EU RESTRICTED. Šia žyma žymima informacija ir medžiaga, kurios neteisėtas atskleidimas būtų nepalankus Europos Sąjungos arba vienos ar kelių valstybių narių interesams.

3 straipsnis

1. Vadovaudamosi savo atitinkamais nacionaliniais įstatymais ir kitais teisės aktais Šalys imasi visų tinkamų priemonių užtikrinti, kad įslaptintai informacijai, kuriai taikomas šis Susitarimas, suteikiamos apsaugos lygis būtų lygiavertis apsaugos lygiui, kuris pagal Europos Sąjungos Tarybos saugumo taisykles suteikiamas ES įslaptintai informacijai, pažymėtai viena iš priede nurodytų atitinkamų slaptumo žymų.

2. Nė viena šio Susitarimo nuostata nedaro poveikio Šalių nacionaliniams įstatymams ar kitiems teisės aktams, susijusiems su galimybe visuomenei susipažinti su dokumentais, taip pat su asmens duomenų apsauga arba įslaptintos informacijos apsauga.

3. Šalys informuoja šio Susitarimo depozitarą apie priede pateiktų slaptumo klasifikacijų pasikeitimus. 11 straipsnis tokiems pranešimams netaikomas.

4 straipsnis

1. Kiekviena Šalis užtikrina, kad įslaptinta informacija, kuri pateikiama arba kuria keičiamasi pagal šį Susitarimą nebūtų:

a) išslaptinta ir nebūtų sumažintas jos slaptumo žymos laipsnis be išankstinio rašytinio įslaptintos informacijos rengėjo sutikimo;
b) panaudota kitiems nei įslaptintos informacijos rengėjo nustatytiems tikslams;
c) atskleista jokiai trečiajai valstybei ar tarptautinei organizacijai be išankstinio rašytinio įslaptintos informacijos rengėjo sutikimo ir be tinkamo susitarimo ar administracinio susitarimo su ta trečiąja valstybe ar tarptautine organizacija dėl įslaptintos informacijos apsaugos.

2. Vadovaudamasi savo konstitucinėmis normomis, nacionaliniais įstatymais ir kitais teisės aktais, kiekviena Šalis laikosi įslaptintos informacijos rengėjo sutikimo principo.

5 straipsnis

1. Kiekviena Šalis užtikrina, kad prieiga prie įslaptintos informacijos būtų suteikiama laikantis principo „būtina žinoti“.

2. Šalys garantuoja, kad prieiga prie įslaptintos informacijos, kuri pažymėta CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma ar priede nurodyta jas atitinkančia slaptumo žyma, yra suteikiama tik asmenims, kurie turi tinkamą darbo su įslaptinta informacija leidimą arba kurie dėl jų vykdomų funkcijų yra kitu būdu pagal nacionalinius įstatymus ir kitus teisės aktus tinkamai įgalioti.

3. Kiekviena Šalis užtikrina, kad visi asmenys, kuriems suteikta prieiga prie įslaptintos informacijos, būtų informuojami apie jų pareigą pagal atitinkamas saugumo taisykles apsaugoti tokią informaciją.

4. Gavusios prašymą, Šalys, laikydamosi savo atitinkamų nacionalinių įstatymų ir kitų teisės aktų, teikia abipusę pagalbą vykdant asmenų, kuriems reikia išduoti leidimus dirbti su įslaptinta informacija, kandidatūrų tikrinimą.

5. Laikydamasi savo nacionalinių įstatymų ir kitų teisės aktų, kiekviena Šalis užtikrina, kad bet kuris jos jurisdikcijai priklausantis subjektas, kuris gali gauti ar rengti įslaptintą informaciją, turi tinkamą leidimą dirbti su įslaptinta informacija ir kad tokie subjektai yra pajėgūs užtikrinti tinkamą apsaugą tinkamu saugumo lygiu, kaip numatyta 3 straipsnio 1 dalyje.

6. Šio Susitarimo taikymo srityje Šalys gali pripažinti kitos Šalies išduotus personalui ir patalpoms skirtus leidimus dirbti su slapta informacija.

6 straipsnis

Šalys užtikrina, kad visa įslaptinta informacija, kuriai taikomas šis Susitarimas ir kurią Šalys persiunčia, kuria keičiasi ar perduoda savo teritorijoje ar tarpusavyje, būtų tinkamai apsaugota, kaip numatyta 3 straipsnio 1 dalyje.

7 straipsnis

Kiekviena Šalis užtikrina, kad būtų įgyvendintos tinkamos priemonės, skirtos įslaptintos informacijos, kuri yra tvarkoma, saugoma ar perduodama ryšių ir informacinėse sistemose, apsaugos priemonės, kaip numatyta 3 straipsnio 1 dalyje. Tokios priemonės turi užtikrinti įslaptintos informacijos konfidencialumą, integralumą, prieinamumą ir atitinkamais atvejais atsakomybės už informaciją prisiėmimą bei autentišku-

mą, taip pat tinkamo lygio su ta informacija susijusių veiksmų apskaitą ir atsekamumą.

8 straipsnis

Šalys, viena kitai pateikusios prašymą, teikia reikiamą informaciją apie savo atitinkamas saugumo taisykles ir teisės aktus.

9 straipsnis

1. Vadovaudamosi atitinkamais nacionaliniais įstatymais ir kitais teisės aktais, Šalys imasi visų tinkamų priemonių, siekdamos ištirti atvejus, kai žinoma arba kai esama pagrįstų priežasčių įtarti, kad įslaptinta informacija, kuriai taikomas šis Susitarimas, buvo neteisėtai atskleista arba prarasta.

2. Šalis, kuri nustato, kad įslaptinta informacija buvo neteisėtai atskleista arba prarasta, atitinkamais kanalais nedelsdama informuoja įslaptintos informacijos rengėją apie tokį įvykį ir vėliau informuoja įslaptintos informacijos rengėją apie galutinius tyrimo rezultatus bei ištaisomąsias priemones, kurių buvo imtasi, siekiant užkirsti kelią tokių įvykių pasikartojimui. Gavusi prašymą bet kuri kita susijusi Šalis gali teikti paramą tyrimui atlikti.

10 straipsnis

1. Šis Susitarimas nedaro poveikio galiojantiems bet kurios Šalies sudarytiems susitarimams ar administraciniams susitarimams dėl įslaptintos informacijos apsaugos ar keitimosi ja.

2. Šis Susitarimas neužkerta kelio Šalims sudaryti kitus susitarimus ar administracinius susitarimus, susijusius su jų pateiktos įslaptintos informacijos apsauga ar keitimusi ja, su sąlyga, kad tokie susitarimai neprieštarauja šiam Susitarimui.

11 straipsnis

Šį Susitarimą galima iš dalies keisti Šalims dėl to susitarus tarpusavyje raštu. Visi pakeitimai įsigalioja apie juos pranešus pagal 13 straips-

nio 2 dalį.

12 straipsnis

Visi dviejų ar daugiau Šalių ginčai dėl šio Susitarimo aiškinimo ar taikymo sprendžiami atitinkamų Šalių tarpusavio konsultacijomis.

13 straipsnis

1. Šalys praneša Europos Sąjungos generaliniam sekretoriui apie šio Susitarimo įsigaliojimui būtinų vidaus procedūrų užbaigimą.

2. Šis Susitarimas įsigalioja antro mėnesio, einančio po to, kai paskutinė Šalis pranešė Europos Sąjungos generaliniam sekretoriui apie šio Susitarimo įsigaliojimui būtinų vidaus procedūrų užbaigimą, pirmą dieną.

3. Europos Sąjungos generalinis sekretorius yra šio Susitarimo, skelbiamo *Europos Sąjungos oficialiajame leidinyje*, depozitaras.

14 straipsnis

Šis Susitarimas sudarytas vienu originalo egzemplioriumi airių, anglų, bulgarų, čekų, danų, estų, graikų, ispanų, italų, latvių, lenkų, lietuvių, maltiečių, olandų, portugalų, prancūzų, rumunų, slovakų, slovėnų, suomių, švedų, vengrų ir vokiečių kalbomis; visi dvidešimt trys tekstai yra vienodai autentiški.

TAI PALIUDYDAMI, tinkamai įgalioti Taryboje posėdžiavę valstybių narių vyriausybių atstovai pasirašė šį Susitarimą.

Pasirašyta du tūkstančiai vienuoliktų metų gegužės ketvirtą dieną Briuselyje.

PRIEDAS

Saugumo klasifikacijų atitikmenys

ES	TRÈS SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Belgija	Très Secret (Loi 1998 12 11) Zeer Geheim (Wet 1998 12 11)	Secret (Loi 1998 12 11) Geheim (Wet 1998 12 11)	Confidentiel (Loi 1998 12 11) Vertrouwelijk (Wet 1998 12 11)	*pastaba toliau* ([1])
Bulgarija	Строго секретно	Секретно	Поверително	За служебно ползване
Čekija	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Danija	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Vokietija	STRENG GEHEIM	GEHEIM	VS ([2]) – VERTRAULICH	VS – NUR FÜR DEN DIENSTGEBRAUCH
Estija	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Airija	Top Secret	Secret	Confidential	Restricted
Graikija	Άκρως Απόρρητο Santrumpa: ΑΑΠ	Απόρρητο Santrumpa: (ΑΠ)	Εμπιστευτικό Santrumpa: (ΕΜ)	Περιορισμένης Χρήσης Santrumpa: (ΠΧ)
Ispanija	SECRETO	RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
Prancūzija	Très Secret Défense	Secret Défense	Confidentiel Défense	*pastaba toliau* ([3])
Italija	Segretissimo	Segreto	Riservatissimo	Riservato
Kipras	Άκρως Απόρρητο Santrumpa: (ΑΑΠ)	Απόρρητο Santrumpa: (ΑΠ)	Εμπιστευτικό Santrumpa: (ΕΜ)	Περιορισμένης Χρήσης Santrumpa: (ΠΧ)
Latvija	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Lietuva	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Liuksemburgas	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Vengrija	Szigorúan titkos!	Titkos!	Bizalmas!	Korlátozott terjesztésű!
Malta	L-Ogħla Segretezza	Sigriet	Kunfidenzjali	Ristrett

Nyderlandai	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Austrija	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Lenkija	Ściśle tajne	Tajne	Poufne	Zastrzeżone
Portugalija	Muito Secreto	Secreto	Confidencial	Reservado
Rumunija	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu
Slovėnija	Strogo tajno	Tajno	Zaupno	Interno
Slovakija	Prísne tajné	Tajné	Dôverné	Vyhradené
Suomija	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Švedija ([4])	HEMLIG/TOP SECRET HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG/SECRET HEMLIG	HEMLIG/CONFIDENTIAL HEMLIG	HEMLIG/RESTRICTED HEMLIG
Jungtinė Karalystė	Top Secret	Secret	Confidential	Restricted

([1]) *Diffusion Restreinte / Beperkte Verspreiding* Belgijoje nėra saugumo žyma. RESTREINT UE/EU RESTRICTED žyma pažymėtą informaciją Belgija tvarko ir saugo taip pat griežtai kaip nustatyta Europos Sąjungos Tarybos saugumo taisyklėse aprašytais standartais ir procedūromis.

([2]) Vokietija: VS – *Verschlusssache*.

([3]) Prancūzijos nacionalinėje sistemoje žyma RESTREINT nenaudojama. RESTREINT UE/EU RESTRICTED žyma pažymėtą informaciją Prancūzija tvarko ir saugo taip pat griežtai, kaip nustatyta Europos Sąjungos Tarybos saugumo taisyklėse aprašytais standartais ir procedūromis.

([4]) Švedija: viršutinėje eilutėje nurodytas saugumo klasifikacijos žymas naudoja gynybos institucijos, o nurodytas apatinėje eilutėje – kitos institucijos.

2.4. AGREEMENT BETWEEN THE MEMBER STATES OF THE EUROPEAN UNION, MEETING WITHIN THE COUNCIL, REGARDING THE PROTECTION OF CLASSIFIED INFORMATION EXCHANGED IN THE INTERESTS OF THE EUROPEAN UNION

AGREEMENT

between the Member States of the European Union, meeting within the Council, regarding the protection of classified information exchanged in the interests of the European Union

2011/C 202/05

THE REPRESENTATIVES OF THE GOVERNMENTS OF THE MEMBER STATES OF THE EUROPEAN UNION, MEETING WITHIN THE COUNCIL,

Whereas:

(1) The Member States of the European Union (hereinafter referred to as 'the Parties') recognise that full and effective consultation and cooperation may require the exchange of classified information among them in the interests of the European Union, and between them and European Union institutions or agencies, bodies or offices established by the latter.

(2) The Parties share the common desire to contribute to putting in place a coherent and comprehensive general framework for the protection of classified information originating in the Parties in the interests of the European Union, in European Union institutions, or in agencies, bodies or offices established by the latter or received from third States or international organisations in this context.

(3) The Parties are conscious that access to and exchanges of such classified information require appropriate security measures for its protection,

HAVE AGREED AS FOLLOWS:

Article 1

The purpose of this Agreement is to ensure the protection by the Parties of classified information:

(a) originating in European Union institutions, or in agencies, bodies or offices established by the latter and provided to or exchanged with the Parties;

(b) originating in the Parties and provided to or exchanged with European Union institutions, or agencies, bodies or offices established by the latter;

(c) originating in the Parties in order to be provided or exchanged between them in the interests of the European Union and marked to indicate that it is subject to this Agreement;

(d) received by European Union institutions or agencies, bodies or offices established by the latter from third States or international organisations and provided to or exchanged with the Parties.

Article 2

For the purposes of this Agreement, 'classified information' shall mean any information or material, in any form, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union, or of one or more of the Member States, and which bears one of the following EU classification markings or a corresponding classification marking as set out in the Annex:

– ‘TRÈS SECRET UE/EU TOP SECRET’. This marking is applied to information and material the unauthorised disclosure of which could cause exceptionally grave prejudice to the essential interests of the European Union or of one or more of the Member States.
– ‘SECRET UE/EU SECRET’. This marking is applied to information and material the unauthorised disclosure of which could seriously harm the essential interests of the European Union or of one or more of the Member States.
– ‘CONFIDENTIEL UE/EU CONFIDENTIAL’. This marking is applied to information and material the unauthorised disclosure of which could harm the essential interests of the European Union or of one or more of the Member States.
– ‘RESTREINT UE/EU RESTRICTED’. This marking is applied to information and material the unauthorised disclosure of which could be disadvantageous to the interests of the European Union or of one or more of the Member States.

Article 3

1. The Parties shall take all appropriate measures in accordance with their respective national laws and regulations to ensure that the level of protection afforded to classified information subject to this Agreement is equivalent to that afforded by the security rules of the Council of the European Union for protecting EU classified information bearing a corresponding classification marking as set out in the Annex.

2. Nothing in this Agreement shall cause prejudice to the national laws and regulations of the Parties regarding public access to documents, the protection of personal data or the protection of classified information.

3. The Parties shall notify the depositary for this Agreement of any changes to the security classifications set out in the Annex. Article 11 shall not apply to such notifications.

Article 4

1. Each Party shall ensure that classified information provided or exchanged under this Agreement is not:

(a) downgraded or declassified without the prior written consent of the originator;
(b) used for purposes other than those established by the originator;

(c) disclosed to any third State or international organisation without the prior written consent of the originator and an appropriate agreement or arrangement for the protection of classified information with the third State or international organisation concerned.

2. The principle of originator consent shall be respected by each Party in accordance with its constitutional requirements, national laws and regulations.

Article 5

1. Each Party shall ensure that access to classified information is granted on the basis of the need-to-know principle.

2. The Parties shall guarantee that access to classified information bearing the classification marking 'CONFIDENTIEL UE/EU CONFIDENTIAL' or above or a corresponding classification marking as set out in the Annex is granted only to individuals who hold an appropriate security clearance or who are otherwise duly authorised by virtue of their functions in accordance with national laws and regulations.

3. Each Party shall ensure that all individuals granted access to classified information are informed of their responsibilities to protect such information in accordance with the appropriate security regulations.

4. Upon request, the Parties shall, in accordance with their respective national laws and regulations, provide mutual assistance in carrying out security investigations relating to security clearances.

5. In accordance with its national laws and regulations, each Party shall ensure that any entity under its jurisdiction which may receive or generate classified information is appropriately security cleared and is capable of providing suitable protection, as provided for in Article 3(1), at the appropriate security level.

6. Within the scope of this Agreement, each Party may acknowledge the personnel and facility security clearances issued by another Party.

Article 6

The Parties shall ensure that all classified information within the scope of this Agreement transmitted, exchanged or transferred within or between any of them shall be appropriately protected, as provided for in Article 3(1).

Article 7

Each Party shall ensure that appropriate measures are implemented for the protection, as provided for in Article 3(1), of classified information processed, stored or transmitted in communication and information systems. Such measures shall ensure the confidentiality, integrity, availability and, where applicable, non-repudiation and authenticity of classified information as well as an appropriate level of accountability and traceability of actions in relation to that information.

Article 8

The Parties shall provide one another, upon request, with relevant information about their respective security rules and regulations.

Article 9

1. The Parties shall take all appropriate measures, in accordance with their respective national laws and regulations, to investigate cases where it is known or where there are reasonable grounds for suspecting that classified information within the scope of this Agreement has been compromised or lost.

2. A Party which discovers a compromise or loss shall, through the appropriate channels, immediately inform the originator of such an occurrence and subsequently inform the originator of the final results of the investigation and of the corrective measures taken to prevent a recurrence. Upon request, any other relevant Party may provide investigative assistance.

Article 10

1. This Agreement shall not affect existing agreements or arrangements on the protection or exchange of classified information entered into by any Party.

2. This Agreement shall not preclude the Parties from entering into other agreements or arrangements relating to the protection and exchange of classified information originated by them, provided that such agreements or arrangements do not conflict with this Agreement.

Article 11

This Agreement may be amended by written agreement between the Parties. Any amendment shall enter into force upon notification pursuant to Article 13(2).

Article 12

Any dispute between two or more Parties relating to the interpretation or application of this Agreement shall be settled through consultations between the Parties concerned.

Article 13

1. The Parties shall notify the Secretary-General of the Council of the European Union of the completion of the internal procedures necessary for the entry into force of this Agreement.

2. This Agreement shall enter into force on the first day of the second month following notification to the Secretary-General of the Council of the European Union of the completion of the internal procedures necessary for its entry into force by the last Party to take this step.

3. The Secretary-General of the Council of the European Union shall act as depositary for this Agreement which shall be published in the *Official Journal of the European Union*.

Article 14

This Agreement is drawn up in a single original in the Bulgarian, Czech, Danish, Dutch, English, Estonian, Finnish, French, German, Greek, Hungarian, Irish, Italian, Latvian, Lithuanian, Maltese, Polish, Portuguese, Romanian, Slovak, Slovenian, Spanish and Swedish languages, all 23 texts being equally authentic.

IN WITNESS WHEREOF, the undersigned Representatives of the Governments of the Member States, meeting within the Council, have signed this Agreement.

Done at Brussels on the fourth day of May in the year two thousand and eleven.

ANNEX

Equivalence of security classifications

EU	TRÈS SECRET UE/ EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/ EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Belgium	Très Secret (Loi 11.12.1998) Zeer Geheim (Wet 11.12.1998)	Secret (Loi 11.12.1998) Geheim (Wet 11.12.1998)	Confidentiel (Loi 11.12.1998) Vertrouwelijk (Wet 11.12.1998)	*nota below* ([1])
Bulgaria	Строго секретно	Секретно	Поверително	За служебно ползване
Czech Republic	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Denmark	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Germany	STRENG GEHEIM	GEHEIM	VS ([2]) – VERTRAULICH	VS – NUR FÜR DEN DIENSTGEBRAUCH
Estonia	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Ireland	Top Secret	Secret	Confidential	Restricted
Greece	Άκρως Απόρρητο Abr: ΑΑΠ	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Spain	SECRETO	RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
France	Très Secret Défense	Secret Défense	Confidentiel Défense	*nota below* ([3])
Italy	Segretissimo	Segreto	Riservatissimo	Riservato
Cyprus	Άκρως Απόρρητο Abr: (ΑΑΠ)	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Latvia	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Lithuania	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Luxembourg	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Hungary	Szigorúan titkos!	Titkos!	Bizalmas!	Korlátozott terjesztésű!

Malta	L-Ogħla Segretezza	Sigriet	Kunfidenzjali	Ristrett
Netherlands	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Austria	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Poland	Ściśle tajne	Tajne	Poufne	Zastrzeżone
Portugal	Muito Secreto	Secreto	Confidencial	Reservado
Romania	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu
Slovenia	Strogo tajno	Tajno	Zaupno	Interno
Slovakia	Prísne tajné	Tajné	Dôverné	Vyhradené
Finland	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Sweden ([4])	HEMLIG/TOP SECRET HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG/SECRET HEMLIG	HEMLIG/CONFIDENTIAL HEMLIG	HEMLIG/RESTRICTED HEMLIG
United Kingdom	Top Secret	Secret	Confidential	Restricted

([1]) 'Diffusion Restreinte/Beperkte Verspreiding' is not a security classification in Belgium. Belgium handles and protects 'RESTREINT UE/EU RESTRICTED' information in a manner no less stringent than the standards and procedures described in the security rules of the Council of the European Union.

([2]) Germany: VS = 'Verschlusssache'.

([3]) France does not use the classification 'RESTREINT' in its national system. France handles and protects 'RESTREINT UE/EU RESTRICTED' information in a manner no less stringent than the standards and procedures described in the security rules of the Council of the European Union.

([4]) Sweden: the security classification markings in the top row are used by the defence authorities and the markings in the bottom row by other authorities.

2.5. 2013 M. RUGSĖJO 23 D. TARYBOS SPRENDIMAS DĖL ES ĮSLAPTINTOS INFORMACIJOS APSAUGAI UŽTIKRINTI SKIRTŲ SAUGUMO TAISYKLIŲ

TARYBOS SPRENDIMAS

2013 m. rugsėjo 23 d.

Dėl ES įslaptintos informacijos apsaugai užtikrinti skirtų saugumo taisyklių (2013/488/ES)

EUROPOS SĄJUNGOS TARYBA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo, ypač į jos 240 straipsnio 3 dalį,

atsižvelgdama į 2009 m. gruodžio 1 d. Tarybos sprendimą 2009/937/ES, patvirtinantį Tarybos darbo tvarkos taisykles ([1]), ypač į jo 24 straipsnį,

kadangi:

(1) siekiant plėtoti Tarybos veiklą visose srityse, kuriose reikia tvarkyti įslaptintą informaciją, tikslinga sukurti Tarybą, jos Generalinį sekretoriatą ir valstybes nares apimančią įslaptintos informacijos apsaugą užtikrinančią visapusišką saugumo sistemą;
(2) šis sprendimas turėtų būti taikomas tais atvejais, kai Taryba, jos parengiamieji organai ir Tarybos Generalinis sekretoriatas (TGS) tvarko ES įslaptintą informaciją (ESĮI);
(3) vadovaudamosi savo nacionaliniais įstatymais ir kitais teisės aktais ir tiek, kiek reikia Tarybos veiklai užtikrinti, valstybės narės turėtų laikytis šio sprendimo, kai jų kompetentingos institucijos, personalas ir rangovai tvarko ESĮI, kad visi būtų tikri, jog yra užtikrinta lygiavertė ESĮI apsauga;

(4) Taryba, Komisija ir Europos išorės veiksmų tarnyba (EIVT) yra įsipareigojusios taikyti lygiaverčius ESĮI apsaugą užtikrinančius saugumo standartus;

(5) Taryba pabrėžia, jog svarbu, kad Europos Parlamentas ir kitos Europos Sąjungos institucijos, įstaigos, tarnybos ar agentūros atitinkamais atvejais prisidėtų prie įslaptintos informacijos apsaugos principų, standartų ir taisyklių, būtinų siekiant apsaugoti Europos Sąjungos ir jos valstybių narių interesus, įgyvendinimo;

(6) Taryba, laikydamasi šio sprendimo ir galiojančių tarpinstitucinių susitarimų, turėtų nustatyti tinkamą Tarybos turimos ESĮI dalijimosi atitinkamai su kitomis Europos Sąjungos institucijomis, įstaigomis, tarnybomis ar agentūromis sistemą;

(7) pagal Europos Sąjungos sutarties (ES sutartis) V antraštinės dalies 2 skyrių įsteigtos Europos Sąjungos įstaigos ir agentūros, Europolas ir Eurojustas, vykdydami savo vidaus darbo organizavimą, turėtų taikyti šiame sprendime nustatytus ESĮI apsaugai užtikrinti skirtus pagrindinius principus ir būtiniausius standartus, jei jie numatyti akte dėl jų įsteigimo;

(8) pagal ES sutarties V antraštinės dalies 2 skyrių nustatytų krizių valdymo operacijų metu turėtų būti taikomos Tarybos patvirtintos ESĮI apsaugai užtikrinti skirtos saugumo taisyklės, jei jos numatytos Tarybos akte dėl tų operacijų nustatymo; jas turėtų taikyti ir jose dalyvaujantis personalas;

(9) ES specialieji įgaliotiniai ir jų darbuotojų grupių nariai turėtų taikyti Tarybos patvirtintas ESĮI apsaugai užtikrinti skirtas saugumo taisykles, jei taip numatyta atitinkame Tarybos akte;

(10) šis sprendimas priimamas nedarant poveikio Sutarties dėl Europos Sąjungos veikimo (SESV) 15 ir 16 straipsniams ir jų įgyvendinamiesiems aktams;

(11) šis sprendimas priimamas nedarant poveikio dabartinei valstybių narių praktikai, susijusiai su nacionalinių parlamentų informavimu apie Europos Sąjungos veiklą;

(12) siekiant užtikrinti, kad, Kroatijos Respublikai prisijungiant prie Europos Sąjungos, ESĮI apsaugai skirtos saugumo taisyklės būtų pradėtos taikyti laiku, šis sprendimas turėtų įsigalioti jo paskelbimo dieną,

PRIĖMĖ ŠĮ SPRENDIMĄ:

1 straipsnis

Tikslas, taikymo sritis ir sąvokų apibrėžtys

1. Šis sprendimas nustato pagrindinius ESĮI apsaugai užtikrinti skirtus saugumo principus ir būtiniausius standartus.

2. Šie pagrindiniai saugumo principai ir būtiniausi standartai taikomi Tarybai bei TGS ir jų privalo laikytis valstybės narės, vadovaudamosi savo atitinkamais nacionaliniais įstatymais ir kitais teisės aktais, kad visi būtų tikri, jog yra užtikrinta lygiavertė ESĮI apsauga.

3. Šio sprendimo taikymo tikslais taikomos A priedėlyje pateiktos sąvokų apibrėžtys.

2 straipsnis

ESĮI sąvokos apibrėžtis, slaptumo žymos ir kitos žymos

1. ES įslaptinta informacija (ESĮI) – bet kuri informacija arba medžiaga, kuriai suteikta ES slaptumo žyma ir kurią neteisėtai atskleidus galėtų būti padaryta tam tikro dydžio žala Europos Sąjungos arba vienos ar kelių valstybių narių interesams.

2. ESĮI žymima viena iš šių slaptumo žymų:

a) TRÈS SECRET UE/ES TOP SECRET: informacija ir medžiaga, kurią neteisėtai atskleidus galėtų būti padaryta ypatingai didelė žala Europos Sąjungos arba vienos ar kelių valstybių narių esminiams interesams;
b) SECRET UE/ES SECRET: informacija ir medžiaga, kurią neteisėtai atskleidus galėtų būti rimtai pakenkta Europos Sąjungos arba vienos ar kelių valstybių narių esminiams interesams;
c) CONFIDENTIEL UE/ES CONFIDENTIAL: informacija ir medžiaga, kurią neteisėtai atskleidus galėtų būti pakenkta Europos Sąjungos arba vienos ar kelių valstybių narių esminiams interesams;
d) RESTREINT UE/ES RESTRICTED: informacija ir medžiaga, kurios neteisėtas atskleidimas galėtų būti nepalankus Europos Sąjungos arba vienos ar kelių valstybių narių interesams.

3. ESĮI žymima slaptumo žyma pagal 2 dalį. Ji gali būti pažymėta papildoma žyma, skirta nurodyti veiklos sritį, su kuria ji yra susijusi, nurodyti įslaptintos informacijos rengėją, apriboti jos platinimą, naudojimą ar suteikimą.

3 straipsnis

Įslaptinimo administravimas

1. Kompetentingos institucijos užtikrina, kad ESĮI būtų žymima tinkama slaptumo žyma, būtų aiškiai nurodoma, kad tai yra įslaptinta informacija, ir jai būtų suteikta slaptumo žyma tik tokiam laikotarpiui, kuris yra būtinas.

2. ESĮI slaptumo žymos laipsnis nesumažinamas arba ji neišslaptinama ir nekeičiamos arba nepanaikinamos 2 straipsnio 3 dalyje nurodytos žymos be išankstinio įslaptintos informacijos rengėjo rašytinio sutikimo.

3. Taryba patvirtina ESĮI rengimo saugumo politiką, kuri apima praktinį žymų vadovą.

4 straipsnis

Įslaptintos informacijos apsauga

1. ESĮI apsaugoma laikantis šio sprendimo.

2. Bet kokios ESĮI turėtojas yra atsakingas už jos apsaugą pagal šį sprendimą.

3. Valstybėms narėms nacionaline slaptumo žyma pažymėtą įslaptintą informaciją įtraukus į Europos Sąjungos struktūras ar tinklus, Taryba ir TGS tą informaciją apsaugo laikydamiesi reikalavimų, taikomų lygiaverčio slaptumo žymos laipsnio ESĮI, kaip nustatyta B priedėlyje pateiktoje slaptumo žymų atitikmenų lentelėje.

4. ESĮI visumos atveju gali būti reikalaujama užtikrinti apsaugos lygį, atitinkantį aukštesnio laipsnio slaptumo žymą, nei jos atskirų komponentų slaptumo žymos.

5 straipsnis

Saugumo rizikos valdymas

1. ESĮI kylančios rizikos valdymas yra procesas. Šio proceso tikslas – nustatyti žinomą saugumo riziką, apibrėžti saugumo priemones tokiai rizikai sumažinti iki priimtino lygio pagal šiame sprendime išdėstytus pagrindinius principus ir būtiniausius standartus ir taikyti tas priemones laikantis nuodugnios apsaugos sąvokos, kaip apibrėžta A priedėlyje. Reguliariai atliekamas tokių priemonių efektyvumo vertinimas.

2. ESĮI apsaugai užtikrinti skirtos saugumo priemonės visą savo gyvavimo ciklą turi atitikti jos slaptumo žymos laipsnį, informacijos ar medžiagos formą ir kiekį, patalpų, kuriose laikoma ESĮI, vietos ir konstrukcijos reikalavimus ir turi būti parenkamos atsižvelgiant į vietos lygiu įvertintą piktavališkos ir (arba) nusikalstamos veiklos, įskaitant šnipinėjimą, sabotažą ar terorizmą, keliamą grėsmę.

3. Nenumatytų atvejų planuose turi būti atsižvelgiama į poreikį apsaugoti ESĮI nepaprastosios padėties atvejais siekiant užkirsti kelią galimybei neteisėtai susipažinti su šia informacija, ją atskleisti ar prarasti jos vientisumą arba galimybę ja naudotis.

4. Veiklos tęstinumo planuose numatomos prevencinės ir atstatymo priemonės siekiant sumažinti didelių klaidų ar incidentų poveikį ESĮI administravimui ir saugojimui.

6 straipsnis

Šio sprendimo įgyvendinimas

1. Remdamasi Saugumo komiteto rekomendacija, Taryba prireikus patvirtina saugumo politiką, kuria nustatomos šio sprendimo įgyvendinimo priemonės.

2. Saugumo komitetas savo lygiu gali susitarti dėl saugumo gairių, kurios skirtos papildyti ar sustiprinti šį sprendimą, ir pritarti Tarybos patvirtintai saugumo politikai.

7 straipsnis

Personalo patikimumas

1. Personalo patikimumas – priemonių taikymas, siekiant užtikrinti, kad galimybė susipažinti su ESĮI būtų suteikta tik asmenims, kurie:
- atitinka principą „būtina žinoti“,
- atitinkamais atvejais turi atitinkamo slaptumo žymos laipsnio asmens patikimumo pažymėjimus ir
- yra informuoti apie jų pareigas.

2. Personalo patikimumo tikrinimo procedūrų tikslas – nustatyti, ar asmeniui, atsižvelgiant į jo lojalumą ir patikimumą, gali būti leidžiama susipažinti su ESĮI.

3. Prieš TGS dirbantiems asmenims, kuriems dėl jų pareigų reikia susipažinti su CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta ESĮI ar ją tvarkyti, leidžiant susipažinti su tokia ESĮI, jų visų patikimumas turi būti patikrintas atitinkamu lygiu. Tokiems asmenims TGS paskyrimų tarnyba turi suteikti leidimą iki nustatytos datos susipažinti su iki tam tikro laipsnio slaptumo žyma pažymėta ESĮI.

4. Prieš 15 straipsnio 3 dalyje nurodytiems valstybių narių darbuotojams, kuriems dėl jų pareigų gali reikėti susipažinti su CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta ESĮI, leidžiant susipažinti su tokia ESĮI, jų patikimumas turi būti patikrintas atitinkamu lygiu arba jie turi turėti kitus tinkamus leidimus atsižvelgiant į jų atliekamas funkcijas pagal nacionalinius įstatymus ir kitus teisės aktus.

5. Visi asmenys, prieš jiems suteikiant leidimą susipažinti su ESĮI, o vėliau – reguliariai, informuojami apie pareigą saugoti ESĮI pagal šį sprendimą ir jie ją patvirtina.

6. Šio straipsnio įgyvendinimo nuostatos išdėstytos I priede.

8 straipsnis

Fizinis saugumas

1. Fizinis saugumas yra fizinių ir techninių apsaugos priemonių taikymas siekiant užkirsti kelią leidimo neturintiems asmenims susipažinti su ESĮI.

2. Fizinės saugumo priemonės skirtos sutrukdyti įsibrauti slaptai arba įsiveržti jėga, atgrasyti nuo neteisėtų veiksmų, sutrukdyti jiems bei juos nustatyti ir sudaryti sąlygas suskirstyti personalą pagal tai, kas gali susipažinti su ESĮI, vadovaujantis principu „būtina žinoti“. Tokios priemonės grindžiamos rizikos valdymo procesu.

3. Fizinio saugumo priemonės taikomos visose patalpose, pastatuose, kabinetuose, salėse ir kitose zonose, kuriose tvarkoma arba saugoma ESĮI, įskaitant zonas, kuriose įrengtos ryšių ir informacinės sistemos, kaip apibrėžta 10 straipsnio 2 dalyje.

4. Zonos, kuriose saugoma CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta ESĮI, įrengiamos kaip saugumo zonos pagal II priedo nuostatas ir patvirtinamos kompetentingos saugumo institucijos.

5. CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėtos ESĮI apsaugai naudojama tik patvirtinta įranga ar prietaisai.

6. Šio straipsnio įgyvendinimo nuostatos išdėstytos II priede.

9 straipsnis

Įslaptintos informacijos administravimas

1. Įslaptintos informacijos administravimas – administracinių ESĮI kontrolės visą jos gyvavimo ciklą priemonių taikymas siekiant papildyti 7, 8 ir 10 straipsniuose numatytas priemones ir atgrasyti nuo tokios informacijos sąmoningo ar tikslingo atskleidimo arba praradimo ir nustatyti tokius atvejus. Tokios priemonės, visų pirma, yra susijusios su ESĮI rengimu, registravimu, kopijavimu, vertimu, slaptumo žymos laipsnio sumažinimu, išslaptinimu, gabenimu ir naikinimu.

2. CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta informacija saugumo tikslais registruojama prieš ją platinant ir ją gavus. TGS kompetentingos tarnybos ir valstybių narių kompetentingos institucijos šiuo tikslu sukuria registratūrų sistemą. Slaptumo žyma TRÈS SECRET UE/ES TOP SECRET pažymėta informacija registruojama tam skirtuose registruose.

3. Tarnybas ir patalpas, kuriose ESĮI tvarkoma arba saugoma, reguliariai tikrina kompetentinga saugumo institucija.

4. Už fiziškai apsaugotų zonų ribų ESĮI iš vienos tarnybos į kitą ir iš vienų patalpų į kitas perduodama šiais būdais:

a) paprastai ESĮI perduodama elektroninėmis priemonėmis apsaugant informaciją pagal 10 straipsnio 6 dalį patvirtintomis šifravimo priemonėmis;

b) kai nenaudojamos a punkte nurodytos priemonės, ESĮI gabenama:

i) elektroninėse laikmenose (pvz., USB atmintinėse, kompaktiniuose diskuose, kietuosiuose diskuose), informaciją apsaugant pagal 10 straipsnio 6 dalį patvirtintomis šifravimo priemonėmis;

ii) visais kitais atvejais, kompetentingos saugumo institucijos nurodytu būdu, laikantis atitinkamų III priede nustatytų apsaugos priemonių.

5. Šio straipsnio įgyvendinimo nuostatos išdėstytos III ir IV prieduose.

10 straipsnis

ESĮI, tvarkomos naudojantis ryšių ir informacinėmis sistemomis, apsauga

1. Informacijos saugumo užtikrinimas (ISU) ryšių ir informacinių sistemų srityje – užtikrinimas, kad tokiose sistemose tvarkoma informacija bus apsaugota ir kad, valdant teisėtiems naudotojams, jos veiks taip, kaip turi veikti, ir tada, kada turi veikti. Veiksmingas ISU užtikrina tinkamą konfidencialumo, vientisumo, prieinamumo, atsakomybės už veiksmus prisiėmimo ir autentiškumo lygį. ISU grindžiamas rizikos valdymo procesu.

2. Ryšių ir informacinė sistema (RIS) – sistema, sudaranti sąlygas tvarkyti informaciją elektroniniu būdu. RIS apima visas sistemos dalis, kurių reikia jos veikimui, įskaitant infrastruktūrą, organizavimą, personalą ir informacijos šaltinius. Šis sprendimas taikomas RIS, kuriose tvarkoma ESĮI.

3. ESĮI RIS tvarkoma laikantis ISU principo.

4. Visa RIS turi būti akredituojama. Akreditavimo tikslas – įsitikinti, kad įgyvendintos visos atitinkamos saugumo priemonės ir kad pasiektas pakankamas ESĮI ir RIS apsaugos lygis, vadovaujantis šiuo sprendimu. Pareiškime dėl akreditavimo nurodomas aukščiausias informacijos, kuri gali būti tvarkoma RIS, slaptumo žymos laipsnis ir atitinkami reikalavimai bei sąlygos.

5. Įgyvendinamos apsaugos priemonės, siekiant apsaugoti RIS, kuriose tvarkoma CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta informacija, kad tokia informacija negalėtų būti neteisėtai atskleista dėl netyčinio elektromagnetinio spinduliavimo (TEMPEST apsaugos priemonės). Tokios apsaugos priemonės turi būti proporcingos neteisėto pasinaudojimo informacija rizikai ir informacijos slaptumo žymos lygiui.

6. Kai ESĮI apsauga užtikrinama šifravimo priemonėmis, tokios priemonės patvirtinamos taip:

a) SECRET UE/ES SECRET ir aukštesnio laipsnio slaptumo žyma pažymėtos informacijos konfidencialumas užtikrinamas taikant šifravimo priemones, kurias remdamasi Saugumo komiteto rekomendacija patvirtina Taryba, vykdydama Kriptografijos patvirtinimo institucijos (KPI) funkcijas;
b) CONFIDENTIEL UE/ES CONFIDENTIAL arba RESTREINT UE/ES RESTRICTED slaptumo žyma pažymėtos informacijos konfidencialumas užtikrinamas taikant šifravimo priemones, kurias remdamasis Saugumo komiteto rekomendacija patvirtina Tarybos Generalinis sekretorius (toliau – Generalinis sekretorius), vykdydamas KPI funkcijas.

Nepažeidžiant b punkto, valstybių narių nacionalinėse sistemose CONFIDENTIEL UE/ES CONFIDENTIAL arba RESTREINT UE/ES RESTRICTED slaptumo žyma pažymėtos ESĮI konfidencialumas gali būti apsaugomas taikant šifravimo priemones, kurias patvirtina valstybės narės KPI.

7. Perduodant ESĮI elektroninėmis priemonėmis naudojamos patvirtintos šifravimo priemonės. Nepaisant šio reikalavimo, esant nepaprastosios padėties sąlygoms arba specifinių techninių konfigūracijų atvejais, kaip nurodyta IV priede, gali būti taikomos specialios procedūros.

8. TGS kompetentingos tarnybos ir valstybių narių kompetentingos institucijos atitinkamai nustato šias ISU funkcijas vykdančias struktūras:

a) ISU instituciją (ISUI);
b) TEMPEST instituciją (TEI);
c) Kriptografijos patvirtinimo instituciją (KPI);
d) Kriptografijos platinimo instituciją (KPLI).

9. TGS kompetentingos tarnybos ir valstybių narių kompetentingos institucijos kiekvienai sistemai atitinkamai nustato:

a) Saugumo akreditavimo instituciją (SAI);
b) ISU operacinę instituciją.

10. Šio straipsnio įgyvendinimo nuostatos išdėstytos IV priede.

11 straipsnis

Pramoninis saugumas

1. Pramoninis saugumas – priemonių, kurias rangovai arba subrangovai taiko derybų dėl sutarčių sudarymo metu ir visą įslaptintų sutarčių gyvavimo ciklą, siekdami užtikrinti ESĮI apsaugą, taikymas. Tokiose sutartyse nenumatoma galimybė susipažinti su slaptumo žyma TRES SECRET UE/ES TOP SECRET pažymėta informacija.

2. TGS sutartimi gali patikėti pramonės arba kitiems subjektams, registruotiems valstybėje narėje arba trečiojoje valstybėje, kuri yra sudariusi susitarimą arba administracinį susitarimą pagal 13 straipsnio 2 dalies a arba b punktą, užduotis, kurioms atlikti reikia arba reikės susipažinti su ESĮI arba ją tvarkyti ar laikyti.

3. TGS, kaip perkančioji institucija, užtikrina, kad sudarant įslaptintas sutartis su pramonės ar kitais subjektais būtų laikomasi šiame sprendime išdėstytų ir sutartyje nurodytų būtiniausių pramoninio saugumo standartų.

4. Kiekvienos valstybės narės nacionalinė saugumo institucija (NSI), paskirtoji saugumo institucija (PSI) ar bet kuri kita kompetentinga institucija, kiek tai įmanoma pagal nacionalinius įstatymus ir kitus teisės aktus, užtikrina, kad jų teritorijoje įregistruoti rangovai ir subrangovai derybų dėl sutarčių sudarymo metu arba vykdydami įslaptintą sutartį imtųsi visų tinkamų ESĮI apsaugos priemonių.

5. Kiekvienos valstybės narės NSI, PSI ar kita kompetentinga saugumo institucija, laikydamosi nacionalinių įstatymų ir kitų teisės aktų, užtikrina, kad atitinkamoje valstybėje narėje įregistruoti rangovai ar subrangovai, dalyvaujantys įslaptintose sutartyse arba subrangos sutartyse, pagal kurias jas vykdant arba prieš jas sudarant turi būti suteikta galimybė savo patalpose susipažinti su įslaptinta informacija, pažymėta slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET, turėtų reikiamą slaptumo žymos laipsnį atitinkantį Įmonės patikimumą patvirtinantį pažymėjimą (ĮPPP).

6. Rangovo ar subrangovo darbuotojams, kuriems vykdant įslaptintą sutartį reikia susipažinti su slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėta informacija,

atitinkama NSI, PSI ar kita kompetentinga saugumo institucija laikydamasi nacionalinių įstatymų ir kitų teisės aktų bei I priede nustatytų būtiniausių saugumo standartų suteikia asmens patikimumo pažymėjimą (APP).

7. Šio straipsnio įgyvendinimo nuostatos išdėstytos V priede.

12 straipsnis

Dalijimasis ESĮI

1. Taryba nustato sąlygas, kuriomis ji gali dalytis savo turima ESĮI su kitomis Europos Sąjungos institucijomis, įstaigomis, tarnybomis ar agentūromis. Tam gali būti sukurta atitinkama sistema, be kita ko, prireikus tuo tikslu sudarant tarpinstitucinius susitarimus ar kitokius susitarimus.

2. Pagal tokią sistemą užtikrinama, kad ESĮI būtų taikoma jos slaptumo žymos lygį atitinkanti apsauga, laikantis pagrindinių principų bei būtiniausių standartų, lygiaverčių nustatytiesiems šiame sprendime.

13 straipsnis

Keitimasis įslaptinta informacija su trečiosiomis valstybėmis ir tarptautinėmis organizacijomis

1. Tarybai nusprendus, kad reikia keistis ESĮI su trečiąja valstybe arba tarptautine organizacija, šiuo tikslu nustatoma tinkama tvarka.

2. Siekdama nustatyti tokią tvarką ir apibrėžti abipusiškumo taisykles dėl įslaptintos informacijos, kuria keičiamasi, apsaugos:

a) Europos Sąjunga sudaro susitarimus su trečiosiomis valstybėmis arba tarptautinėmis organizacijomis dėl keitimuisi ESĮI ir jos apsaugai užtikrinti skirtų saugumo procedūrų (toliau – susitarimai dėl informacijos saugumo);
b) Generalinis sekretorius gali pagal VI priedo 17 punktą TGS vardu sudaryti administracinius susitarimus tuomet, kai ESĮI, kuri turi būti suteikta, slaptumo žymos laipsnis paprastai nėra aukštesnis nei RESTREINT UE/ES RESTRICTED.

3. 2 dalyje nurodytuose susitarimuose dėl informacijos saugumo arba administraciniuose susitarimuose numatomos nuostatos, kuriomis užtikrinama, jog trečiosioms valstybėms arba tarptautinėms organizacijoms gavus ESĮI tai informacijai užtikrinama jos slaptumo žymos laipsnį ati-

tinkanti apsauga, remiantis būtiniausiais standartais, kurie yra ne mažiau griežti nei šiame sprendime nustatyti standartai.

4. Sprendimą suteikti Tarybos parengtą ESĮI trečiajai valstybei arba tarptautinei organizacijai priima Taryba atskirai kiekvienu konkrečiu atveju atsižvelgdama į tokios informacijos pobūdį ir turinį bei gavėjo atitiktį principui „būtina žinoti“ ir įvertinusi naudą Europos Sąjungai. Jeigu Taryba nėra įslaptintos informacijos, kurią prašoma suteikti, rengėja, TGS pirmiausia bando gauti jos įslaptintos informacijos rengėjo raštišką sutikimą suteikti tą informaciją. Jei įslaptintos informacijos rengėjo neįmanoma nustatyti, jo pareigą prisiima Taryba.

5. Įvertinimo vizitai rengiami siekiant įsitikinti, kad trečiojoje valstybėje arba tarptautinėje organizacijoje taikomos ESĮI arba įslaptintos informacijos, kuri suteikta ar kuria keičiamasi, apsaugos priemonės yra veiksmingos.

6. Šio straipsnio įgyvendinimo nuostatos išdėstytos VI priede.

14 straipsnis

ESĮI saugumo pažeidimai ir neteisėtas atskleidimas

1. Saugumo pažeidimu laikomas šiame sprendime nustatytoms saugumo taisyklėms priešingas asmens veiksmas arba neveikimas.

2. Laikoma, kad ESĮI neteisėtai atskleista, jeigu pažeidus saugumo taisykles ji visa arba jos dalis yra atskleista leidimo neturintiems asmenims.

3. Apie visus saugumo pažeidimus arba įtariamus saugumo pažeidimus nedelsiant pranešama kompetentingai saugumo institucijai.

4. Tais atvejais, kai žinoma arba yra pagrįstų priežasčių manyti, kad ESĮI buvo neteisėtai atskleista arba prarasta, NSI ar kita kompetentinga institucija, vadovaudamasi atitinkamais įstatymais ir kitais teisės aktais, imasi visų atitinkamų priemonių:

a) informuoti įslaptintos informacijos rengėją;
b) užtikrinti, kad siekiant nustatyti faktus tokį atvejį nagrinėtų su pažeidimu tiesiogiai nesusijęs personalas;
c) įvertinti galimą Europos Sąjungai ar valstybių narių interesams padarytą žalą;
d) imtis atitinkamų priemonių, kad būtų užkirstas kelias pažeidimui pasikartoti;

e) kad atitinkamos institucijos būtų informuotos apie atliktus veiksmus.

5. Bet kuriam asmeniui, kuris pažeidė šiame sprendime nustatytas saugumo taisykles, gali būti taikomos drausminės priemonės vadovaujantis taikomomis taisyklėmis. Asmeniui, kuris neteisėtai atskleidė ar pametė ESĮI, taikomos drausminės ir (arba) teisinės priemonės vadovaujantis taikomais įstatymais, taisyklėmis ir kitais teisės aktais.

15 straipsnis

Atsakomybė už įgyvendinimą

1. Taryba imasi visų priemonių, būtinų siekiant užtikrinti bendrą šio sprendimo taikymo nuoseklumą.

2. Generalinis sekretorius imasi visų priemonių, būtinų užtikrinti, kad TGS pareigūnai ir kiti tarnautojai, į TGS komandiruoti darbuotojai ir TGS samdyti rangovai, tvarkydami arba saugodami ESĮI arba kitą įslaptintą informaciją Tarybos naudojamose patalpose ir TGS, laikytųsi šio sprendimo.

3. Vadovaudamosi savo atitinkamais nacionaliniais įstatymais ir kitais teisės aktais, valstybės narės imasi visų atitinkamų priemonių siekdamos užtikrinti, kad tvarkydami ar saugodami ESĮI šio sprendimo laikytųsi:

a) valstybių narių nuolatinių atstovybių Europos Sąjungoje darbuotojai ir Tarybos arba jos parengiamųjų organų posėdžiuose ar kitoje Tarybos veikloje dalyvaujantys nacionalinių delegacijų nariai;
b) kiti valstybių narių nacionalinių administracinių įstaigų darbuotojai dirbantys tiek valstybėse narėse, tiek užsienyje, įskaitant į tas administracines įstaigas komandiruotus darbuotojus;
c) kiti asmenys, kuriems valstybėse narėse dėl jų funkcijų yra suteiktas tinkamas leidimas susipažinti su ESĮI;
d) valstybių narių rangovai, dirbantys tiek valstybėse narėse, tiek užsienyje.

16 straipsnis

Saugumo organizavimas Taryboje

1. Atlikdama savo vaidmenį užtikrinti bendrą šio sprendimo taikymo nuoseklumą, Taryba tvirtina:

a) 13 straipsnio 2 dalies a punkte nurodytus susitarimus;
b) sprendimus, kuriais įgaliojama arba sutinkama Tarybos parengtą arba turimą ESĮI suteikti trečiosioms valstybėms ir tarptautinėms organizacijoms, laikantis informacijos rengėjo sutikimo principo;
c) metinę įvertinimo vizitų programą, kurią rekomenduoja Saugumo komitetas ir kuri yra skirta įvertinimo vizitams į valstybių narių tarnybas bei patalpas, Europos Sąjungos įstaigas, agentūras bei subjektus, taikančius šį sprendimą ar jo principus, taip pat įvertinimo vizitams į trečiąsias valstybes bei tarptautines organizacijas siekiant įsitikinti priemonių, įgyvendintų siekiant apsaugoti ESĮI, veiksmingumu;
d) saugumo politiką, kaip numatyta 6 straipsnio 1 dalyje.

2. Generalinis sekretorius vykdo TGS saugumo tarnybos funkcijas. Vykdydamas tas funkcijas Generalinis sekretorius:

a) įgyvendina Tarybos saugumo politiką ir ją nuolat peržiūri;
b) bendradarbiauja su valstybių narių NSI visais su Tarybos veikla susijusiais saugumo klausimais dėl įslaptintos informacijos apsaugos;
c) pagal 7 straipsnio 3 dalį suteikia TGS pareigūnams, kitiems tarnautojams ir komandiruotiems nacionaliniams ekspertams įgaliojimus susipažinti su CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta informacija;
d) atitinkamais atvejais nurodo ištirti Tarybos turimos ar parengtos įslaptintos informacijos faktinio ar įtariamo neteisėto atskleidimo arba praradimo atvejus ir prašo atitinkamų saugumo institucijų padėti atlikti šiuos tyrimus;
e) reguliariai tikrina įslaptintos informacijos apsaugai užtikrinti skirtas saugumo priemones TGS patalpose;
f) reguliariai rengia vizitus siekdamas įvertinti ESĮI apsaugai užtikrinti skirtas saugumo priemones Europos Sąjungos įstaigose, agentūrose ir subjektuose, taikančiuose šį sprendimą ar jo principus;
g) kartu su atitinkama NSI ir suderinęs su ja reguliariai vertina ESĮI apsaugai užtikrinti skirtas saugumo priemones valstybių narių tarnybose ir patalpose;

h) užtikrina, kad apsaugos priemonės prireikus būtų derinamos su valstybių narių kompetentingomis institucijomis, kurios yra atsakingos už įslaptintos informacijos apsaugą, ir atitinkamai su trečiosiomis valstybėmis ar tarptautinėmis organizacijomis, įskaitant dėl grėsmių ESĮI saugumui pobūdžio ir apsaugos nuo jų priemonių;

i) sudaro administracinius susitarimus, nurodytus 13 straipsnio 2 dalies b punkte.

TGS saugumo tarnyba padeda Generaliniam sekretoriui vykdyti šias užduotis.

3. Įgyvendindamos 15 straipsnio 3 dalį valstybės narės turėtų:

a) paskirti už ESĮI apsaugai užtikrinti skirtas saugumo priemones atsakingą NSI, nurodytą C priedėlyje pateiktame sąraše, tam, kad:

i) viešosiose ar privačiose nacionalinėse institucijose, įstaigose ar agentūrose, esančiose valstybės teritorijoje arba užsienyje, laikoma ESĮI būtų apsaugota pagal šį sprendimą;

ii) būtų užtikrintas ESĮI apsaugai skirtų saugumo priemonių reguliarus tikrinimas arba vertinimas;

iii) dėl jų atliekamų funkcijų visų nacionalinėse administracinėse įstaigose dirbančių asmenų ir rangovo pasamdytų asmenų, kuriems gali būti leista susipažinti su CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta informacija, patikimumas būtų tinkamai patikrintas arba jie turėtų kitus tinkamus leidimus pagal nacionalinius įstatymus ir kitus teisės aktus;

iv) siekiant iki minimumo sumažinti ESĮI neteisėto atskleidimo ar praradimo pavojų būtų įdiegtos būtinos saugumo programos;

v) su ESĮI apsauga susiję saugumo klausimai būtų derinami su kitomis kompetentingomis nacionalinėmis institucijomis, įskaitant su nurodytosiomis šiame sprendime;

vi) būtų atsakyta, visų pirma, į atitinkamus Europos Sąjungos įstaigų, agentūrų ir subjektų, pagal ES sutarties 2 skyriaus V antraštinę dalį nustatytų operacijų ir ES specialiųjų įgaliotinių (ESSĮ) bei jų darbuotojų grupių narių, taikančių šį sprendimą ar jo principus, prašymus išduoti asmens patikimumo pažymėjimus;

b) užtikrinti, kad jų kompetentingos institucijos vyriausybėms, o per jas Tarybai teiktų informaciją apie ESĮI saugumui kylančių grėsmių pobūdį ir apsaugos nuo jų priemones bei patartų šiais klausimais.

17 straipsnis

Saugumo komitetas

1. Įsteigiamas Saugumo komitetas. Jis nagrinėja ir vertina saugumo klausimus, kuriems taikomas šis sprendimas, ir atitinkamai teikia rekomendacijas Tarybai.

2. Saugumo komitetą sudaro valstybių narių NSI atstovai, o jo posėdžiuose dalyvauja Komisijos ir EIVT atstovas. Jam pirmininkauja Generalinis sekretorius arba jo paskirtas atstovas. Jo posėdžiai rengiami pagal Tarybos nurodymus arba Generalinio sekretoriaus ar NSI prašymu.

Europos Sąjungos įstaigų, agentūrų ir subjektų, taikančių šį sprendimą ar jo principus, atstovai gali būti kviečiami dalyvauti posėdžiuose svarstant jiems svarbius klausimus.

3. Saugumo komitetas savo veiklą organizuoja taip, kad galėtų teikti rekomendacijas konkrečių saugumo sričių klausimais. Jis įsteigia ekspertų pogrupį ISU klausimais ir prireikus kitus ekspertų pogrupius. Šis komitetas parengia tokių ekspertų pogrupių įgaliojimus, o šie pogrupiai teikia jam savo veiklos ataskaitas, įskaitant prireikus bet kurias rekomendacijas Tarybai.

18 straipsnis

Ankstesnio sprendimo pakeitimas

1. Šis sprendimas panaikina ir pakeičia Tarybos sprendimą 2011/292/ES ([2]).

2. Visa ESĮI, įslaptinta pagal Tarybos sprendimą 2001/264/EB ([3]) ir Sprendimą 2011/292/ES, toliau saugoma pagal atitinkamas šio sprendimo nuostatas.

19 straipsnis

Įsigaliojimas

Šis sprendimas įsigalioja jo paskelbimo *Europos Sąjungos oficialiajame leidinyje* dieną.

Priimta Briuselyje 2013 m. rugsėjo 23 d.

Tarybos vardu

Pirmininkas

V. JUKNA

([1]) OL L 325, 2009 12 11, p. 35.

([2]) 2011 m. kovo 31 d. Tarybos sprendimas 2011/292/ES dėl ES įslaptintos informacijos apsaugai užtikrinti skirtų saugumo taisyklių (OL L 141, 2011 5 27, p. 17).

([3]) 2001 m. kovo 19 d. Tarybos sprendimas 2001/264/EB dėl Tarybos saugumo nuostatų patvirtinimo (OL L 101, 2001 4 11, p. 1).

PRIEDAI

I PRIEDAS

Personalo patikimumas

II PRIEDAS

Fizinis saugumas

III PRIEDAS

Įslaptintos informacijos administravimas

IV PRIEDAS

RIS tvarkomos ESĮI apsauga

V PRIEDAS

Pramoninis saugumas

VI PRIEDAS

Keitimasis įslaptinta informacija su trečiosiomis valstybėmis ir tarptautinėmis organizacijomis

I PRIEDAS

PERSONALO PATIKIMUMAS

I. ĮVADAS

1. Šiame priede nustatytos 7 straipsnio įgyvendinimo nuostatos. Jame nustatomi kriterijai, kuriais remiantis nustatoma, ar asmeniui, atsižvelgiant į jo lojalumą ir patikimumą, gali būti leidžiama susipažinti su ESĮI, ir šiuo tikslu taikytinos tikrinimo bei administracinės procedūros.

II. LEIDIMO SUSIPAŽINTI SU ESĮI SUTEIKIMAS

2. Leidimas susipažinti su įslaptinta informacija asmeniui suteikiamas tik po to, kai:

   a) nustatoma, kad jis atitinka principą „būtina žinoti“;

   b) jis buvo informuotas apie ESĮI apsaugai užtikrinti skirtas saugumo taisykles bei procedūras ir patvirtino savo pareigą saugoti tokią informaciją;

   c) informacijos, pažymėtos CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma, atveju:

   – dėl jo atliekamų funkcijų jam suteiktas APP, pagal kurį jis gali susipažinti su iki atitinkamo laipsnio slaptumo žyma pažymėta informacija, arba jam buvo išduoti kiti tinkami leidimai pagal nacionalinius įstatymus ir kitus teisės aktus;

   – arba TGS pareigūnų, kitų tarnautojų ar komandiruotų nacionalinių ekspertų atveju – TGS paskyrimų tarnyba pagal 16–25 punktus suteikė jam leidimą iki nustatytos datos susipažinti su iki tam tikro laipsnio slaptumo žyma pažymėta ESĮI.
3. Kiekviena valstybė narė ir TGS savo struktūrose nustato tas pareigybes, kurias užimantiems asmenims reikia susipažinti su CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta informacija ir todėl jų patikimumas turi būti patvirtintas, suteikiant teisę susipažinti su atitinkamo laipsnio slaptumo žyma pažymėta informacija.

III. ASMENS PATIKIMUMO PAŽYMĖJIMUI TAIKOMI REIKALAVIMAI

4. NSI ir kitos kompetentingos nacionalinės institucijos, gavusios pagal tinkamus įgaliojimus pateiktą prašymą, privalo užtikrinti, kad būtų vykdomas jų piliečių, kuriems turi būti sudaryta galimybė susipažinti su CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesne slaptumo žyma pažymėta informacija, patikimumo tikrinimas. Tikrinimo standartai, siekiant atitinkamai išduoti asmens patikimumo pažymėjimą arba įsitikinti, kad asmeniui galima leisti susipažinti su ESĮI, turi atitikti nacionalinius įstatymus ir kitus teisės aktus.
5. Jeigu atitinkamas asmuo nuolat gyvena kitos valstybės narės ar trečiosios valstybės teritorijoje, kompetentingos nacionalinės institucijos prašo gyvenamosios vietos valstybės kompetentingos institucijos pagalbos laikydamosi nacionalinių įstatymų ir kitų teisės aktų. Valstybės narės padeda viena kitai vykdyti patikimumo tikrinimą pagal nacionalinius įstatymus ir kitus teisės aktus.
6. Jei leidžiama pagal nacionalinius įstatymus ir kitus teisės aktus, NSI arba kitos kompetentingos nacionalinės institucijos gali vykdyti ne jų valstybės piliečių, kuriems reikia susipažinti su CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesne slaptumo žyma pažymėta informacija, patikimumo tikrinimą. Tikrinimo standartai turi atitikti nacionalinius įstatymus ir kitus teisės aktus.

Patikimumo tikrinimo kriterijai

7. Asmens lojalumas ir patikimumas, kad jo patikimumas galėtų būti patvirtintas suteikiant teisę susipažinti su CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesne slaptumo žyma pažymėta informacija, nustatomas vykdant patikimumo tikrinimą. Kompetentinga nacionalinė institucija atlieka bendrą vertinimą, remdamasi tokio patikimumo tikrinimo išvadomis. Šiuo tikslu taikomi pagrindiniai kriterijai apima, atsižvelgiant į nacionalinius įstatymus ir kitus teisės aktus, nagrinėjimą, ar asmuo:

   a) įvykdė ar bandė, susitarė su kitais asmenimis arba padėjo kitiems asmenims įvykdyti šnipinėjimo, terorizmo, sabotažo, išdavystės ar kurstymo aktą;

   b) yra ar buvo šnipų, teroristų, sabotuotojų ar asmenų, pagrįstai tuo

įtariamų, bendrininkas arba yra ar buvo organizacijų ar užsienio valstybių, įskaitant užsienio valstybių žvalgybos tarnybas, kurios gali kelti grėsmę Europos Sąjungos ir (arba) valstybių narių saugumui, atstovų bendrininkas, išskyrus atvejus, kai tokiam bendrininkavimui buvo suteiktas leidimas jam vykdant oficialias pareigas;

c) yra ar buvo bet kurios organizacijos, kuri smurtinėmis, ardomosiomis ar kitomis neteisėtomis priemonėmis siekia, *inter alia*, nuversti valstybės narės Vyriausybę, pakeisti valstybės narės konstitucinę tvarką arba pakeisti jos valdymo formą ar politiką, narys;

d) yra ar buvo c punkte apibūdintos bet kurios organizacijos rėmėjas arba yra ar buvo glaudžiai susijęs su tokių organizacijų nariais;

e) tyčia nuslėpė, iškreipė ar suklastojo svarbią, ypač susijusią su saugumo aspektais, informaciją arba tyčia melavo pildydamas asmens patikimumo tikrinimo klausimyną ar dalyvaudamas patikimumo tikrinimo pokalbyje;

f) buvo nuteistas už nusikalstamą veiką ar nusikalstamas veikas;

g) piktnaudžiauja alkoholiu, vartoja nelegalius narkotikus ir (arba) piktnaudžiauja legaliomis narkotinėmis medžiagomis;

h) atlieka ar atliko veiksmus, dėl kurių jį galima šantažuoti ar daryti jam spaudimą;

i) savo elgesiu ar žodžiais pasirodė esąs nesąžiningas, nelojalus ar nepatikimas;

j) rimtai ar pakartotinai pažeidė saugumo nuostatus arba bandė atlikti ar sėkmingai atliko neteisėtus veiksmus, susijusius su ryšių ir informacinėmis sistemomis;

k) gali patirti spaudimą (pvz., dėl vienos ar kelių ne ES pilietybių turėjimo arba dėl giminaičių ar artimų asmenų, kurie galėtų būti pažeidžiami dėl užsienio žvalgybos tarnybų, teroristų grupių ar kitų ardomojo pobūdžio organizacijų ar asmenų, kurių siekiai gali kelti grėsmę Europos Sąjungos ir (arba) valstybių narių saugumo interesams, poveikio).

8. Vykdant patikimumo tikrinimą, atitinkamais atvejais vadovaujantis nacionaliniais įstatymais ir kitais teisės aktais, taip pat gali būti svarbi informacija apie asmens finansinę padėtį ir sveikatą.

9. Vykdant patikimumo tikrinimą, atitinkamais atvejais vadovaujantis nacionaliniais įstatymais ir kitais teisės aktais, taip pat gali būti svarbūs sutuoktinio, sugyventinio ar artimo šeimos nario elgesys ir gyvenimo aplinkybės.

Susipažinimui su ESĮI taikomi tikrinimo reikalavimai

Patikimumo pažymėjimo išdavimas pirmą kartą

10. Pradinis patikimumo pažymėjimas, leidžiantis susipažinti su slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėta informacija, grindžiamas patikimumo patikrinimu, apimančiu bent 5 paskutinių metų laikotarpį arba laikotarpį nuo 18 metų amžiaus iki patikrinimo datos, pasirenkant trumpesnį laikotarpį. Patikrinimas apima šiuos aspektus:

    a) užpildomas nacionalinis asmens patikimumo tikrinimo klausimynas, atsižvelgiant į ESĮI, su kuria asmeniui gali reikėti susipažinti, slaptumo žymos laipsnį, kuris perduodamas kompetentingai saugumo institucijai;

    b) patikrinta asmens tapatybė / pilietybė / nacionalinė priklausomybė – tikrinama asmens gimimo data bei vieta ir jo tapatybė. Nustatoma buvusi ir dabartinė asmens pilietybė / nacionalinė priklausomybė, taip pat įvertinamas bet kuris asmens pažeidžiamumas, susijęs su galimu užsienio subjektų spaudimu, pavyzdžiui, dėl ankstesnės gyvenamosios vietos ar buvusių ryšių atsirandantis pažeidžiamumas;

    c) patikrinami nacionaliniai ir vietiniai duomenys – tikrinamas nacionalinio saugumo registras ir centrinis nuosprendžių registras, jei tokie egzistuoja, ir (arba) kiti palyginami Vyriausybės ir policijos registrai. Tikrinami teisėsaugos įstaigų, kurių teisinei jurisdikcijai priklausė asmens gyvenamoji arba darbo vieta, registrai.

11. Pradinis patikimumo pažymėjimas, leidžiantis susipažinti su slaptumo žyma TRES SECRET UE/ES TOP SECRET pažymėta informacija, grindžiamas patikimumo patikrinimu, apimančiu bent dešimt paskutinių metų laikotarpį arba laikotarpį nuo 18 metų amžiaus iki patikrinimo datos, pasirenkant trumpesnį laikotarpį. Jei organizuojami pokalbiai, kaip toliau nurodyta e punkte, patikrinimas apima bent septynerių paskutinių metų laikotarpį arba laikotarpį nuo 18 metų

amžiaus iki patikrinimo datos, pasirenkant trumpesnį laikotarpį. Patikimumo pažymėjimų, leidžiančių susipažinti su slaptumo žyma TRES SECRET UE/ES TOP SECRET pažymėta informacija, išdavimui, atsižvelgiant į nacionalinius įstatymus ir kitus teisės aktus, taikomi ne tik 7 punkte nurodyti kriterijai, bet ir tikrinami toliau išvardyti aspektai; jie taip pat gali būti tikrinami prieš išduodant asmens patikimumo pažymėjimus, leidžiančius susipažinti su slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėta informacija, jei tai privaloma pagal nacionalinius įstatymus ir kitus teisės aktus:

a) finansinė padėtis – renkama informacija apie asmens finansinę padėtį, kad būtų galima įvertinti dėl rimtų finansinių sunkumų galintį atsirasti pažeidžiamumą užsienio ar šalies vidaus subjektų spaudimo atveju arba kad būtų nustatytas nepaaiškinamas turto padidėjimas;

b) išsilavinimas – renkama informacija siekiant sužinoti apie asmens įgytą išsilavinimą mokyklose, universitetuose ir kitose švietimo įstaigose nuo jo aštuonioliktojo gimtadienio ar per kitą, patikimumo tikrinimą atliekančios institucijos manymu, tinkamą laikotarpį;

c) darbovietės – renkama informacija apie dabartinę ir ankstesnes darbovietes, remiantis tokiais šaltiniais kaip darbo charakteristika, veiklos ar efektyvumo ataskaitos, taip pat darbdavių ar viršininkų informacija;

d) karo tarnyba – jei taikoma, tikrinama, ar asmuo tarnavo ginkluotosiose pajėgose ir kokiu būdu buvo išleistas į atsargą;

e) pokalbiai – kai tai numatyta ir leidžiama pagal nacionalinę teisę, organizuojamas (-i) pokalbis (-iai) su asmeniu. Į pokalbį taip pat kviečiami kiti asmenys, kurie gali nešališkai įvertinti asmens biografijos faktus, veiklą, lojalumą ir patikimumą. Kai pagal nacionalinę praktiką tikrinamo asmens prašoma pateikti rekomendacijas, turi būti apklausiami rekomendacijas pateikę asmenys, išskyrus atvejus, kai yra pagrįstų priežasčių to nedaryti.

12. Prireikus vadovaujantis nacionaliniais įstatymais ir kitais teisės aktais gali būti atliekami papildomi patikrinimai, kad būtų surinkta visa svarbi informacija apie asmenį ir kad būtų pagrįsta arba paneigta nepalanki informacija.

Patikimumo pažymėjimo atnaujinimas

13. Po to, kai patikimumo pažymėjimas suteiktas pirmą kartą, ir jeigu asmuo nuolat dirbo nacionalinėje administracinėje įstaigoje ar TGS bei jam nuolat reikia dirbti su ESĮI, patikimumo pažymėjimas peržiūrimas siekiant jį atnaujinti ne rečiau kaip kas penkerius metus pažymėjimų, leidžiančių susipažinti su slaptumo žyma TRES SECRET UE/ES TOP SECRET pažymėta informacija, atveju ir ne rečiau kaip kas dešimt metų pažymėjimų, leidžiančių susipažinti su slaptumo žymomis SECRET UE/ES SECRET ir CONFIDENTIEL UE/ES CONFIDENTIAL pažymėta informacija, atveju, skaičiuojant nuo paskutinio patikimumo patikrinimo, kuriuo remiantis buvo išduotas pažymėjimas, rezultatų pranešimo datos. Visuose dėl patikimumo pažymėjimo atnaujinimo atliekamuose patikimumo patikrinimuose tikrinamas laikotarpis nuo ankstesnio tikrinimo datos.
14. Siekiant atnaujinti patikimumo pažymėjimą, tikrinami 10 ir 11 punktuose apibūdinti aspektai.
15. Prašymai dėl atnaujinimo teikiami laiku, atsižvelgiant į tokiam patikimumo tikrinimui atlikti reikiamą laiką. Tačiau atitinkamai NSI ar kitai kompetentingai nacionalinei institucijai gavus atitinkamą prašymą dėl atnaujinimo ir atitinkamą asmens patikimumo tikrinimo klausimyną nepasibaigus patikimumo pažymėjimo galiojimo laikotarpiui ir dar neužbaigus būtino patikimumo patikrinimo, kompetentinga nacionalinė institucija gali pratęsti turimo patikimumo pažymėjimo galiojimo laikotarpį ne ilgiau kaip 12 mėnesių, jeigu leidžia nacionaliniai įstatymai ir kiti teisės aktai. Jeigu pasibaigus šiam 12 mėnesių laikotarpiui patikimumo patikrinimas dar nebaigtas, asmeniui skiriamos tokios užduotys, kurioms atlikti nereikia turėti patikimumo pažymėjimo.

TGS taikomos leidimo suteikimo procedūros

16. TGS pareigūnų ir kitų tarnautojų atveju TGS saugumo tarnyba nusiunčia užpildytą asmens patikimumo tikrinimo klausimyną valstybės narės, kurios pilietis asmuo yra, NSI, prašydama atlikti patikimumo patikrinimą, skirtą gauti leidimą naudotis tam tikro slaptumo žymos laipsnio ESĮI, su kuria asmeniui reikės susipažinti.

17. Jei TGS sužino patikimumo patikrinimui svarbios informacijos apie asmenį, kuris pateikė prašymą dėl patikimumo pažymėjimo, leidžiančio susipažinti su ESĮI, TGS, laikydamasis atitinkamų taisyklių ir teisės aktų, apie tai praneša atitinkamai NSI.
18. Užbaigusi patikimumo patikrinimą atitinkama NSI praneša TGS saugumo tarnybai tokio patikrinimo rezultatus, naudodama Saugumo komiteto nustatytą korespondencijai skirtą standartinę formą.
    a) Jei patikimumo tikrinimo rezultatai iš tikrųjų rodo, kad neturima jokios nepalankios informacijos, kuri leistų abejoti asmens lojalumu ir patikimumu, TGS paskyrimų tarnyba gali asmeniui išduoti leidimą susipažinti su iki tam tikro laipsnio slaptumo žyma pažymėta ESĮI iki nustatytos datos;
    b) Jei patikimumo tikrinimo rezultatai nėra tokie patikimi, TGS paskyrimų tarnyba apie tai praneša atitinkamam asmeniui, kuris gali prašyti, kad Paskyrimų tarnyba jį išklausytų. Paskyrimų tarnyba gali prašyti kompetentingos NSI pateikti daugiau paaiškinimų, kuriuos ji gali pateikti pagal savo nacionalinius įstatymus ir kitus teisės aktus. Jei rezultatai pasitvirtina, leidimas susipažinti su ESĮI neišduodamas.
19. Patikimumo tikrinimui bei gautiems rezultatams taikomi atitinkamoje valstybėje narėje galiojantys įstatymai ir kiti teisės aktai, įskaitant su apskundimu susijusius įstatymus ir kitus teisės aktus. TGS paskyrimų tarnybos sprendimai gali būtų apskųsti pagal Europos Sąjungos pareigūnų tarnybos nuostatus ir kitų Europos Sąjungos tarnautojų įdarbinimo sąlygas, nustatytus Tarybos reglamente (EEB, Euratomas, EAPB) Nr. 259/68 ([1]) (toliau – Tarnybos nuostatai ir įdarbinimo sąlygos).
20. Į TGS komandiruoti nacionaliniai ekspertai, siekiantys eiti pareigas, kurioms reikia galimybės susipažinti su CONFIDENTIEL UE/ES CONFIDENTIAL ar aukštesne slaptumo žyma pažymėta ES informacija, prieš pradėdami tarnybą TGS saugumo tarnybai pateikia galiojančią asmens patikimumo pažymėjimą patvirtinančią pažymą (APPP), suteikiančią teisę susipažinti su ESĮI, o paskyrimų tarnyba tuo remdamasi suteikia leidimą susipažinti su ESĮI.
21. TGS pripažįsta kitos Europos Sąjungos institucijos, įstaigos ar agentūros suteiktą leidimą susipažinti su ESĮI su sąlyga, kad jis tebegalioja. Leidimas galioja visoms užduotims, kurias tas asmuo vykdo TGS. Europos Sąjungos institucija, įstaiga ar agentūra, kurioje asmuo pradeda dirbti, praneša atitinkamai NSI apie darbdavio pasikeitimą.

22. Jeigu asmens tarnyba neprasideda per 12 mėnesių nuo patikimumo patikrinimo rezultatų pranešimo TGS paskyrimų tarnybai arba jeigu asmens tarnyboje daroma 12 mėnesių pertrauka ir tuo laikotarpiu jis nėra priimtas į pareigybę TGS ar valstybės narės nacionalinėje administracinėje įstaigoje, atitinkamos NSI prašoma patvirtinti, kad rezultatai tebegalioja bei yra tinkami.
23. Jei TGS sužino informacijos apie tai, kad asmuo, turintis leidimą susipažinti su ESĮI, kelia pavojų saugumui, TGS, laikydamasis atitinkamų taisyklių ir teisės aktų, apie tai praneša atitinkamai NSI ir gali asmeniui laikinai nesuteikti galimybės susipažinti su ESĮI arba panaikinti leidimą susipažinti su ESĮI.
24. Kai NSI informuoja TGS apie tai, kad pagal 18 punkto a papunktį suteiktas užtikrinimas dėl asmens, turinčio leidimą susipažinti su ESĮI, panaikinamas, TGS paskyrimų tarnyba gali paprašyti pateikti paaiškinimą, kurį NSI gali pateikti pagal nacionalinius įstatymus ir kitus teisės aktus. Jei nepalanki informacija patvirtinama, leidimas panaikinamas, o asmeniui neleidžiama susipažinti su ESĮI ir eiti pareigų, kurias einant jis galėtų susipažinti su ta informacija arba sukelti pavojų saugumui.
25. Apie sprendimą panaikinti arba sustabdyti TGS pareigūno ar kito tarnautojo leidimą susipažinti su ESĮI ir, atitinkamais atvejais, tokio panaikinimo arba sustabdymo priežastis pranešama atitinkamam pareigūnui, o jis gali prašyti, kad TGS paskyrimų tarnyba jį išklausytų. NSI teikiamą informaciją reglamentuoja atitinkamoje valstybėje narėje galiojantys įstatymai ir kiti teisės aktai, įskaitant su apeliacijomis susijusius įstatymus ir kitus teisės aktus. TGS paskyrimų tarnybos sprendimai gali būtų apskųsti pagal Tarnybos nuostatus ir įdarbinimo sąlygas.

Patikimumo pažymėjimų ir leidimų registravimas

26. APP ir leidimų, leidžiančių susipažinti su CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesne slaptumo žyma pažymėta informacija, registrus tvarko atitinkamai kiekviena valstybė narė ir TGS. Šiuose registruose bent jau nurodoma ESĮI, su kuria tam asmeniui gali būti leista susipažinti, slaptumo žyma, patikimumo pažymėjimo išdavimo data ir jo galiojimo laikas.

27. Kompetentinga saugumo institucija gali išduoti APPP, kurioje nurodomas ESĮI, su kuria tam asmeniui gali būti leista susipažinti, slaptumo žyma (CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnė slaptumo žyma), atitinkamo APP, leidžiančio susipažinti su ESĮI, ar leidimo susipažinti su ESĮI galiojimo laikas ir pačios pažymos galiojimo laikas.

Reikalavimo turėti APP taikymo išimtys

28. Teisė susipažinti su ESĮI asmenims, kuriems dėl jų atliekamų funkcijų suteiktas tinkamas leidimas, valstybėse narėse nustatoma pagal nacionalinius įstatymus ir kitus teisės aktus. Tokie asmenys informuojami apie jų saugumo įsipareigojimus ESĮI apsaugos srityje.

IV. ŠVIETIMAS SAUGUMO KLAUSIMAIS IR SAUGUMO SUPRATIMAS

29. Visi asmenys, kuriems išduotas patikimumo pažymėjimas, raštu patvirtina, kad jie supranta savo įsipareigojimus saugoti ESĮI ir padarinius, jei ESĮI būtų neteisėtai atskleista. Atitinkamai valstybė narė ir TGS registruoja tokius rašytinius patvirtinimus.
30. Visi asmenys, kuriems leidžiama susipažinti su ESĮI arba kurie turi dirbti su ESĮI, yra iš pat pradžių informuojami ir paskui reguliariai informuojami apie grėsmes saugumui ir jie turi nedelsdami pranešti atitinkamoms saugumo tarnyboms apie bet kokius bandymus užmegzti kontaktą ar veiklą, kurie, jų nuomone, yra įtartini ar neįprasti.
31. Visi asmenys, kurie nebeina pareigų, kurias einant jiems reikia susipažinti su ESĮI, yra informuojami apie jų įsipareigojimus toliau saugoti ESĮI slaptumą ir atitinkamais atvejais jie tai patvirtina raštu.

V. IŠSKIRTINĖS APLINKYBĖS

32. Kai leidžia nacionaliniai įstatymai ir kiti teisės aktai, valstybės narės kompetentingos nacionalinės institucijos išduotas patikimumo pažymėjimas, kuriuo leidžiama susipažinti su nacionaliniu lygiu įslaptinta informacija, gali laikinai, kol bus išduotas APP susipažinti su ESĮI, suteikti teisę nacionaliniams pareigūnams susipažinti su ne aukštesne nei lygiaverčio slaptumo žymos laipsnio ESĮI, kaip nustatyta B priedėlyje pateiktoje atitikmenų lentelėje, kai Europos Sąjungos interesais būtina suteikti tokią laikiną teisę susipažinti su informacija. NSI informuoja Saugumo komitetą, kai pagal nacionalinius įstatymus ir kitus teisės aktus tokia laikina teisė susipažinti su ESĮI negali būti suteikta.
33. Dėl skubos priežasčių, kurios pagrįstos tarnybos interesais, laukiant išsamaus patikimumo patikrinimo pabaigos, TGS paskyrimų tarnyba, pasikonsultavusi su valstybės narės, kurios pilietis yra atitinkamas asmuo, NSI ir atsižvelgusi į preliminaraus patikrinimo, skirto patikrinti, ar nėra žinomos nepalankios informacijos apie asmenį, rezultatus, gali TGS pareigūnams ir kitiems tarnautojams išduoti laikiną leidimą susipažinti su ESĮI konkrečiai funkcijai atlikti. Tokie laikini leidimai galioja ne ilgiau kaip šešis mėnesius ir nesuteikia teisės susipažinti su slaptumo žyma TRES SECRET UE/ES TOP SECRET pažymėta informacija. Visi asmenys, kuriems išduotas laikinas leidimas, raštu patvirtina, kad jie supranta savo įsipareigojimus saugoti ESĮI ir ESĮI neteisėto atskleidimo pasekmes. TGS registruoja tokius rašytinius patvirtinimus.
34. Kai asmuo turi būti paskirtas į pareigybę, kuriai užimti reikalingas vienu laipsniu aukštesnis nei turimas patikimumo pažymėjimas, jis gali būti paskirtas į tą pareigybę laikinai, jeigu:

    a) asmens vadovas raštu įtikinamai pagrindžia, kad būtina susipažinti su aukštesnio laipsnio ESĮI;

    b) suteikiama teisė susipažinti tik su konkrečia ESĮI, kurios reikia užduočiai atlikti;

    c) asmuo turi galiojantį APP arba leidimą susipažinti su ESĮI;

    d) imtasi veiksmų pareigybei reikiamo laipsnio leidimui gauti;

    e) kompetentinga institucija atliko pakankamus patikrinimus, kad asmuo nėra rimtai ar pakartotinai pažeidęs saugumo nuostatų;

    f) asmens paskyrimą patvirtino kompetentinga institucija;

    g) išimtys, įskaitant informacijos, su kuria leista susipažinti, aprašymą, registruojamos atsakingame registre ar subregistre.

35. Pirmiau nurodytos procedūros laikomasi, kai reikia suteikti leidimą vieną kartą susipažinti su vienu laipsniu aukštesne slaptumo žyma pažymėta ESĮI nei ta, su kuria susipažinti jiems buvo leista atlikus patikimumo patikrinimą. Tokia procedūra neturi būti naudojama pakartotinai.
36. Itin išskirtinėmis aplinkybėmis, tokiomis kaip vykdant užduotis priešiškoje aplinkoje arba kylant tarptautinei įtampai, kai to reikia imantis neatidėliotinų priemonių, visų pirma, siekiant išsaugoti žmonių gyvybes, valstybės narės ir Generalinis sekretorius arba Generalinio sekretoriaus pavaduotojas gali, kai įmanoma – raštu, suteikti galimybę susipažinti su slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėta informacija asmenims, neturintiems reikiamo patikimumo pažymėjimo, jeigu tokio leidimo tikrai reikia ir jeigu nėra pagrįstų abejonių dėl atitinkamo asmens lojalumo ir patikimumo. Toks leidimas registruojamas, kartu aprašant informaciją, su kuria leista susipažinti.
37. Slaptumo žyma TRES SECRET UE/ES TOP SECRET pažymėtos informacijos atveju toks leidimo suteikimas skubos tvarka taikomas tik tiems Europos Sąjungos piliečiams, kuriems buvo leista susipažinti su nacionaline informacija, atitinkančia TRES SECRET UE/ES TOP SECRET slaptumo laipsnį, arba su slaptumo žyma SECRET UE/ES SECRET pažymėta informacija.
38. Saugumo komitetas informuojamas apie atvejus, kai naudojamasi 36 ir 37 punktuose išdėstyta procedūra.
39. Kai valstybės narės nacionaliniai įstatymai ir kiti teisės aktai nustato griežtesnes taisykles dėl laikinų leidimų, laikinų paskyrimų, asmenims susipažinti su įslaptinta informacija vieną kartą ar skubos tvarka leidžiama ir šiame skirsnyje numatytos procedūros taikomos tik nepažeidžiant atitinkamų įstatymų ir kitų teisės aktų nustatytų apribojimų.
40. Saugumo komitetui pateikiama šiame skirsnyje numatytų procedūrų taikymo metinė ataskaita.

VI. DALYVAVIMAS TARYBOJE VYKSTANČIUOSE POSĖDŽIUOSE

41. Vadovaujantis 28 punktu, asmenys, paskirti dalyvauti Tarybos arba Tarybos parengiamųjų organų posėdžiuose, kuriuose aptariama CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesne slaptumo žyma pažymėta informacija, gali tai daryti tik patvirtinus, kad jie turi patikimumo pažymėjimą. Deleguotų asmenų APPP ar kitus patikimumo pažymėjimo įrodymus atitinkamos institucijos siunčia TGS saugumo tarnybai arba išimtiniais atvejais ją pateikia atitinkamas deleguotas asmuo. Jei taikoma, gali būti naudojamas suvestinis pavardžių sąrašas, kuriame pateikiami atitinkami įrodymai apie patikimumo pažymėjimą.
42. Kai asmens, kuris eidamas savo pareigas turi dalyvauti Tarybos ir Tarybos parengiamųjų organų posėdžiuose, APP susipažinti su ESĮI panaikinamas saugumo sumetimais, kompetentinga institucija apie tai informuoja TGS.

VII. GALIMA PRIEIGA PRIE ESĮI

43. Kurjerių, apsaugos darbuotojų ir lydinčių asmenų patikimumas turi būti patikrintas atitinkamu lygiu arba jie turi būti kitaip deramai patikrinti vadovaujantis nacionaliniais įstatymais ir kitais teisės aktais. Jie yra supažindinami su ESĮI apsaugai užtikrinti skirtomis saugumo procedūromis ir jiems išdėstomos jų pareigos jiems patikėtos tokios informacijos apsaugos srityje.

([1]) 1968 m. vasario 29 d. Tarybos reglamentas (EEB, Euratomas, EAPB) Nr. 259/68, nustatantis Europos Bendrijų pareigūnų tarnybos nuostatus ir kitų Europos Bendrijų tarnautojų įdarbinimo sąlygas bei Komisijos pareigūnams laikinai taikomas specialias priemones (OL L 56, 1968 3 4, p. 1).

II PRIEDAS

FIZINIS SAUGUMAS

I. ĮVADAS

1. Šiame priede nustatytos 8 straipsnio įgyvendinimo nuostatos. Jame išdėstyti būtiniausi reikalavimai, taikomi patalpų, pastatų, kabinetų, salių ir kitų zonų, kuriose tvarkoma ir saugoma ESĮI, įskaitant zonas, kuriose yra RIS, fizinei apsaugai.
2. Fizinio saugumo priemonės yra skirtos užkirsti kelią leidimo neturintiems asmenims susipažinti su ESĮI:

   a) užtikrinant, kad ESĮI būtų tinkamai tvarkoma ir saugoma;

   b) sudarant sąlygas suskirstyti personalą pagal tai, kas gali susipažinti su ESĮI, remiantis principu „būtina žinoti“ ir atitinkamais atvejais – personalo narių patikimumo pažymėjimais;

   c) atgrasant nuo neteisėtų veiksmų, sutrukdant jiems bei juos nustatant;

   d) sutrukdant asmenims įsibrauti slaptai arba įsiveržti jėga arba juos užlaikant.

II. FIZINIO SAUGUMO REIKALAVIMAI IR PRIEMONĖS

3. Fizinio saugumo priemonės parenkamos remiantis grėsmių įvertinimu, kurį atlieka kompetentingos institucijos. ESĮI apsaugai užtikrinti savo patalpose TGS ir valstybės narės taiko rizikos valdymo procesą, kad užtikrintų, jog, atsižvelgiant į įvertintą riziką, būtų taikoma atitinkamo lygio fizinė apsauga. Rizikos valdymo procese atsižvelgiama į visus svarbius veiksnius, visų pirma:

   a) ESĮI slaptumo žymos laipsnį;

   b) ESĮI formą ir kiekį, atsižvelgiant į tai, kad dideliam ESĮI kiekiui ar rinkiniui apsaugoti gali reikėti taikyti griežtesnes apsaugos priemones;

   c) pastatus ar zonas, kuriose laikoma ESĮI, supančią aplinką ir jų struktūrą;

   d) įvertintą žvalgybos tarnybų, kurių veikla nukreipta prieš Europos Sąjungą arba jos valstybes nares, keliamą grėsmę ir grėsmę dėl sabotažo, terorizmo, ardomosios arba kitų rūšių nusikalstamos veiklos.

4. Kompetentinga saugumo tarnyba, taikydama nuodugnios apsaugos sąvoką, nustato tinkamas įgyvendintinas fizinio saugumo priemones. Tai gali būti viena (ar daugiau) iš šių priemonių:

   a) perimetro barjeras: fizinis barjeras, kuris skirtas zonos, kurioje reikalinga apsauga, ribos apsaugai užtikrinti;

   b) įsibrovimo aptikimo sistemos (ĮAS): ĮAS gali būti naudojama siekiant padidinti perimetro barjero teikiamo saugumo lygį arba patalpose ir pastatuose vietoj apsaugos personalo ar jam padėti;

   c) patekimo kontrolė: gali būti kontroliuojamas patekimas į objektą, pastatą ar pastatus objekte arba į zonas ar patalpas pastate. Kontrolė gali būti vykdoma elektroninėmis arba elektroninėmis-mechaninėmis priemonėmis. Ją gali vykdyti apsaugos personalas ir (arba) priimamojo darbuotojas arba ji gali būti vykdoma kitomis fizinėmis priemonėmis;

   d) apsaugos personalas: siekiant atgrasyti slaptą įsibrovimą planuojančius asmenis, galima įdarbinti apmokytą ir prižiūrimą apsaugos personalą, *inter alia*, prireikus tinkamai patikrinant jų patikimumą;

   e) apsauginės vaizdo stebėjimo sistemos (AVSS): apsaugos personalas gali naudotis AVSS, kad patikrintų incidentus ir ĮAS pavojaus signalus dideliuose objektuose ar ties perimetru;

   f) apsauginis apšvietimas: apsauginis apšvietimas ne tik skleidžia šviesą, būtiną veiksmingam stebėjimui, kurį tiesiogiai atlieka apsaugos personalas arba kuris netiesiogiai atliekamas per AVSS sistemą, bet jį taip pat galima naudoti siekiant atgrasyti potencialų įsibrovėlį;

   g) kitos tinkamos fizinės priemonės, skirtos atgrasyti asmenis be leidimo naudotis ESĮI, nustatyti tokio naudojimo atvejus arba užkirsti kelią tam, kad ESĮI būtų prarasta ar jai būtų padaryta žala.
5. Kompetentinga institucija gali būti įgaliojama apieškoti įeinančius ir išeinančius asmenis siekiant atgrasyti nuo neleistino medžiagos įnešimo arba neleistino ESĮI išnešimo iš patalpų ar pastatų.
6. Iškilus pavojui, kad ESĮI bus pamatyta, netgi atsitiktinai, imamasi tinkamų priemonių siekiant išvengti šio pavojaus.
7. Naujos infrastruktūros atveju infrastruktūros planavimo ir projektavimo metu apibrėžiami fizinio saugumo reikalavimai ir jos funkcinės specifikacijos. Esamos infrastruktūros atveju kiek įmanoma įgyvendinami fizinio saugumo reikalavimai.

III. ESĮI FIZINEI APSAUGAI SKIRTA ĮRANGA

8. Įsigydama ESĮI fizinei apsaugai užtikrinti skirtą įrangą (pavyzdžiui, apsaugines talpyklas, naikiklius, durų užraktus, elektronines patekimo kontrolės sistemas, įsibrovimo aptikimo sistemas, signalizacijos sistemas), kompetentinga saugumo institucija užtikrina, kad įranga atitiktų patvirtintus techninius standartus ir būtiniausius reikalavimus.
9. ESĮI fizinei apsaugai užtikrinti naudotinos įrangos techninės specifikacijos išdėstomos saugumo gairėse, kurias turi patvirtinti Saugumo komitetas.
10. Saugumo sistemos reguliariai tikrinamos ir reguliariai atliekama įrangos priežiūra. Atliekant priežiūrą atsižvelgiama į patikrinimų rezultatus, kad būtų užtikrinta, jog įrenginiai toliau veiktų optimaliai.
11. Kiekvieno patikrinimo metu iš naujo vertinamas individualių saugumo priemonių ir visos saugumo sistemos veiksmingumas.

IV. FIZIŠKAI APSAUGOTOS ZONOS

12. ESĮI fizinės apsaugos tikslais nustatomos dviejų tipų fiziškai apsaugotos zonos arba nacionalinės lygiavertės zonos:

    a) administracinės zonos;

    b) saugumo zonos (įskaitant techniniu požiūriu saugias saugumo zonas).

    Šiame sprendime visos nuorodos į administracines zonas ir saugumo zonas, įskaitant techniniu požiūriu saugias saugumo zonas, laikomos ir nuorodomis į nacionalines lygiavertes zonas.
13. Kompetentinga saugumo institucija nustato, kad zona atitinka reikalavimus, jog būtų klasifikuojama kaip administracinė zona, saugumo zona ar techniniu požiūriu saugi saugumo zona.
14. Administracinių zonų atveju:

    a) nustatoma aiškiai apibrėžta išorinė riba, kad būtų galima tikrinti asmenis ir, jei įmanoma, transporto priemones;

    b) į šias zonas įeiti nelydimiems leidžiama tik tiems asmenims, kuriems kompetentinga institucija suteikė tinkamą leidimą;

    c) visi kiti asmenys turi būti visą laiką lydimi arba jiems turi būti taikomos lygiavertės kontrolės priemonės.

15. Saugumo zonų atveju:

a) nustatoma aiškiai apibrėžta ir saugoma išorinė riba, per kurią kiekvienas įėjimas ir išėjimas yra kontroliuojamas naudojantis leidimų arba asmens atpažinimo sistema;

b) į zoną įeiti nelydimiems leidžiama tik tiems asmenims, kurių patikimumas patikrintas ir kurie turi specialų leidimą įeiti į zoną, vadovaujantis principu „būtina žinoti“;

c) visi kiti asmenys turi būti visą laiką lydimi arba jiems turi būti taikomos lygiavertės kontrolės priemonės.

16. Tais atvejais, kai įėjus į saugumo zoną galima visais praktiniais tikslais tiesiogiai susipažinti su joje laikoma įslaptinta informacija, taikomi tokie papildomi reikalavimai:

a) turi būti aiškiai nurodyta paprastai zonoje laikomos informacijos aukščiausio slaptumo žymos laipsnio specifikacija;

b) visi lankytojai privalo turėti specialų leidimą, suteikiantį teisę įeiti į zoną, turi būti visą laiką lydimi ir jų patikimumas turi būti tinkamai patikrintas, nebent imtasi priemonių užtikrinti, kad nebūtų įmanoma susipažinti su ESĮI.

17. Saugumo zonos, kurios turi būti apsaugotos nuo pasiklausymo, klasifikuojamos kaip techniniu požiūriu saugios saugumo zonos. Taikomi šie papildomi reikalavimai:

a) tokiose zonose turi būti įdiegta ĮAS ir, kai jose nedirbama, jos turi būti rakinamos, o kai dirbama – saugomos. Visi raktai apskaitomi ir saugomi vadovaujantis VI skirsniu;

b) visi į tokias zonas įeinantys asmenys ar įnešamos medžiagos turi būti kontroliuojami;

c) tokios zonos reguliariai fiziškai ir (arba) techniškai tikrinamos, kaip reikalauja kompetentinga saugumo institucija. Tokie patikrinimai atliekami, kai į zoną buvo įeita be leidimo ar įtariama apie tokį patekimą;

d) tokiose zonose negali būti ryšių linijų, kurioms nesuteiktas leidimas, telefonų, kuriems nesuteiktas leidimas, ar kitų ryšių prietaisų bei elektros ar elektroninės įrangos, kuriems nesuteiktas leidimas.

18. Nepaisant 17 punkto d papunkčio, prieš naudojantis ryšių prietaisais ir elektros ar elektronine įranga zonose, kuriose rengiami susitikimai ar atliekamas darbas, susijęs su SECRET UE/ES SECRET arba aukštesne slaptumo žyma pažymėta informacija, taip pat, kai grėsmė ESĮI vertinama kaip didelė, tokius prietaisus ir įrangą, visų pirma, ištiria kompetentinga saugumo institucija, siekdama užtikrinti, kad naudojantis šia įranga nebūtų galima perduoti jokios suprantamos informacijos per neapdairumą ar neteisėtai už saugumo zonos perimetro.
19. Saugumo zonos, kuriose nėra visą parą budinčio personalo, atitinkamais atvejais tikrinamos pasibaigus įprastai darbo dienai ir atsitiktiniais intervalais ne tomis darbo valandomis, kurios įprastos, išskyrus atvejus, kai įdiegta ĮAS.
20. Siekiant surengti susitikimą, kuriame naudojama įslaptinta informacija, arba bet kokiu kitu panašiu tikslu administracinėje zonoje gali būti laikinai įrengtos saugumo zonos ir techniniu požiūriu saugios saugumo zonos.
21. Saugios eksploatacijos taisyklės rengiamos kiekvienai saugumo zonai ir jose nustatoma:

    a) ESĮI, kuri gali būti tvarkoma ir saugoma toje zonoje, slaptumo žymos laipsnis;

    b) įdiegtinos stebėjimo ir apsaugos priemonės;

    c) kokie asmenys turi leidimą nelydimi patekti į zoną, vadovaujantis principu „būtina žinoti“ ir asmens patikimumo pažymėjimu;

    d) atitinkamais atvejais palydos tvarka ir ESĮI apsaugos tvarka, kai kitiems asmenims leidžiama patekti į zoną;

    e) bet kurios kitos atitinkamos priemonės ir procedūros.
22. Saugumo zonose įrengiamos saugyklos. Sienos, grindys, lubos, langai ir durys su užraktais turi būti kompetentingos saugumo institucijos patvirtintos ir užtikrinti apsaugą, kurią užtikrina apsauginės talpyklos, patvirtintos to paties laipsnio slaptumo žymos ESĮI saugoti.

V. FIZINĖS APSAUGOS PRIEMONĖS TVARKANT IR SAUGANT ESĮI

23. Slaptumo žyma RESTREINT UE/ES RESTRICTED pažymėta ESĮI gali būti tvarkoma:

a) saugumo zonose;

b) administracinėse zonose, jeigu ta ESĮI yra apsaugota taip, kad su ja negalėtų susipažinti leidimo neturintys asmenys;

c) ne saugumo zonose ar administracinėse zonose, jeigu turėtojas gabena ESĮI pagal III priedo 28–41 punktus ir yra įsipareigojęs taikyti kompensacines priemones, nustatytas kompetentingos saugumo institucijos parengtose saugumo instrukcijose, kad būtų užtikrinta, jog ESĮI yra apsaugota taip, kad su ja negalėtų susipažinti leidimo neturintys asmenys.

24. Slaptumo žyma RESTREINT UE/ES RESTRICTED pažymėta ESĮI saugoma tinkamuose rakinamuose biuro balduose administracinėse zonose arba saugumo zonose. Laikinai ji gali būti saugoma ne saugumo zonose ar administracinėse zonose, jeigu turėtojas yra įsipareigojęs taikyti kompensacines priemones, nustatytas kompetentingos saugumo institucijos parengtose saugumo instrukcijose.

25. Slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėta ESĮI gali būti tvarkoma:

a) saugumo zonose;

b) administracinėse zonose, jeigu ta ESĮI yra apsaugota taip, kad su ja negalėtų susipažinti leidimo neturintys asmenys;

c) ne saugumo zonose ar administracinėse zonose, jeigu turėtojas:

i) gabena ESĮI pagal III priedo 28–41 punktus;

ii) yra įsipareigojęs taikyti kompensacines priemones, nustatytas kompetentingos saugumo institucijos parengtose saugumo instrukcijose, kad būtų užtikrinta, jog ESĮI yra apsaugota taip, kad su ja negalėtų susipažinti leidimo neturintys asmenys;

iii) visą laiką asmeniškai kontroliuoja šią ESĮI;

iv) jei dokumentai yra popieriniu pavidalu, apie tai pranešė atitinkamai registratūrai.

26. Slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėta ESĮI saugoma saugumo zonose esančiose apsauginėse talpyklose arba saugyklose.

27. Slaptumo žyma TRES SECRET UE/ES TOP SECRET pažymėta ESĮI tvarkoma saugumo zonose.
28. Slaptumo žyma TRES SECRET UE/ES TOP SECRET pažymėta ESĮI saugoma saugumo zonose laikantis kurios nors iš toliau nurodytų sąlygų:

a) apsauginėje talpykloje laikantis 8 punkto reikalavimų, taikant bent vieną iš toliau nurodytų papildomos kontrolės priemonių:

i) nuolatinė apsauga arba tikrinimas, kurį vykdo apsaugos personalas arba budintis personalas, kurio patikimumas patikrintas;

ii) patvirtinta ĮAS kartu veikiant reagavimo apsaugos personalui;

b) saugykloje su įrengta ĮAS kartu veikiant reagavimo apsaugos personalui.

29. ESĮI gabenimą už fiziškai apsaugotų zonų ribų reglamentuojančios taisyklės išdėstytos III priede.

VI. ESĮI APSAUGAI UŽTIKRINTI NAUDOJAMŲ RAKTŲ IR KODŲ KONTROLĖ

30. Kompetentinga saugumo institucija nustato kabinetų, patalpų, saugyklų ir apsauginių talpyklų raktų bei kodų valdymo procedūras. Tokios procedūros apsaugo nuo neleistino susipažinimo su informacija.
31. Kodai patikimi kuo mažesniam asmenų skaičiui ir tik tiems asmenims, kuriems reikia juos naudoti. Šie asmenys kodus įsimena. Apsauginių talpyklų ir saugyklų, kuriose saugoma ESĮI, kodai keičiami:

a) gavus naują talpyklą;

b) pasikeitus kodus žinančiam personalui;

c) iškilus pavojui ar įtarimui;

d) po spynos techninio patikrinimo ar remonto;

e) bent kas 12 mėnesių.

III PRIEDAS

ĮSLAPTINTOS INFORMACIJOS ADMINISTRAVIMAS

I. ĮVADAS

1. Šiame priede nustatytos 9 straipsnio įgyvendinimo nuostatos. Jame išdėstytos administracinės ESĮI kontrolės visą jos gyvavimo ciklą priemonės siekiant atgrasyti nuo tokios informacijos sąmoningo ar atsitiktinio neteisėto atskleidimo arba praradimo ir nustatyti tokius atvejus.

II. ĮSLAPTINIMO ADMINISTRAVIMAS

Slaptumo žymos ir kitos žymos

2. Informacija įslaptinama tuo atveju, jei dėl jos konfidencialumo reikia ją apsaugoti.
3. ESĮI rengėjas atsako už slaptumo žymos laipsnio nustatymą pagal atitinkamas įslaptinimo gaires ir už pirminį informacijos platinimą.
4. ESĮI slaptumo žymos laipsnis nustatomas vadovaujantis 2 straipsnio 2 dalimi ir remiantis saugumo politika, kuri turi būti tvirtinama pagal 3 straipsnio 3 dalį.
5. Slaptumo žyma nurodoma aiškiai ir teisingai, neatsižvelgiant į tai, ar ESĮI yra pateikiama popieriuje, žodžiu, elektronine ar bet kuria kita forma.
6. Atskiroms dokumento dalims (t. y. puslapiams, dalims, skirsniams, priedams ir priedėliams) gali būti suteikiamos skirtingos slaptumo žymos ir jos atitinkamai pažymimos, taip pat tais atvejais, kai jos saugomos elektronine forma.
7. Dokumento ar dokumentų bylos bendras slaptumo žymos laipsnis nustatomas pagal aukščiausią slaptumo žymos laipsnį turinčią jo dalį. Kai renkama informacija iš įvairių šaltinių, galutinis dokumentas peržiūrimas siekiant nustatyti jo bendrą slaptumo žymos laipsnį, nes gali paaiškėti, kad jam turi būti suteiktas aukštesnis slaptumo žymos laipsnis nei jo dalims.

8. Kiek įmanoma, dokumentams, kurių dalys pažymėtos skirtingo laipsnio slaptumo žymomis, suteikiama tokia struktūra, kad skirtingo laipsnio slaptumo žymomis pažymėtas dalis būtų galima lengvai nustatyti ir prireikus atskirti.
9. Pridedamų dokumentų lydinčiųjų dokumentų slaptumo žymos laipsnis atitinka priedų aukščiausio laipsnio slaptumo žymas. Jei tokie dokumentai pateikiami atskirai nuo priedų, įslaptintos informacijos rengėjas turi aiškiai nurodyti, koks slaptumo žymos laipsnis jiems suteikiamas, naudodamas atitinkamą žymą, pavyzdžiui,

   CONFIDENTIEL UE/ES CONFIDENTIAL

   be priedo (-ų) RESTREINT UE/ES RESTRICTED.

Žymos

10. Be vienos iš slaptumo žymų, nurodytų 2 straipsnio 2 dalyje, ESĮI gali būti pažymėta papildomomis žymomis, pavyzdžiui:

    a) identifikatoriumi, kuriuo nurodomas įslaptintos informacijos rengėjas;

    b) bet kuriais apribojimais, kodiniais žodžiais ar santrumpomis, kuriais nurodoma veiklos sritis, su kuria dokumentas yra susijęs, jo specialus platinimas vadovaujantis principu „būtina žinoti“ arba naudojimo apribojimai;

    c) paskirstymo žymomis;

    d) jei taikoma, nurodant datą ar konkretų įvykį, po kurio informacijos slaptumo žymos laipsnis gali būti sumažintas arba ji gali būti išslaptinta.

Žymų santrumpos

11. Siekiant nurodyti atskirų teksto pastraipų slaptumo žymos laipsnį, gali būti naudojamos standartinės slaptumo žymų santrumpos. Santrumpos nepakeičia pilnų slaptumo žymų.

12. ES įslaptintuose dokumentuose gali būti naudojamos šios standartinės santrumpos, kuriomis nurodomas skirsnių arba teksto dalių, užimančių mažiau nei vieną puslapį, slaptumo žymos laipsnis:
TRES SECRET UE/ES TOP SECRET – TS-UE/ES-TS;
SECRET UE/ES SECRET – S-UE/ES-S;
CONFIDENTIEL UE/ES CONFIDENTIAL – C-UE/ES-C;
RESTREINT UE/ES RESTRICTED – R-UE/ES-R.

ESĮI rengimas

13. Rengiant ES įslaptintą dokumentą:

a) kiekvienas puslapis aiškiai pažymimas slaptumo žyma;

b) kiekvienas puslapis numeruojamas;

c) dokumente nurodomas jo numeris ir dalykas, kurie nėra įslaptinta informacija, išskyrus tuo atveju, kai jie pažymėti kaip įslaptinta informacija;

d) dokumente nurodoma data;

e) jei platinamos kelios dokumentų, pažymėtų SECRET UE/ES SECRET ir aukštesnio laipsnio slaptumo žyma, kopijos, kiekvienos iš jų kiekviename puslapyje nurodomas kopijos numeris.

14. Kai rengiant ESĮI neįmanoma taikyti 13 punkte išdėstytų reikalavimų, taikomos kitos atitinkamos priemonės, vadovaujantis saugumo gairėmis, parengtomis remiantis 6 straipsnio 2 dalimi.

ESĮI slaptumo žymos laipsnio sumažinimas ir ESĮI išslaptinimas

15. Įslaptintos informacijos rengėjas, kai įmanoma, rengdamas ESĮI, ypač RESTREINT UE/ES RESTRICTED slaptumo žyma pažymėtą informaciją, nurodo, ar tam tikrą dieną arba po tam tikro įvykio galima sumažinti ESĮI slaptumo žymos laipsnį arba ją išslaptinti.
16. TGS reguliariai peržiūri jo turimą ESĮI, siekdamas įsitikinti, ar slaptumo žymos lygis vis dar taikomas. TGS sukuria sistemą, skirtą peržiūrėti ESĮI, kurią jis parengė, slaptumo žymos laipsnį ne rečiau kaip kas penkerius metus. Tokia peržiūra nėra reikalinga, jeigu įslaptintos informacijos rengėjas iš pat pradžių nurodo, kad informacijos slaptumo žymos laipsnis bus sumažintas arba informacija išslaptinta automatiškai, o informacija buvo atitinkamai pažymėta.

III. ESĮI REGISTRAVIMAS SAUGUMO TIKSLAIS

17. Kiekviename TGS ir valstybių narių nacionalinių administracinių įstaigų organizaciniame vienete, kuriame tvarkoma ESĮI, steigiamos atsakingos registratūros, siekiant užtikrinti, kad ESĮI būtų administruojama pagal šį sprendimą. Registratūros steigiamos kaip II priede apibrėžtos saugumo zonos.
18. Šiame sprendime registravimas saugumo tikslais (toliau – registravimas) – procedūrų, kuriomis užregistruojamas dokumento gyvavimo ciklas, įskaitant jo platinimą ir sunaikinimą, taikymas.
19. Kai organizacinis vienetas gauna CONFIDENTIEL UE/ES CONFIDENTIAL ir aukštesne slaptumo žyma pažymėtą medžiagą ir kai ją išsiunčia, visa ši medžiaga registruojama tam skirtose registratūrose.
20. Centrinė TGS registratūra registruoja visą įslaptintą informaciją, kurią Taryba ir TGS suteikė trečiosioms valstybėms ir tarptautinėms organizacijoms, bei visą įslaptintą informaciją, gautą iš trečiųjų valstybių ir tarptautinių organizacijų.
21. RIS atveju registravimo procedūros gali būti atliekamos vykdant procesus pačioje RIS.
22. Taryba patvirtina ESĮI registravimo saugumo tikslais saugumo politiką.

TRES SECRET UE/ES TOP SECRET registratūros

23. Valstybėse narėse ir TGS paskiriama registratūra, kuri veikia kaip centrinė slaptumo žyma TRES SECRET UE/ES TOP SECRET pažymėtą informaciją gaunanti ir siunčianti tarnyba. Prireikus gali būti paskirtos antrinės registratūros, kurios tvarko tokią informaciją jos registravimo tikslais.
24. Tokios antrinės registratūros negali perduoti slaptumo žyma TRES SECRET UE/ES TOP SECRET pažymėtų dokumentų tiesiogiai kitoms tos pačios centrinės TRES SECRET UE/ES TOP SECRET registratūros antrinėms registratūroms arba į išorę be aiškaus rašytinio tos registratūros leidimo.

IV. ES ĮSLAPTINTŲ DOKUMENTŲ KOPIJAVIMAS IR VERTIMAS

25. Slaptumo žyma TRES SECRET UE/ES TOP SECRET pažymėti dokumentai kopijuojami arba verčiami tik gavus išankstinį rašytinį įslaptintos informacijos rengėjo sutikimą.
26. Jeigu SECRET UE/ES SECRET arba žemesnio laipsnio slaptumo žyma pažymėtų dokumentų įslaptintos informacijos rengėjas nenustatė apribojimų dėl jų kopijavimo ar vertimo, dokumento turėtojo nurodymu tokius dokumentus galima kopijuoti arba versti.
27. Dokumento kopijoms ir vertimams taikomos tos pačios saugumo priemonės, kaip ir dokumento originalui.

V. ESĮI GABENIMAS

28. Gabenant ESĮI taikomos 30–41 punktuose išdėstytos apsaugos priemonės. Kai ESĮI gabenama elektroninėje laikmenoje ir nepaisant 9 straipsnio 4 dalies, toliau išvardytas apsaugos priemones gali papildyti kompetentingos saugumo institucijos nurodytos atitinkamos techninės kontrpriemonės, kad būtų sumažinta rizika, jog informacija bus prarasta ar atskleista.
29. TGS ir valstybių narių kompetentingos saugumo institucijos parengia ESĮI gabenimo instrukcijas remdamosi šiuo sprendimu.

Pastate arba uždaroje pastatų grupėje

30. Pastate arba uždaroje pastatų grupėje gabenama informacija turi būti uždengta, kad nebūtų galima stebėti jos turinio.
31. Slaptumo žyma TRES SECRET UE/ES TOP SECRET pažymėta informacija pastate arba uždaroje pastatų grupėje turi būti gabenama apsaugotame voke, ant kurio nurodytas tik gavėjo vardas ir pavardė.

Europos Sąjungoje

32. ESĮI, gabenama iš vieno pastato ar patalpos į kitą Europos Sąjungoje, turi būti supakuota taip, kad ji būtų apsaugota nuo neteisėto atskleidimo.

33. CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET slaptumo žyma pažymėtą informaciją Europos Sąjungoje gabena:

a) atitinkamai karinis, vyriausybinis ar diplomatinis kurjeris;

b) kurjeris su sąlyga, kad:

i) ESĮI nepaliekama be ją gabenančio asmens priežiūros, išskyrus tuo atveju, kai ji saugoma laikantis II priede nustatytų reikalavimų;

ii) paketas su ESĮI neatidaromas gabenimo metu arba ESĮI neskaitoma viešose vietose;

iii) asmenys informuojami apie jų pareigas, susijusias su saugumu;

iv) prireikus asmenims suteikiamas kurjerio pažymėjimas;

c) pašto tarnybos arba komercinės kurjerių pašto tarnybos su sąlyga, kad:

i) jos yra patvirtintos atitinkamos NSI vadovaujantis nacionaliniais įstatymais ir kitais teisės aktais;

ii) jos taiko atitinkamas apsaugos priemones, laikydamosi būtiniausių reikalavimų, kurie turi būti nustatyti saugumo gairėse pagal 6 straipsnio 2 dalį.

Gabenimo iš vienos valstybės narės į kitą atveju c papunkčio nuostatos taikomos tik gabenant informaciją, pažymėtą slaptumo žyma iki CONFIDENTIEL UE/ES CONFIDENTIAL.

34. Slaptumo žyma RESTREINT UE/ES RESTRICTED pažymėtą informaciją taip pat gali gabenti pašto tarnybos arba komercinės kurjerių pašto tarnybos. Tokios informacijos gabenimui kurjerio pažymėjimas nereikalingas.

35. CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET slaptumo žyma pažymėtą medžiagą (pavyzdžiui, įrangą ar įrenginius), kurios negalima gabenti 33 punkte nurodytomis priemonėmis, kaip krovinį pagal V priedą gabena komercinės vežėjų bendrovės.

36. TRES SECRET UE/ES TOP SECRET slaptumo žyma pažymėtą informaciją iš vieno pastato ar patalpos į kitą Europos Sąjungoje gabena atitinkamai karinis, vyriausybinis ar diplomatinis kurjeris.

Iš Europos Sąjungos į trečiosios valstybės teritoriją

37. ESĮI, gabenama iš Europos Sąjungos į trečiosios valstybės teritoriją, turi būti supakuota taip, kad ji būtų apsaugota nuo neteisėto atskleidimo.
38. CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET slaptumo žyma pažymėtą informaciją iš Europos Sąjungos į trečiosios valstybės teritoriją gabena:

    a) karinis ar diplomatinis kurjeris;

    b) kurjeris su sąlyga, kad:

    i) ant paketo yra oficialus spaudas arba ESĮI supakuota aiškiai nurodant, kad tai yra oficiali siunta ir jai neturėtų būti taikomas muitinės ar saugumo patikrinimas;

    ii) asmenys turi kurjerio pažymėjimą, kuriame nurodytas paketas ir kuris suteikia jiems teisę gabenti paketą;

    iii) ESĮI nepaliekama be ją gabenančio asmens priežiūros, išskyrus tuo atveju, kai ji saugoma laikantis II priede nustatytų reikalavimų;

    iv) paketas su ESĮI neatidaromas gabenimo metu arba ESĮI neskaitoma viešose vietose;

    v) asmenys informuojami apie jų pareigas, susijusias su saugumu.
39. Gabenant Europos Sąjungos parengtą trečiajai valstybei ar tarptautinei organizacijai skirtą slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėtą informaciją laikomasi atitinkamų nuostatų, numatytų susitarime dėl informacijos saugumo arba administraciniame susitarime pagal 13 straipsnio 2 dalies a arba b papunktį.
40. Slaptumo žyma RESTREINT UE/ES RESTRICTED pažymėtą informaciją taip pat gali gabenti pašto tarnybos ar komercinės kurjerių pašto tarnybos.
41. Slaptumo žyma TRES SECRET UE/ES TOP SECRET pažymėtą informaciją iš Europos Sąjungos į trečiosios valstybės teritoriją gabena karinis ar diplomatinis kurjeris.

VI. ESĮI NAIKINIMAS

42. Nebereikalingi ES įslaptinti dokumentai gali būti sunaikinti nepažeidžiant atitinkamų taisyklių ir nuostatų dėl archyvavimo.

43. Dokumentus, kurie turi būti registruojami pagal 9 straipsnio 2 dalį, turėtojo arba kompetentingos institucijos nurodymu sunaikina atsakinga registratūra. Registracijos knygos ir kita registravimo informacija atitinkamai atnaujinama.
44. Dokumentai, pažymėti SECRET UE/ES SECRET arba TRES SECRET UE/ES TOP SECRET slaptumo žyma, naikinami dalyvaujant liudytojui, kuris turi leidimą susipažinti su ne žemesnio už naikinamo dokumento slaptumo žymos laipsnio įslaptinta informacija.
45. Atsakingas registratūros darbuotojas ir liudytojas, kai pastarojo dalyvavimas privalomas, pasirašo sunaikinimo aktą, kuris registruojamas atitinkamame registre. Slaptumo žyma TRES SECRET UE/ES TOP SECRET pažymėtų dokumentų sunaikinimo aktai registre saugomi bent dešimt metų, o CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET slaptumo žyma pažymėtų dokumentų – bent penkerius metus.
46. Įslaptinti dokumentai, įskaitant pažymėtus slaptumo žyma RESTREINT UE/ES RESTRICTED, sunaikinami tokiais būdais, kurie atitinka atitinkamus Europos Sąjungos arba lygiaverčius standartus arba kuriuos valstybės narės patvirtino laikydamosi nacionalinių techninių standartų, kad jų nebūtų galima visiškai ar iš dalies atkurti.
47. Kompiuterinių duomenų saugojimo laikmenos, naudotos ESĮI, sunaikinamos vadovaujantis IV priedo 37 punkto nuostatomis.
48. Ekstremalios situacijos atveju, jei gresia tiesioginis neteisėto atskleidimo pavojus, ESĮI turėtojas sunaikina ją taip, kad ji negalėtų būti atkurta visa arba iš dalies. Rengėjas ir pradinis registras informuojami apie registruotos ESĮI sunaikinimą dėl ekstremalios situacijos.

VII. ĮVERTINIMO VIZITAI

49. Sąvoka „įvertinimo vizitas“ toliau vartojama nurodant:

    a) patikrinimus arba įvertinimo vizitus pagal 9 straipsnio 3 dalį ir 16 straipsnio 2 dalies e, f ir g papunkčius;

    b) įvertinimo vizitą pagal 13 straipsnio 5 dalį, kurių metu vertinamas priemonių, įgyvendintų siekiant apsaugoti ESĮI, veiksmingumas.

50. Įvertinimo vizitai atliekami, *inter alia*, siekiant:

a) užtikrinti, kad būtų laikomasi šiame sprendime nustatytų būtiniausių ESĮI apsaugos standartų;

b) tikrinamuose subjektuose pabrėžti saugumo ir veiksmingo rizikos valdymo svarbą;

c) rekomenduoti atsakomąsias priemones konkrečiam įslaptintos informacijos konfidencialumo praradimo, jos vientisumo ar prieinamumo netekimo poveikiui sušvelninti;

d) sustiprinti saugumo institucijų vykdomas švietimo saugumo klausimais ir sąmoningumo ugdymo programas.

51. Iki kiekvienų kalendorinių metų pabaigos Taryba patvirtina kitų metų įvertinimo vizitų programą, kaip numatyta 16 straipsnio 1 dalies c papunktyje. Faktinės kiekvieno įvertinimo vizito datos nustatomos suderinus su atitinkama Europos Sąjungos įstaiga ar agentūra, valstybe nare, trečiąja valstybe ar tarptautine organizacija.

Įvertinimo vizitų vykdymas

52. Įvertinimo vizitai atliekami siekiant patikrinti lankomo subjekto atitinkamas taisykles, reglamentus ir procedūras, taip pat patikrinti, ar subjekto praktika atitinka šiame sprendime nustatytus pagrindinius principus ir būtiniausius standartus ir keitimąsi įslaptinta informacija su tuo subjektu reglamentuojančias nuostatas.
53. Įvertinimo vizitai atliekami dviem etapais. Prieš vizitą prireikus organizuojamas parengiamasis susitikimas su atitinkamu subjektu. Po šio parengiamojo susitikimo įvertinimo grupė, suderinusi su atitinkamu subjektu, sudaro išsamią įvertinimo vizito programą, apimančią visas saugumo sritis. Įvertinimo vizito grupei turėtų būti leidžiama patekti į visas vietas, kuriose tvarkoma ESĮI, visų pirma, registrus ir RIS įrengimo vietas.
54. Įvertinimo vizitai į valstybių narių nacionalines administracines įstaigas, trečiąsias valstybes ir tarptautines organizacijas atliekami visapusiškai bendradarbiaujant su subjekto, trečiosios valstybės ar tarptautinės organizacijos, į kuriuos atliekamas vizitas, pareigūnais.
55. Įvertinimo vizitai į Europos Sąjungos įstaigas, agentūras ir subjektus, taikančius šį sprendimą arba jo principus, atliekami padedant NSI, kurios teritorijoje yra įsikūrusi įstaiga ar agentūra, ekspertams.

56. Įvertinimo vizitų į Europos Sąjungos įstaigas, agentūras ir subjektus, taikančius šį sprendimą ar jo principus, taip pat į trečiąsias valstybes bei tarptautines organizacijas atveju gali būti prašoma NSI ekspertų pagalbos ir nuomonių, laikantis išsamios tvarkos, dėl kurios turi susitarti Saugumo komitetas.

Ataskaitos

57. Pabaigus įvertinimo vizitą subjektui, į kurį atliktas vizitas, pateikiamos pagrindinės išvados ir rekomendacijos. Po to parengiama įvertinimo vizito ataskaita. Jei buvo pasiūlyti taisomieji veiksmai ir pateiktos rekomendacijos, ataskaitoje padarytos išvados turėtų būti pakankamai išsamiai pagrįstos. Ataskaita pateikiama atitinkamai subjekto, į kurį atliktas vizitas, tarnybai.
58. Jei įvertinimo vizitai atliekami valstybių narių nacionalinėse administracinėse įstaigose:

    a) įvertinimo ataskaitos projektas nusiunčiamas atitinkamai NSI, kad ši patikrintų jame pateikiamų faktų teisingumą, taip pat ar jame nėra jokios informacijos, pažymėtos aukštesnio laipsnio nei RESTREINT UE/ES RESTRICTED slaptumo žyma;

    b) išskyrus atvejus, kai atitinkamos valstybės narės NSI paprašo, kad įvertinimo ataskaitos nebūtų platinamos, jos išplatinamos Saugumo komitetui. Ataskaita įslaptinama pažymint slaptumo žyma RESTREINT UE/ES RESTRICTED.

    TGS saugumo tarnyba atsako už tai, kad būtų rengiama reguliari ataskaita, kurioje būtų akcentuojama nurodytu laikotarpiu valstybėse narėse atliktų įvertinimo vizitų metu įgyta patirtis ir kurią išnagrinėtų Saugumo komitetas.
59. Trečiųjų valstybių ir tarptautinių organizacijų įvertinimo vizitų atveju ataskaita išplatinama Saugumo komitetui. Ataskaita pažymima ne žemesnio laipsnio nei RESTREINT UE/ES RESTRICTED slaptumo žyma. Taisomieji veiksmai patikrinami kito vizito metu ir apie juos pranešama Saugumo komitetui.

60. Įvertinimo vizitų į Europos Sąjungos įstaigas, agentūras ir subjektus, taikančius šį sprendimą ar jo principus, atveju įvertinimo vizitų ataskaitos išplatinamos Saugumo komitetui. Įvertinimo vizito ataskaitos projektas nusiunčiamas atitinkamai agentūrai ar įstaigai, kad ši patikrintų jame pateikiamų faktų teisingumą, taip pat ar jame nėra jokios informacijos, pažymėtos aukštesne nei RESTREINT UE/ES RESTRICTED slaptumo žyma. Taisomieji veiksmai patikrinami kito vizito metu ir apie juos pranešama Saugumo komitetui.
61. TGS saugumo tarnyba vykdo reguliarius TGS organizacinių vienetų patikrinimus 50 punkte nustatytais tikslais.

Kontrolinis sąrašas

62. TGS saugumo tarnyba parengia ir atnaujina dalykų, tikrintinų vykdant įvertinimo vizitą, kontrolinį sąrašą. Šis kontrolinis sąrašas pateikiamas Saugumo komitetui.
63. Kontroliniam sąrašui užpildyti būtina informacija gaunama, visų pirma, vizito metu iš tikrinamo subjekto saugumo valdymo tarnybų. Išsamiai užpildžius kontrolinį sąrašą, susitarus su tikrinamu subjektu, sąrašas įslaptinamas. Jis negali būti patikrinimo ataskaitos sudedamoji dalis.

IV PRIEDAS

RIS TVARKOMOS ESĮI APSAUGA

I. ĮVADAS

1. Šiame priede nustatytos 10 straipsnio įgyvendinimo nuostatos.
2. Toliau išdėstytos ISU savybės ir sąvokos yra būtinos saugumui ir tinkamam RIS operacijų vykdymui užtikrinti:

Autentiškumas:	užtikrinimas, kad informacija yra tikra ir gauta iš *bona fide* šaltinių;
Prieinamumas:	galimybė leidimą turinčiam subjektui pateikus prašymą gauti informaciją ir ja naudotis;
Konfidencialumas:	savybė, kuri reiškia, kad informacija nėra atskleidžiama neturintiems leidimo asmenims, subjektams ar procesams;
Vientisumas:	savybė, kuri reiškia, kad apsaugomas informacijos tikslumas ir išsamumas bei turtas;
Atsakomybės už veiksmus prisiėmimas:	galimybė įrodyti, kad veiksmas buvo atliktas ar įvykis įvyko, kad šio įvykio ar veiksmo po to negalima būtų išsižadėti.

II. INFORMACIJOS SAUGUMO UŽTIKRINIMO PRINCIPAI

3. Toliau išdėstytos nuostatos yra RIS, kurioje tvarkoma ESĮI, saugumo užtikrinimo pagrindas. Išsamūs šių nuostatų įgyvendinimo reikalavimai nustatyti ISU saugumo politikoje ir saugumo gairėse.

Saugumo rizikos valdymas

4. Saugumo rizikos valdymas yra neatsiejama RIS apibrėžties, kūrimo, veikimo ir priežiūros dalis. Rizikos valdymą (įvertinimą, traktavimą, pripažinimą ir informavimą), kaip kartotinį procesą, kartu vykdo sistemos savininkų, projekto institucijų, vykdančiųjų institucijų ir saugumo patvirtinimo institucijų atstovai, taikydami pavirtintą, skaidrų ir visiškai suprantamą rizikos įvertinimo procesą. RIS ir jos turinio taikymo sritis aiškiai apibrėžiama rizikos valdymo proceso pradžioje.
5. Kompetentingos institucijos peržiūri pavojus, kurie gali kilti RIS, ir nuolat vykdo naujausiais duomenimis grindžiamus ir tikslius pavojų įvertinimus, kurie atspindi esamą sistemos operacinę aplinką. Jos nuolat atnaujina savo žinias pažeidžiamumo klausimais ir reguliariai peržiūri pažeidžiamumo įvertinimą, neatsilikdamos nuo informacinių technologijų (IT) aplinkos pokyčių.
6. Tvarkant saugumo riziką siekiama taikyti apsaugos priemonių rinkinį, kuris užtikrina tinkamą vartotojų reikalavimų, sąnaudų ir likutinės rizikos, susijusios su saugumu, pusiausvyrą.
7. RIS akreditavimui taikomi konkretūs reikalavimai, reikalavimai dėl informacijos apimties ir išsamumo, kuriuos nustato atitinkama SAI, turi atitikti įvertintą riziką, atsižvelgiant į visus svarbius veiksnius, įskaitant ESĮI, kuri tvarkoma RIS, slaptumo žymos laipsnį. Akreditavimas apima atsakingos institucijos oficialų pareiškimą dėl likutinės rizikos ir likutinės rizikos pripažinimą.

Saugumas viso RIS gyvavimo ciklo metu

8. Saugumas turi būti užtikrintas viso RIS gyvavimo ciklo metu – nuo pradžios iki naudojimosi pabaigos.
9. Kiekvienu gyvavimo ciklo etapu nustatomas kiekvieno RIS dalyvio ir jo sąveikos su kitais dalyviais vaidmuo saugumo požiūriu.
10. RIS, įskaitant technines ir netechnines saugumo priemones, bandomos saugumo požiūriu akreditavimo proceso metu siekiant užtikrinti tinkamą saugumo užtikrinimo lygį ir patikrinti, ar jos teisingai įdiegtos, integruotos ir sukonfigūruotos.
11. Saugumo įvertinimai, patikrinimai ir peržiūros atliekami reguliariai RIS veikimo ir techninės priežiūros metu bei susidarius išskirtinėms aplinkybėms.

12. RIS saugumo dokumentų atnaujinimas viso jos gyvavimo ciklo metu vykdomas kaip neatsiejama pakeitimų atlikimo ir konfigūracijos tvarkymo proceso dalis.

Geriausia patirtis

13. TGS ir valstybės narės bendradarbiauja rengdami geriausios praktikos pavyzdžius RIS tvarkomai ESĮI apsaugoti. Geriausios praktikos gairėse išdėstomos RIS skirtos techninės, fizinės, organizacinės ir procedūrinės saugumo priemonės, kurių veiksmingumas apsisaugant nuo konkrečių grėsmių ir pažeidžiamumo buvo įrodytas.
14. RIS tvarkomos ESĮI apsauga grindžiama ir Europos Sąjungoje, ir už jos ribų ISU srityje dirbančių subjektų įgyta patirtimi.
15. Geriausios praktikos pavyzdžių platinimu ir jų įgyvendinimu prisidedama prie siekio užtikrinti lygiavertį įvairių TGS ir valstybių narių naudojamų RIS, kuriose tvarkoma ESĮI, saugumo užtikrinimo lygį.

Nuodugni apsauga

16. Siekiant sušvelninti pavojų RIS, įgyvendinama daug techninių ir netechninių saugumo priemonių, kurios grupuojamos kaip kelios gynybinės linijos. Jos apima:

    a) atgrasymą – saugumo priemones, skirtas įtikinti nerengti priešiškų planų pulti RIS;

    b) prevenciją – saugumo priemones, skirtas apsunkinti RIS puolimą arba jam sutrukdyti;

    c) aptikimą – saugumo priemones, skirtas aptikti RIS puolimo atvejį;

    d) atsparumą – saugumo priemones, skirtas apriboti puolimo poveikį iki mažiausio informacijos rinkinio ar RIS dalių grupės bei užkirsti kelią tolesnei žalai;

    e) atstatymą – saugumo priemones, skirtas RIS saugiai padėčiai atkurti.

    Tokių saugumo priemonių griežtumo lygis nustatomas atsižvelgiant į rizikos įvertinimą.

17. NSI ar kita kompetentinga institucija užtikrina, kad:

    a) būtų įdiegti kibernetinės gynybos pajėgumai, reikalingi reaguojant į grėsmes, galinčias apimti kelias organizacijas ar valstybes;

    b) atsakomieji veiksmai būtų koordinuojami ir būtų dalijamasi informacija apie šias grėsmes, incidentus bei susijusią riziką (kompiuterinių incidentų tyrimo gebėjimai).

Minimalumo ir mažiausių privilegijų principas

18. Įdiegiamos tik atsižvelgiant į operacinius reikalavimus būtinos funkcijos, prietaisai ir paslaugos siekiant išvengti bereikalingos rizikos.
19. RIS naudotojams ir automatizuotiems procesams suteikiama tik tokia prieiga, privilegijos ar leidimai, kokios jiems reikia savo užduotims atlikti, siekiant apriboti žalą, kuri padaroma dėl avarijų, klaidų ar RIS išteklių naudojimo be leidimo.
20. RIS atliekamos registravimo procedūros prireikus patikrinamos akreditavimo proceso metu.

Informuotumas informacijos saugumo užtikrinimo srityje

21. Informuotumas apie riziką ir turimas saugumo priemones yra pirmoji RIS saugumo gynybos linija. Visų pirma, visi personalo nariai, susiję su RIS gyvavimo ciklu, įskaitant naudotojus, suvokia:

    a) kad saugumo spragos gali labai pakenkti RIS;

    b) galimą žalą kitiems, kuri gali kilti dėl tarpusavio sujungimo ir tarpusavio priklausomybės;

    c) savo asmeninę atsakomybę ir atsakingumą už RIS saugumą atsižvelgdami į savo vaidmenį naudojant sistemas ir procesus.
22. Siekiant užtikrinti, kad būtų suvokiama atsakomybė už saugumą visam dalyvaujančiam personalui, įskaitant aukštesniąją vadovybę ir RIS naudotojus, yra privalomi ISU švietimo ir informuotumo mokymai.

IT saugumo priemonių vertinimas ir patvirtinimas

23. Reikiamas saugumo priemonių patikimumo lygis, apibrėžiamas kaip saugumo užtikrinimo lygis, nustatomas remiantis rizikos valdymo proceso rezultatais ir laikantis atitinkamos saugumo politikos bei saugumo gairių.
24. Saugumo užtikrinimo lygis patikrinamas naudojant tarptautiniu arba nacionaliniu lygiu patvirtintus procesus ir metodus. Tai apima pirminį įvertinimą, kontrolę ir auditą.
25. ESĮI apsaugai skirtas šifravimo priemones įvertina ir patvirtina valstybės narės nacionalinė KPI.
26. Prieš rekomenduojant, kad pagal 10 straipsnio 6 dalį jas pavirtintų Taryba arba Generalinis sekretorius, tokias šifravimo priemones turi būti įvertinusi antra šalis, t. y. valstybės narės Tinkamos kvalifikacijos institucija (TKI), kuri nesusijusi su įrangos projektavimu arba gamyba. Reikalaujamas antros šalies įvertinimo išsamumo lygis priklauso nuo numatomo didžiausio ESĮI, kuri bus apsaugoma šiomis priemonėmis, slaptumo žymos laipsnio. Taryba patvirtina šifravimo priemonių vertinimo ir patvirtinimo saugumo politiką.
27. Atitinkamai Taryba arba Generalinis sekretorius, remdamiesi Saugumo komiteto rekomendacija, gali netaikyti šio priedo 25 arba 26 punkte nustatytų reikalavimų ir tam tikram laikotarpiui suteikti laikiną patvirtinimą laikydamiesi 10 straipsnio 6 dalyje nustatytos tvarkos, kai tai pateisinama dėl konkrečių su veikla susijusių priežasčių.
28. Taryba, remdamasi Saugumo komiteto rekomendacija, gali pritarti trečiosios valstybės arba tarptautinės organizacijos šifravimo priemonių vertinimo, atrankos ir patvirtinimo procesui ir atitinkamai tokias šifravimo priemones laikyti patvirtintomis, siekdama apsaugoti ESĮI, suteikiamą tai trečiajai valstybei arba tarptautinei organizacijai.
29. TKI yra valstybės narės KPI, kuri buvo akredituota remiantis Tarybos nustatytais kriterijais antram ESĮI apsaugai skirtų šifravimo priemonių įvertinimui atlikti.
30. Taryba patvirtina *ne šifravimo* IT saugumo priemonių reikalavimų atitikimo ir patvirtinimo saugumo politiką.

Perdavimas saugumo ir administracinėse zonose

31. Nepaisant šio sprendimo nuostatų, kai ESĮI perdavimas vykdomas saugumo zonose arba administracinėse zonose, remiantis rizikos valdymo proceso rezultatais ir SAI pritarus, gali būti naudojamas nešifruotas perdavimas arba šifravimas žemesniu lygiu.

Saugus RIS tarpusavio sujungimas

32. Šiame sprendime sistemų tarpusavio sujungimas reiškia tiesioginį dviejų ar daugiau IT sistemų sujungimą siekiant dalytis duomenimis ir kitais informacijos šaltiniais (pavyzdžiui, ryšiais) vienakrypčiu arba daugiakrypčiu būdu.
33. RIS kiekviena tarpusavyje sujungta IT sistema pirmiausia yra traktuojama kaip nepatikima ir sistemoje įdiegiamos apsaugos priemonės keitimuisi įslaptinta informacija kontroliuoti.
34. Bet kokio RIS ir kitos IT sistemos tarpusavio sujungimo atveju laikomasi toliau išdėstytų pagrindinių reikalavimų:

    a) tokiems tarpusavio sujungimams taikomus veiklos arba operacinius reikalavimus nurodo ir patvirtina atsakingos institucijos;

    b) tarpusavio sujungimui taikomas rizikos valdymas ir akreditavimo procesas bei yra reikalingas kompetentingų SAI pavirtinimas;

    c) ribų apsaugos priemonės (RAP) įdiegiamos visų RIS perimetre.
35. Akredituota RIS ir neapsaugotas arba viešas tinklas negali būti tarpusavyje sujungiami, išskyrus atvejus, kai tarp RIS ir neapsaugoto arba viešo tinklo yra šiuo tikslu įdiegtos patvirtintos ribų apsaugos priemonės. Tokiems tarpusavio sujungimams taikytinas saugumo priemones peržiūri kompetentinga ISUI ir patvirtina kompetentinga SAI.

    Kai duomenys, perduodami neapsaugotu arba viešu tinklu, yra užšifruojami pagal 10 straipsnį patvirtinta šifravimo priemone. Toks sujungimas nelaikomas tarpusavio sujungimu.
36. Draudžiamas tiesioginis arba pakopinis RIS, akredituotos tvarkyti slaptumo žyma TRES SECFRET UE/ES TOP SECRET pažymėtą informaciją, ir neapsaugoto arba viešo tinklo tarpusavio sujungimas.

Kompiuterinių duomenų saugojimo laikmenos

37. Kompiuterinių duomenų saugojimo laikmenos sunaikinamos laikantis kompetentingos saugumo institucijos patvirtintų procedūrų.
38. Kompiuterinių duomenų saugojimo laikmenos gali būti naudojamos pakartotinai, gali būti sumažintas jų slaptumo žymos laipsnis arba jos gali būti išslaptinamos laikantis saugumo gairių, kurios turi būti nustatytos pagal 6 straipsnio 2 dalį.

Nepaprastosios padėties sąlygos

39. Nepaisant šio sprendimo nuostatų, toliau apibūdintos specialios procedūros gali būti taikomos esant nepaprastajai padėčiai, pavyzdžiui, gresiant ar esant krizei, konfliktui ar karinei padėčiai arba susidarius išskirtinėms su eksploatavimu susijusioms sąlygoms.
40. ESĮI gali būti perduodama naudojant šifravimo priemones, kurios buvo patvirtintos žemesnio įslaptinimo laipsnio informacijai, arba nešifruota kompetentingai institucijai pritarus, jei vėlavimas padarytų aiškiai didesnę žalą, negu įslaptintos medžiagos atskleidimas, ir jei:

    a) siuntėjas ir gavėjas neturi reikiamos šifravimo įrangos arba jokios šifravimo įrangos;

    b) įslaptinta medžiaga negali būti laiku perduota kitomis priemonėmis.
41. 39 punkte išdėstytomis aplinkybėmis perduodama įslaptinta informacija nėra pažymėta jokiomis žymomis arba nuorodomis, kurios sudarytų sąlygas ją atskirti nuo neįslaptintos informacijos arba kurią galima apsaugoti naudojant turimas šifravimo priemones. Gavėjams kitomis priemonėmis nedelsiant pranešama apie informacijos slaptumo laipsnį.
42. Jeigu taikomas 39 punktas, kompetentingai institucijai ir Saugumo komitetui vėliau pateikiama ataskaita.

III. SU INFORMACIJOS SAUGUMO UŽTIKRINIMU SUSIJUSIOS FUNKCIJOS IR INSTITUCIJOS

43. Valstybėse narėse ir TGS nustatomos toliau išdėstytos su informacijos saugumo užtikrinimu susijusios funkcijos. Šioms funkcijoms nereikalingas vienas bendras organizacinis subjektas. Joms suteikiami atskiri įgaliojimai. Tačiau šios funkcijos ir su jomis susijusi atsakomybė gali būti sujungtos arba integruotos viename organizaciniame vienete arba padalytos skirtingiems organizaciniams vienetams, jei išvengiama vidaus interesų arba užduočių konfliktų.

Informacijos saugumo užtikrinimo institucija

44. ISUI atsako už šias sritis:

a) ISU srities saugumo politikos formavimą ir saugumo gairių rengimą bei jų veiksmingumo bei tinkamumo stebėseną;

b) su šifravimo priemonėmis susijusios techninės informacijos apsaugą ir administravimą;

c) užtikrinimą, kad ESĮI apsaugai parinktos ISU priemonės atitiktų atitinkamą jų tinkamumo nustatymo ir atrankos politiką;

d) užtikrinimą, kad šifravimo priemonės būtų pasirenkamos laikantis jų tinkamumo nustatymo ir atrankos politikos;

e) mokymo ir informuotumo ISU srityje derinimą;

f) konsultavimąsi su sistemos tiekėju, saugumo srities subjektais ir vartotojų atstovais ISU saugumo politikos ir saugumo gairių klausimais;

g) užtikrinimą, kad Saugumo komiteto ISU klausimais ekspertų pogrupis turėtų atitinkamų žinių.

TEI

45. TEI užtikrina, kad RIS atitiktų TEMPEST politiką ir gaires. Ji patvirtina TEMPEST kontrpriemones, skirtas įrenginiams ir priemonėms, siekiant apsaugoti ESĮI iki nustatyto slaptumo žymos laipsnio operacinėje aplinkoje.

Kriptografijos patvirtinimo institucija

46. Kriptografijos patvirtinimo institucijos (KPI) pareiga – užtikrinti, kad šifravimo priemonės atitiktų nacionalinę šifravimo politiką arba Tarybos šifravimo politiką. Ji suteikia leidimą naudoti šifravimo priemonę siekiant apsaugoti ESĮI iki nustatyto slaptumo žymos laipsnio operacinėje aplinkoje. Valstybėse narėse KPI papildomai atsako už šifravimo priemonių įvertinimą.

Kriptografijos platinimo institucija

47. Kriptografijos platinimo institucija atsako už šias sritis:

a) ES šifravimo medžiagos valdymą ir apskaitą;

b) užtikrinimą, kad visos ES šifravimo medžiagos apskaitai, saugiam tvarkymui, saugojimui ir platinimui būtų taikomos tinkamos procedūros ir nustatyti tinkami kanalai;

c) ES šifravimo medžiagos perdavimo ją naudojantiems asmenims ir tarnyboms arba priėmimo iš jų užtikrinimą.

Saugumo akreditavimo institucija

48. Kiekvienai sistemai skirta SAI atsako už šias sritis:

a) užtikrinimą, kad RIS atitiktų atitinkamą saugumo politiką ir saugumo gaires, pareiškimo dėl RIS patvirtinimo, leidžiant jas naudoti tvarkant ESĮI iki nustatyto slaptumo žymos laipsnio operacinėje aplinkoje, pateikimą, nurodant akreditavimo reikalavimus ir sąlygas bei kriterijus, kuriais remiantis sprendžiama, kad reikia iš naujo patvirtinti arba akredituoti RIS;

b) saugumo akreditavimo proceso nustatymą, vadovaujantis atitinkama politika, aiškiai nurodant patvirtinimo sąlygas, nustatytas jos priežiūrai pavestoms RIS;

c) saugumo akreditavimo strategijos, kurioje išdėstytas akreditavimo proceso išsamumo lygis, atitinkantis reikiamą saugumo užtikrinimo lygį, nustatymą;

d) su saugumu susijusių dokumentų, įskaitant pareiškimus dėl rizikos valdymo ir likutinės rizikos, sistemos saugumo reikmių aktus (toliau – SSRA), saugumo įgyvendinimo patikrinimo dokumentus ir saugios eksploatacijos taisykles (toliau – SecOPs), nagrinėjimą ir patvirtinimą bei užtikrinimą, kad jie atitiktų Tarybos saugumo taisykles ir politiką;

e) su RIS susijusių saugumo priemonių įgyvendinimo patikrinimą vykdant saugumo įvertinimus, patikrinimus ar peržiūras arba juos finansuojant;

f) saugumo reikalavimų (pavyzdžiui, susijusių su personalo patikimumo laipsniais), taikomų svarbiausioms, susijusioms su RIS apsauga pareigybėms, nustatymą;

g) patvirtintų šifravimo ir TEMPEST priemonių, naudojamų siekiant užtikrinti RIS saugumą, parinkimo patvirtinimą;

h) RIS tarpusavio sujungimo su kitomis RIS patvirtinimą arba prireikus dalyvavimą bendrame patvirtinime;

i) sistemos tiekėjo, saugumo srities subjektų ir vartotojų atstovų konsultavimą saugumo rizikos valdymo, visų pirma, likutinės rizikos, ir pareiškimo dėl patvirtinimo reikalavimų ir sąlygų klausimais.

49. TGS SAI atsako už visų TGS kompetencijai priklausančių RIS akreditavimą.
50. Atitinkama valstybės narės SAI atsako už tos valstybės narės kompetencijai priklausančių RIS ir jų sisteminių komponentų akreditavimą.
51. Jungtinė saugumo akreditacijos valdyba (SAV) yra atsakinga tiek už TGS SAI žinioje, tiek už valstybių narių SAI žinioje esančių RIS akreditavimą. Ją sudaro po vieną kiekvienos valstybės narės SAI atstovą, o jos posėdžiuose dalyvauja Europos Komisijos atstovas SAI klausimais. Kiti subjektai, turintys prijungimo prie RIS mazgus, kviečiami dalyvauti posėdžiuose, kai svarstomi su ta sistema susiję klausimai.

    SAV pirmininkauja TGS SAI atstovas. Ji sprendimus priima institucijų, valstybių narių ir kitų subjektų, turinčių prijungimo prie RIS mazgus, SAI atstovų sutarimu. SAV reguliariai teikia savo veiklos ataskaitas Saugumo komitetui ir jam praneša apie visus pareiškimus dėl akreditavimo.

Informacijos saugumo užtikrinimo operacinė institucija

52. Kiekvienai sistemai skirta ISU operacinė institucija atsako už šias sritis:

a) saugumo dokumentų, atitinkančių saugumo politiką ir saugumo gaires, rengimą, visų pirma, SSRA, įskaitant pareiškimą dėl likutinės rizikos, SecOPs ir šifravimo planą vykdant RIS akreditavimo procesą, rengimą;

b) dalyvavimą atrenkant ir bandant konkrečioms sistemoms skirtas techninio saugumo priemones, prietaisus ir programinę įrangą, jų įgyvendinimo priežiūrą ir užtikrinimą, kad jie būtų saugiai įdiegti, sukonfigūruoti bei eksploatuojami pagal atitinkamus saugumo dokumentus;

c) dalyvavimą parenkant TEMPEST saugumo priemones ir prietaisus, jei reikia pagal SSRA, ir užtikrinimą, kad jie būtų saugiai įdiegti ir eksploatuojami bendradarbiaujant su TEI;

d) SecOps įgyvendinimo ir taikymo stebėseną; prireikus atsakomybę už eksploatavimo saugumą deleguojant sistemos savininkui;

e) šifravimo priemonių valdymą ir tvarkymą užtikrinant šifravimo ir kontroliuojamų objektų saugojimą ir prireikus užtikrinant šifravimo kintamųjų generavimą;

f) saugumo analizės peržiūros ir bandymų atlikimą, visų pirma, siekiant parengti atitinkamas rizikos ataskaitas, kurių reikalauja SAI;

g) mokymo konkrečioms RIS skirto ISU klausimais rengimą;

h) konkrečioms RIS skirtų apsaugos priemonių įgyvendinimą ir vykdymą.

V PRIEDAS

PRAMONINIS SAUGUMAS

I. ĮVADAS

1. Šiame priede nustatytos 11 straipsnio įgyvendinimo nuostatos. Jame išdėstytos bendros saugumo nuostatos, taikomos pramonės ar kitiems subjektams derybų dėl sutarčių sudarymo metu arba visą TGS sudarytų įslaptintų sutarčių gyvavimo ciklą.
2. Taryba patvirtina pramoninio saugumo gaires, kuriose, visų pirma, apibrėžiami išsamūs reikalavimai, susiję su ĮPPP, saugumo aspektų paaiškinimais (SAP), vizitais, ESĮI perdavimu ir gabenimu.

II. SAUGUMO ASPEKTAI ĮSLAPTINTOSE SUTARTYSE

Slaptumo žymų vadovas (SŽV)

3. Prieš paskelbdamas kvietimą teikti pasiūlymus įslaptintai sutarčiai sudaryti arba prieš sudarydamas įslaptintą sutartį, TGS, kaip perkančioji institucija, nustato visos informacijos, kuri turi būti suteikta konkurso dalyviams ir rangovams, slaptumo žymą, taip pat visos informacijos, kurią turi parengti rangovas, slaptumo žymą. Šiuo tikslu TGS parengia SŽV, kuris turi būti naudojamas vykdant sutartį.
4. Siekiant nustatyti skirtingų įslaptintos sutarties dalių slaptumo žymą, taikomi toliau nurodyti principai:

   a) rengdamas SŽV, TGS atsižvelgia į visus svarbius saugumo aspektus, įskaitant slaptumo žymą, kurią informacijai priskyrė jos įslaptintos informacijos rengėjas ir kurią jis patvirtino kaip naudotiną tai sutarčiai;

   b) bendras sutarties slaptumo žymos laipsnis negali būti žemesnis nei aukščiausia bet kurios jos dalies slaptumo žyma;

   c) atitinkamais atvejais, jei daromi pakeitimai, susiję su slaptumo žymų suteikimu informacijai, parengtai rangovų ar jiems suteiktai vykdant sutartį, ir jei daromi vėlesni SŽV pakeitimai, TGS palaiko ryšius su valstybių narių NSI/PSI ar kitomis atitinkamomis kompetentingomis saugumo institucijomis.

Saugumo aspektų paaiškinimas (SAP)

5. Konkrečioms sutartims skirti saugumo reikalavimai aprašomi SAP. Prireikus į SAP įtraukiamas SŽV. SAP yra neatsiejama įslaptintos sutarties ar subrangos sutarties dalis.
6. SAP nustatomos nuostatos, pagal kurias reikalaujama, kad rangovas ir (arba) subrangovas laikytųsi būtiniausių šiame sprendime nustatytų standartų. Šių būtiniausių standartų nesilaikymas gali būti pakankamas pagrindas sutarčiai nutraukti.

Programos / projekto saugumo instrukcijos (PRSI)

7. Atsižvelgdama į programų ar projektų, kuriuos vykdant reikia susipažinti su ESĮI arba ją tvarkyti ar saugoti, apimtį, programą ar projektą valdyti paskirta perkančioji institucija gali parengti konkrečios PRSI. PRSI turi patvirtinti valstybių narių NSI/PSI ar kita PRSI dalyvaujanti kompetentinga saugumo institucija. Jose gali būti nustatyta papildomų saugumo reikalavimų.

III. ĮMONĖS PATIKIMUMĄ PATVIRTINANTIS PAŽYMĖJIMAS (ĮPPP)

8. ĮPPP išduoda valstybės narės NSI arba PSI ar kita kompetentinga saugumo institucija ir jame pagal nacionalinius įstatymus ir kitus teisės aktus nurodoma, kad pramonės arba kitas subjektas savo patalpose gali apsaugoti atitinkamos slaptumo žymos (CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET) ESĮI. Prieš rangovui ar subrangovui arba potencialiam rangovui ar subrangovui suteikiant ESĮI arba galimybę susipažinti su ESĮI, TGS, kaip perkančiajai institucijai, turi būti pateikiamas ĮPPP.
9. Išduodama ĮPPP atitinkama NSI ar PSI, mažų mažiausiai:

   a) įvertina pramonės ar kitų subjektų patikimumą;

   b) įvertina nuosavybę, kontrolę ar nederamos įtakos tikimybę, kurie gali būti laikomi saugumo rizika;

   c) įsitikina, kad pramonės arba kitas subjektas patalpose yra sukūręs saugumo sistemą, kuri apima visas atitinkamas saugumo priemones, būtinas, kad būtų apsaugota informacija ar medžiaga, pažymėta CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET slaptumo žyma, laikantis šiame sprendime nustatytų reikalavimų;

d) įsitikina, kad vadovybės, savininkų ir darbuotojų, kurie turi turėti galimybę susipažinti su informacija, pažymėta CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET slaptumo žyma, asmens patikimumo statusas yra nustatytas laikantis šiame sprendime nustatytų reikalavimų;

e) įsitikina, kad pramonės arba kitas subjektas yra paskyręs patalpų saugumo pareigūną, kuris yra atsakingas vadovybei už saugumo įsipareigojimų tokiame subjekte vykdymo užtikrinimą.

10. Atitinkamais atvejais TGS, kaip perkančioji institucija, praneša atitinkamai NSI/PSI ar kitai kompetentingai saugumo institucijai, kad prieš sudarant sutartį arba sutarties vykdymui reikalingas ĮPPP. ĮPPP arba APP reikalaujama prieš sudarant sutartį, tais atvejais, kai ESĮI, pažymėta CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET slaptumo žyma, turi būti suteikta paraiškų teikimo proceso metu.
11. Perkančioji institucija nesudaro įslaptintos sutarties su pasirinktu dalyviu prieš tai negavusi valstybės narės, kurioje yra registruotas atitinkamas rangovas ar subrangovas, NSI/PSI ar kitos kompetentingos saugumo institucijos patvirtinimo, kad reikiamais atvejais yra išduotas tinkamas ĮPPP.
12. ĮPPP išdavusi NSI/PSI ar kita kompetentinga saugumo institucija praneša TGS, kaip perkančiajai institucijai, apie pasikeitimus, turinčius įtakos ĮPPP. Subrangos sutarties atveju atitinkamai informuojama NSI/PSI ar kita kompetentinga saugumo institucija.
13. Jeigu atitinkama NSI/PSI ar kita kompetentinga saugumo institucija panaikina ĮPPP, tai yra pakankamas pagrindas TGS, kaip perkančiajai institucijai, nutraukti įslaptintą sutartį arba pašalinti dalyvį iš konkurso.

IV. ĮSLAPTINTOS SUTARTYS IR SUBRANGOS SUTARTYS

14. Tais atvejais, kai ESĮI suteikiama dalyviui prieš sudarant sutartį, kvietime teikti paraiškas numatoma nuostata, kuria paraiškos nepateikęs dalyvis arba dalyvis, kuris nebuvo atrinktas, įpareigojamas per nurodytą laiką grąžinti visus įslaptintus dokumentus.
15. Sudarius įslaptintą sutartį ar subrangos sutartį, TGS, kaip perkančioji institucija, praneša rangovo ar subrangovo NSI/PSI ar kitai kompetentingai saugumo institucijai tos įslaptintos sutarties saugumo nuostatas.

16. Nutraukus tokią sutartį, TGS, kaip perkančioji institucija (ir (arba) atitinkamai NSI/PSI ar kita kompetentinga saugumo institucija subrangos sutarties atveju) skubiai apie tai praneša valstybės narės, kurioje registruotas rangovas arba subrangovas, NSI/PSI ar kitai kompetentingai saugumo institucijai.
17. Paprastai reikalaujama, kad nutraukus įslaptintą sutartį ar subrangos sutartį rangovas arba subrangovas perkančiajai institucijai grąžintų visą turimą ESĮI.
18. Konkrečios nuostatos dėl ESĮI sunaikinimo vykdant sutartį arba ją nutraukus nustatomos SAP.
19. Tais atvejais, kai rangovui arba subrangovui duotas leidimas nutraukus sutartį pasilikti ESĮI, rangovas ir subrangovas toliau laikosi šiame sprendime nustatytų būtiniausių standartų bei užtikrina ESĮI konfidencialumą.
20. Sąlygos, kuriomis rangovas gali sudaryti subrangos sutartis, nurodomos kvietime teikti paraiškas ir sutartyje.
21. Prieš sudarydamas subrangos sutartis dėl įslaptintos sutarties dalių, rangovas turi gauti TGS, kaip perkančiosios institucijos, leidimą. Su pramonės arba kitais subjektais, registruotais valstybėje, kuri nėra ES valstybė narė ir nėra sudariusi susitarimo dėl informacijos saugumo su Europos Sąjunga, subrangos sutartys negali būti sudaromos.
22. Rangovas atsako už tai, kad visa subrangos veikla būtų vykdoma laikantis šiame sprendime nustatytų būtiniausių standartų, ir negali suteikti subrangovui ESĮI be išankstinio rašytinio perkančiosios institucijos sutikimo.
23. ESĮI, kurią parengė ar tvarko rangovas arba subrangovas, atžvilgiu įslaptintos informacijos rengėjo teisėmis naudojasi perkančioji institucija.

V. SU ĮSLAPTINTOMIS SUTARTIMIS SUSIJĘ VIZITAI

24. Jei, vykdant įslaptintą sutartį, TGS, rangovų ar subrangovų personalui vienas kito patalpose reikia susipažinti su CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET slaptumo žyma pažymėta informacija, dėl vizitų susitariama palaikant ryšius su NSI/PSI arba kita susijusia kompetentinga saugumo institucija. Tačiau atsižvelgiant į tam tikrus projektus NSI/PSI gali taip pat susitarti dėl tvarkos, pagal kurią dėl tokių vizitų gali būti susitariama tiesiogiai.

25. Tam, kad būtų leista susipažinti su ESĮI, susijusia su TGS sutartimi, visi lankytojai turi turėti atitinkamą APP ir turi būti vadovaujamasi principu „būtina žinoti“.
26. Lankytojams leidžiama susipažinti tik su ta ESĮI, kuri yra susijusi su vizito tikslu.

VI. ESĮI PERDAVIMAS IR GABENIMAS

27. Perduodant ESĮI elektroninėmis priemonėmis taikomos atitinkamos 10 straipsnio ir IV priedo nuostatos.
28. Gabenant ESĮI taikomos atitinkamos III priedo nuostatos, laikantis nacionalinių įstatymų ir kitų teisės aktų.
29. Nustatant įslaptintos medžiagos, kaip krovinio, gabenimui taikomą saugumo tvarką taikomi toliau nurodyti principai:

    a) saugumas užtikrinamas visuose gabenimo etapuose nuo gabenimo pradžios vietos iki galutinės paskirties vietos;

    b) siuntai suteikiamas apsaugos lygis nustatomas pagal joje esančios medžiagos aukščiausią slaptumo žymos laipsnį;

    c) gabenimą užtikrinančios bendrovės turi gauti atitinkamos slaptumo žymos ĮPPP. Tokiais atvejais laikantis I priedo turi būti patikrintas siuntą gabenančio personalo patikimumas;

    d) prieš gabenant per valstybių sienas medžiagą, pažymėtą CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET slaptumo žyma, siuntėjas parengia, o atitinkamos NSI/PSI ar kitos kompetentingos saugumo institucijos patvirtina gabenimo planą;

    e) stengiamasi, kad kelionės vyktų be sustojimo ir būtų užbaigtos kuo greičiau, atsižvelgiant į aplinkybes;

    f) kai galima, turėtų būti pasirenkami maršrutai tik per valstybių narių teritorijas. Maršrutais per valstybes, kurios nėra valstybės narės, turėtų būti gabenama tik gavus siuntėjo ir gavėjo valstybių NSI/PSI ar kitos kompetentingos saugumo institucijos leidimą.

VII. ESĮI PERDAVIMAS TREČIOSIOSE VALSTYBĖSE ĮSIKŪRUSIEMS RANGOVAMS

30. ESĮI trečiosiose valstybėse įsikūrusiems rangovams ir subrangovams perduodama laikantis saugumo priemonių, dėl kurių susitarė TGS, kaip perkančioji institucija, ir atitinkamos trečiosios valstybės, kurioje registruotas rangovas, NSI/PSI.

VIII. RESTREINT UE/ES RESTRICTED SLAPTUMO ŽYMA PAŽYMĖTA INFORMACIJA

31. Palaikydamas ryšius su valstybės narės NSI/PSI TGS, kaip perkančioji institucija, prireikus turi teisę remiantis sutarties nuostatomis rengti rangovo / subrangovo patalpų patikrinimus, kad įsitikintų, ar įgyvendintos pagal sutartį reikalaujamos tinkamos saugumo priemonės, skirtos apsaugoti RESTREINT UE/ES RESTRICTED slaptumo žyma pažymėtą ESĮI.
32. Kiek būtina pagal nacionalinius įstatymus ir kitus teisės aktus, NSI/PSI ar kitoms kompetentingoms saugumo institucijoms TGS, kaip perkančioji institucija, praneša apie sutartis arba subrangos sutartis, kuriose yra RESTREINT UE/ES RESTRICTED slaptumo žyma pažymėtos informacijos.
33. TGS sudarytų sutarčių, kuriose yra RESTREINT UE/ES RESTRICTED slaptumo žyma pažymėtos informacijos, atveju rangovai ar subrangovai ir jų personalas neprivalo turėti ĮPPP ar APP.
34. TGS, kaip perkančioji institucija, išnagrinėja atsakymus į kvietimus dalyvauti konkurse dėl sutarčių, pagal kurias turi būti suteikta galimybė susipažinti su RESTREINT UE/ES RESTRICTED slaptumo žyma pažymėta informacija, neatsižvelgdama į reikalavimus, susijusius su ĮPPP ar APP, kurie gali būti numatyti nacionaliniuose įstatymuose ir kituose teisės aktuose.
35. Sąlygos, kuriomis rangovas gali sudaryti subrangos sutartis, turi atitikti 21 punkto reikalavimus.
36. Kai pagal sutartį numatytas informacijos, pažymėtos RESTREINT UE/ES RESTRICTED slaptumo žyma, tvarkymas rangovo naudojamoje RIS, TGS, kaip perkančioji institucija, užtikrina, kad sutartyje arba subrangos sutartyje būtų nustatyti su RIS akreditavimu susiję būtini techniniai ir administraciniai reikalavimai, kurie atitiktų įvertintą riziką, atsižvelgiant į visus svarbius veiksnius. Perkančioji institucija ir atitinkama NSI/PSI susitaria dėl tokio RIS akreditavimo masto.

VI PRIEDAS

KEITIMASIS ĮSLAPTINTA INFORMACIJA SU TREČIOSIOMIS VALSTYBĖMIS IR TARPTAUTINĖMIS ORGANIZACIJOMIS

I. ĮVADAS

1. Šiame priede nustatytos 13 straipsnio įgyvendinimo nuostatos.

II. TVARKA, REGLAMENTUOJANTI KEITIMĄSI ĮSLAPTINTA INFORMACIJA

2. Tarybai nustačius, kad yra ilgalaikis poreikis keistis įslaptinta informacija, sudaromas susitarimas dėl informacijos saugumo arba administracinis susitarimas, vadovaujantis 13 straipsnio 2 dalimi ir III bei IV skirsniais bei remiantis Saugumo komiteto rekomendacija.
3. Tais atvejais, kai BSGP operacijos vykdymui surinkta ESĮI gali būti suteikiama tokioje operacijoje dalyvaujančioms trečiosioms valstybėms ar tarptautinėms organizacijoms, ir jeigu nėra nustatyta 2 punkte nurodyta tvarka, keitimasis ESĮI su dalyvaujančiąja trečiąja valstybe arba tarptautine organizacija vadovaujantis V skirsniu reglamentuojamas:

   – susitarimu dėl dalyvavimo bendrųjų sąlygų;

   – *ad hoc* susitarimu dėl dalyvavimo;

   – jeigu nėra sudarytas nė vienas iš pirmiau nurodytų susitarimų, – *ad hoc* administraciniu susitarimu.
4. Jeigu nėra nustatyta 2 ir 3 dalyse nurodyta tvarka ir jeigu priimamas sprendimas vadovaujantis VI skirsniu suteikti ESĮI trečiajai valstybei ar tarptautinei organizacijai išimtine *ad hoc* tvarka, iš atitinkamos trečiosios valstybės ar tarptautinės organizacijos turi būti gautas raštiškas patvirtinimas, kad ji saugos bet kokią jai suteiktą ESĮI laikydamasi šiame sprendime nustatytų pagrindinių principų ir būtiniausių standartų.

III. SUSITARIMAI DĖL INFORMACIJOS SAUGUMO

5. Susitarimais dėl informacijos saugumo nustatomi pagrindiniai principai ir būtiniausi standartai, reglamentuojantys Europos Sąjungos ir trečiosios valstybės ar tarptautinės organizacijos keitimąsi įslaptinta informacija.
6. Susitarimuose dėl informacijos saugumo numatomi techniniai įgyvendinimo susitarimai, dėl kurių turi susitarti atitinkamų Europos Sąjungos institucijų bei įstaigų kompetentingos saugumo tarnybos ir kompetentinga atitinkamos trečiosios valstybės ar tarptautinės organizacijos saugumo institucija. Tokiuose susitarimuose atsižvelgiama į atitinkamoje trečiojoje valstybėje ar tarptautinėje organizacijoje galiojančiais saugumo nuostatais ir esamomis struktūromis bei procedūromis užtikrinamą apsaugos lygį. Šiuos susitarimus patvirtina Saugumo komitetas.
7. Keistis ESĮI elektroninėmis priemonėmis pagal susitarimą dėl informacijos saugumo neleidžiama, jei tai nėra aiškiai numatyta susitarime arba atitinkamuose techniniuose įgyvendinimo susitarimuose.
8. Kai Taryba sudaro susitarimą dėl informacijos saugumo, kiekvienoje šalyje paskiriama po vieną registratūrą, kuri yra pagrindinis įslaptintos informacijos gavimo ir išsiuntimo punktas.
9. Siekiant įvertinti atitinkamos trečiosios valstybės ar tarptautinės organizacijos saugumo nuostatus, struktūras ir procedūras, abipusiu susitarimu su atitinkama trečiąja valstybe ar tarptautine organizacija rengiami įvertinimo vizitai. Tokie įvertinimo vizitai rengiami laikantis atitinkamų III priedo nuostatų ir jų metu įvertinama:

   a) įslaptintai informacijai apsaugoti taikoma reglamentavimo sistema;

   b) bet kurie konkretūs saugumo politikos ypatumai ir saugumo organizavimo tvarka trečiojoje valstybėje arba tarptautinėje organizacijoje, kurie galėtų daryti poveikį įslaptintos informacijos, kuria gali būti keičiamasi, slaptumo žymos laipsniui;

   c) faktiškai taikomos saugumo priemonės ir procedūros;

   d) patikimumo patikrinimo procedūros, susijusios su numatomos suteikti ESĮI slaptumo žymos laipsniu.

10. Europos Sąjungos vardu įvertinimo vizitą atliekanti grupė įvertina, ar atitinkamoje trečiojoje valstybėje arba tarptautinėje organizacijoje saugumo nuostatai ir procedūros yra tinkami, kad būtų apsaugota atitinkamo slaptumo žymos laipsnio ESĮI.
11. Šių vizitų rezultatai pateikiami ataskaitoje, kuria remdamasis Saugumo komitetas nustato, koks gali būti aukščiausias ESĮI, kuria gali būti keičiamasi su atitinkama trečiąja šalimi popieriuje ir prireikus elektroninėmis priemonėmis, slaptumo žymos laipsnis, bei konkrečias sąlygas, reglamentuojančias keitimąsi šia informacija su ta šalimi.
12. Būtina dėti visas pastangas, kad būtų surengtas vizitas į atitinkamą trečiąją valstybę arba tarptautinę organizaciją saugumui visapusiškai įvertinti prieš tai, kai Saugumo komitetas patvirtina įgyvendinamuosius susitarimus, siekiant nustatyti taikomos saugumo sistemos pobūdį ir veiksmingumą. Tačiau jei tai nėra įmanoma, TGS saugumo tarnyba Saugumo komitetui pateikia kuo išsamesnę ataskaitą, pagrįstą turima informacija, informuodama Saugumo komitetą apie taikomus saugumo nuostatus ir saugumo organizavimo tvarką atitinkamoje trečiojoje valstybėje arba tarptautinėje organizacijoje.
13. Atitinkamai trečiajai valstybei ar tarptautinei organizacijai ESĮI faktiškai suteikiama tik po to, kai Saugumo komitetui pateikiama įvertinimo vizito ataskaita arba, jeigu tokios ataskaitos nėra, 12 punkte nurodyta ataskaita ir jis šią ataskaitą teigiamai įvertina.
14. Europos Sąjungos institucijų ir įstaigų kompetentingos saugumo tarnybos trečiajai valstybei ar tarptautinei organizacijai praneša datą, nuo kurios Europos Sąjunga pagal susitarimą gali suteikti ESĮI, taip pat nurodyti, kokio didžiausio slaptumo žymos laipsnio ESĮI gali būti keičiamasi popieriniu pavidalu arba elektroninėmis priemonėmis.
15. Prireikus rengiami tolesni įvertinimo vizitai, visų pirma, tuo atveju, jei:

    a) reikia padidinti ESĮI, kuri gali būti suteikta, slaptumo žymos laipsnį;

    b) Europos Sąjungai buvo pranešta apie esminius saugumo tvarkos trečiojoje valstybėje ar tarptautinėje organizacijoje pokyčius, galinčius turėti poveikį tam, kaip ji saugo ESĮI;

    c) įvyko rimtas incidentas, per kurį buvo neteisėtai atskleista ESĮI.

16. Kai susitarimas dėl informacijos saugumo įsigalioja ir keičiamasi įslaptinta informacija su atitinkama trečiąja valstybe ar tarptautine organizacija, Saugumo komitetas gali nuspręsti pakeisti ESĮI, kuria gali būti keičiamasi popieriniu pavidalu ar elektroninėmis priemonėmis, aukščiausią slaptumo žymos laipsnį, visų pirma, atsižvelgdamas į tolesnių įvertinimo vizitų rezultatus.

IV. ADMINISTRACINIAI SUSITARIMAI

17. Esant ilgalaikiam poreikiui su trečiąja valstybe ar tarptautine organizacija keistis įslaptinta informacija, kurios slaptumo žyma paprastai nėra aukštesnė nei RESTREINT UE/ES RESTRICTED, ir Saugumo komitetui nustačius, kad atitinkama šalis neturi pakankamai išplėtotos tokiai informacijai skirtos saugumo sistemos, kad ta šalis galėtų sudaryti susitarimą dėl informacijos saugumo, Generalinis sekretorius gali, pritarus Tarybai, TGS vardu sudaryti administracinį susitarimą su atitinkamos trečiosios valstybės ar tarptautinės organizacijos atitinkamomis institucijomis.
18. Tais atvejais, kai dėl skubių operatyvinių priežasčių reikia greitai nustatyti keitimosi įslaptinta informacija tvarką, tik Taryba gali nuspręsti, kad būtų sudarytas administracinis susitarimas siekiant keistis aukštesnio slaptumo žymos laipsnio informacija.
19. Administraciniai susitarimai paprastai sudaromi pasikeičiant laiškais.
20. Atitinkamai trečiajai valstybei ar tarptautinei organizacijai ESĮI suteikiama tik po to, kai atliekamas 9 punkte nurodytas įvertinimo vizitas, Saugumo komitetui pateikiama jo ataskaita arba, jeigu tokios ataskaitos nėra, 12 punkte nurodyta ataskaita, ir jis šią ataskaitą teigiamai įvertina.
21. Keistis ESĮI elektroninėmis priemonėmis pagal administracinį susitarimą neleidžiama, jei tai nėra aiškiai numatyta susitarime.

V. KEITIMASIS ĮSLAPTINTA INFORMACIJA VYKDANT BSGP OPERACIJAS

22. Trečiųjų valstybių ar tarptautinių organizacijų dalyvavimą BSGP operacijose reglamentuoja susitarimai dėl dalyvavimo bendrųjų sąlygų. Tokiuose susitarimuose nustatomos nuostatos dėl BSGP operacijų vykdymui surinktos ESĮI suteikimo jose dalyvaujančiosioms trečiosioms valstybėms ar tarptautinėms organizacijoms. Aukščiausias ESĮI, kuria gali būti keičiamasi, slaptumo žymos laipsnis yra RESTREINT UE/ES RESTRICTED BSGP civilinėms operacijoms ir CONFIDENTIEL UE/ES CONFIDENTIAL BSGP karinėms operacijoms, išskyrus atvejus, kai nustatyta kitaip sprendime, kuriuo įsteigiama kiekviena BSGP operacija.
23. *Ad hoc* susitarimuose dėl dalyvavimo, sudarytuose dėl konkrečios BSGP operacijos, nustatomos nuostatos dėl tos operacijos vykdymui surinktos ESĮI suteikimo joje dalyvaujančiajai trečiajai valstybei ar tarptautinei organizacijai. Aukščiausias ESĮI, kuria gali būti keičiamasi, slaptumo žymos laipsnis yra RESTREINT UE/ES RESTRICTED BSGP civilinėms operacijoms ir CONFIDENTIEL UE/ES CONFIDENTIAL BSGP karinėms operacijoms, išskyrus atvejus, kai nustatyta kitaip sprendime, kuriuo įsteigiama kiekviena BSGP operacija.
24. Jeigu nėra susitarimo dėl informacijos saugumo, kol nesudarytas susitarimas dėl dalyvavimo, operacijos tikslais parengtos ESĮI suteikimas operacijoje dalyvaujančiai trečiajai valstybei arba tarptautinei organizacijai reglamentuojamas vyriausiojo įgaliotinio sudarytu administraciniu susitarimu arba jam taikomas sprendimas dėl informacijos suteikimo *ad hoc* tvarka pagal VI skirsnį. Pagal tokį susitarimą ESĮI keičiamasi tik tol, kol vis dar planuojamas trečiosios valstybės arba tarptautinės organizacijos dalyvavimas. Aukščiausias ESĮI, kuria gali būti keičiamasi, slaptumo žymos laipsnis yra RESTREINT UE/ES RESTRICTED BSGP civilinėms operacijoms ir CONFIDENTIEL UE/ES CONFIDENTIAL BSGP karinėms operacijoms, išskyrus atvejus, kai nustatyta kitaip sprendime, kuriuo įsteigiama kiekviena BSGP operacija.

25. Nuostatose dėl įslaptintos informacijos, kurios turi būti įtrauktos į susitarimus dėl dalyvavimo bendrųjų sąlygų ir į 22–24 punktuose nurodytus *ad hoc* administracinius susitarimus, nustatoma, kad atitinkama trečioji valstybė ar tarptautinė organizacija užtikrina, kad jos personalas, komandiruotas į bet kokią operaciją, saugos ESĮI pagal Tarybos saugumo taisykles ir vadovaudamasis tolesniais kompetentingų institucijų, įskaitant operacijos vadovavimo grandinės pareigūnus, pateiktais nurodymais.
26. Jeigu vėliau sudaromas Europos Sąjungos ir dalyvaujančiosios trečiosios valstybės ar tarptautinės organizacijos susitarimas dėl informacijos saugumo, šio susitarimo dėl informacijos saugumo nuostatos yra viršesnės už bet kokiuose susitarimuose dėl dalyvavimo bendrųjų sąlygų, *ad hoc* susitarimuose dėl dalyvavimo arba *ad hoc* administraciniuose susitarimuose išdėstytas nuostatas dėl keitimosi įslaptinta informacija, kiek tai susiję su keitimusi ESĮI ir jos apdorojimu.
27. Keistis ESĮI elektroninėmis priemonėmis pagal susitarimą dėl dalyvavimo bendrųjų sąlygų, *ad hoc* susitarimą dėl dalyvavimo ar *ad hoc* administracinį susitarimą su trečiąja valstybe ar tarptautine organizacija neleidžiama, jei tai nėra aiškiai numatyta atitinkamame susitarime arba administraciniame susitarime.
28. BSGP operacijos vykdymui surinkta ESĮI gali būti suteikiama trečiųjų valstybių ar tarptautinių organizacijų į tą operaciją komandiruotam personalui, vadovaujantis 22–27 punktų nuostatomis. Kai tokiam personalui leidžiama susipažinti su ESĮI BSGP operacijos patalpose ar RIS, turi būti imamasi priemonių (įskaitant suteiktos ESĮI registravimą), kad būtų sumažinta rizika, jog informacija bus prarasta ar atskleista. Tokios priemonės nurodomos atitinkamuose planavimo ar misijos dokumentuose.
29. Jeigu nėra susitarimo dėl informacijos saugumo, ESĮI suteikimas priimančiajai valstybei, kurios teritorijoje vykdoma BSGP operacija, konkretaus ir neatidėliotino operatyvinio poreikio atveju gali būti reglamentuojamas vyriausiojo įgaliotinio sudarytu administraciniu susitarimu. Ši galimybė numatoma sprendime, kuriuo įsteigiama BSGP operacija. Tokiomis aplinkybėmis suteikiama tik ta ESĮI, kuri buvo surinkta BSGP operacijai vykdyti ir kurios slaptumo žymos laipsnis nėra aukštesnis nei RESTREINT UE/ES RESTRICTED, nebent Sprendime dėl BSGP operacijos įsteigimo yra nurodytas aukštesnis slaptumo žymos laipsnis. Pagal tokį administracinį susitarimą

priimančioji valstybė privalo įsipareigoti saugoti ESĮI laikydamasi būtiniausių standartų, kurie turi būti ne mažiau griežti nei nustatytieji šiame sprendime.

30. Jeigu nėra susitarimo dėl informacijos saugumo, ESĮI suteikimas atitinkamoms trečiosioms valstybėms ir tarptautinėms organizacijoms, išskyrus dalyvaujančias BSGP operacijoje, gali būti reglamentuojamas vyriausiojo įgaliotinio sudarytu administraciniu susitarimu. Atitinkamais atvejais ši galimybė ir jai taikomos sąlygos numatomos sprendime, kuriuo įsteigiama BSGP operacija. Tokiomis aplinkybėmis suteikiama tik ta ESĮI, kuri buvo surinkta BSGP operacijai vykdyti ir kurios slaptumo žymos laipsnis nėra aukštesnis nei RESTREINT UE/ES RESTRICTED, nebent Sprendime dėl BSGP operacijos įsteigimo yra nurodytas aukštesnis slaptumo žymos laipsnis. Pagal tokį administracinį susitarimą atitinkama trečioji valstybė arba tarptautinė organizacija privalo įsipareigoti saugoti ESĮI laikydamasi būtiniausių standartų, kurie turi būti ne mažiau griežti nei nustatytieji šiame sprendime.

31. Prieš įgyvendinant nuostatas dėl ESĮI suteikimo pagal 22, 23 ir 24 punktus, nėra būtina sudaryti įgyvendinimo susitarimus ar rengti įvertinimo vizitus.

VI. ESĮI *AD HOC* SUTEIKIMAS IŠIMTINE TVARKA

32. Jei nėra nustatyta galiojančios tvarkos pagal III–V skirsnius ir Tarybai ar vienam iš jos parengiamųjų organų nusprendus, kad išimtiniu atveju reikia suteikti ESĮI trečiajai valstybei ar tarptautinei organizacijai, TGS:

a) kiek įmanoma, patikrina atitinkamas trečiosios valstybės ar tarptautinės organizacijos saugumo institucijas, ar jų saugumo nuostatai, struktūros bei procedūros yra pakankami, kad užtikrintų, jog joms suteikta ESĮI būtų apsaugota pagal ne mažiau griežtus standartus nei yra nustatyti šiame sprendime;

b) kartu prašo Saugumo komiteto, kad remdamasis turima informacija pateiktų rekomendaciją, kiek galima pasitikėti atitinkamos trečiosios valstybės ar tarptautinės organizacijos, kuriai bus suteikta ESĮI, saugumo nuostatais, struktūromis bei procedūromis.

33. Jeigu Saugumo komitetas pateikia rekomendaciją, kuria pritaria ESĮI suteikimui, klausimas perduodamas Nuolatinių atstovų komitetui (COREPER), kuris priima sprendimą dėl šios ESĮI suteikimo.
34. Jeigu Saugumo komiteto rekomendacijoje nepritariama ESĮI suteikimui:

    a) su BUSP/BSGP susijusiose srityse Politinis ir saugumo komitetas aptaria šį klausimą ir suformuluoja rekomendaciją dėl Nuolatinių atstovų komiteto sprendimo;

    b) visose kitose srityse Nuolatinių atstovų komitetas aptarią šį klausimą ir priima sprendimą.
35. Jei manoma, kad tikslinga, ir iš anksto gavus rašytinį įslaptintos informacijos rengėjo sutikimą, Nuolatinių atstovų komitetas gali nuspręsti, kad įslaptinta informacija gali būti suteikta tik iš dalies ir tik tuo atveju, jei prieš tai jos slaptumo žymos laipsnis sumažinamas arba ji išslaptinama arba kad informacija, kurią suteikti numatyta, turi būti parengta nenurodant šaltinio ar pirminio ES slaptumo žymos laipsnio.
36. Priėmus sprendimą suteikti ESĮI, TGS perduoda atitinkamą dokumentą, pažymėtą leidimo suteikti informaciją žyma, nurodant trečiąją valstybę ar tarptautinę organizaciją, kuriai ji buvo suteikta. Prieš suteikiant tokią informaciją arba faktinio jos suteikimo metu atitinkama trečioji šalis raštu įsipareigoja apsaugoti ESĮI, kurią ji gauna, pagal šiame sprendime nustatytus pagrindinius principus ir būtiniausius standartus.

VII. LEIDIMAS SUTEIKTI ESĮI TREČIOSIOMS VALSTYBĖMS ARBA TARPTAUTINĖMS ORGANIZACIJOMS

37. Kai yra nustatyta 2 punkte nurodyta tvarka, reglamentuojanti keitimąsi įslaptinta informacija su trečiąja valstybe ar tarptautine organizacija, Taryba priima sprendimą suteikti leidimą Generaliniam sekretoriui suteikti ESĮI atitinkamai trečiajai valstybei ar tarptautinei organizacijai, laikantis principo, kad su tuo turi sutikti įslaptintos informacijos rengėjas. Generalinis sekretorius gali perduoti šią teisę vyresniesiems TGS pareigūnams.

38. Jei yra sudarytas 2 punkto pirmoje įtraukoje nurodytas susitarimas dėl informacijos saugumo, Taryba gali priimti sprendimą suteikti leidimą vyriausiajam įgaliotiniui Taryboje parengtą bendros saugumo ir gynybos politikos srities ESĮI, gavus joje esančios pradinės medžiagos rengėjo sutikimą, suteikti atitinkamai trečiajai valstybei arba tarptautinei organizacijai. Vyriausiasis įgaliotinis gali perduoti šį leidimą vyresniesiems EIVT pareigūnams arba ES specialiesiems įgaliotiniams.
39. Kai yra nustatyta 2 arba 3 punkte nurodyta tvarka, reglamentuojanti keitimąsi įslaptinta informacija su trečiąja valstybe ar tarptautine organizacija, vyriausiajam įgaliotiniui suteikiamas leidimas suteikti ESĮI, vadovaujantis tuo sprendimu, kuriuo įsteigiama BSGP operacija, ir laikantis principo, kad su tuo turi sutikti įslaptintos informacijos rengėjas. Vyriausiasis įgaliotinis gali perduoti šį leidimą vyresniesiems EIVT pareigūnams, ES operacijų, pajėgų ar misijų vadams arba ES misijų vadovams.

Priedėliai

A Priedėlis

Apibrėžtys

B Priedėlis

Slaptumo žymų atitikmenys

C Priedėlis

Nacionalinių saugumo institucijų (NSI) sąrašas

D Priedėlis

Santrumpų sąrašas

A priedėlis

APIBRĖŽTYS

Šiame sprendime vartojamos tokios sąvokų apibrėžtys:

Akreditavimas – procesas, po kurio Saugumo akreditavimo institucija (SAI) pateikia oficialų pareiškimą, patvirtinantį, kad sistemai yra leista veikti taikant nustatytą slaptumo žymos laipsnį konkrečiu slaptumo režimu jos operacinėje aplinkoje ir priimtinu rizikos lygiu, laikantis prielaidos, kad įgyvendintas patvirtintas techninių, fizinių, organizacinių ir procedūrinių saugumo priemonių rinkinys;

Turtas – viskas, kas turi tam tikrą vertę organizacijai, jos veiklos operacijoms bei jų tęstinumui, įskaitant informacijos išteklius, padedančius vykdyti organizacijos misiją;

Leidimas susipažinti su ESĮI – remiantis valstybės narės kompetentingos institucijos patvirtinimu priimtas TGS paskyrimų tarnybos sprendimas, kad TGS pareigūnui, kitam tarnautojui arba komandiruotam nacionaliniam ekspertui gali būti leidžiama susipažinti su iki tam tikro laipsnio slaptumo žyma (CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma) pažymėta ESĮI iki nustatytos datos, jei nustatyta, kad asmuo atitinka principą „būtina žinoti“ ir jis buvo tinkamai informuotas apie savo atsakomybę;

RIS gyvavimo ciklas – visa RIS egzistavimo trukmė, įskaitant inicijavimą, koncepciją, planavimą, reikalavimų analizę, projektavimą, sukūrimą, bandymą, įdiegimą, veikimą ir priežiūrą bei naudojimo nutraukimą;

Įslaptinta sutartis – TGS ir rangovo sudaryta prekių tiekimo, darbų vykdymo arba paslaugų teikimo sutartis, kurią vykdant reikia susipažinti su ESĮI ar ją rengti arba suteikiama galimybė su ja susipažinti ar ją rengti;

Įslaptinta subrangos sutartis – TGS rangovo ir kito rangovo (t. y. subrangovo) sudaryta prekių tiekimo, darbų vykdymo arba paslaugų teikimo sutartis, kurią vykdant reikia susipažinti su ESĮI ar ją rengti arba suteikiama galimybė su ja susipažinti ar ją rengti;

Ryšių ir informacinė sistema (RIS) – žr. 10 straipsnio 2 dalį;

Rangovas – fizinis arba juridinis asmuo, turintis teisnumą ir veiksnumą sudaryti sutartis;

Šifravimo priemonės – šifravimo algoritmai, šifravimo techninės ir

programinės įrangos moduliai, priemonės, apimančios vykdymo informaciją bei susijusius dokumentus ir raktų duomenis;

šifravimo priemonė – priemonė, kurios pradinė ir pagrindinė paskirtis yra susijusių saugumo funkcijų (konfidencialumo, vientisumo, prieinamumo, autentiškumo, atsakomybės už veiksmus prisiėmimo) užtikrinimas taikant vieną ar kelis šifravimo metodus;

BSGP operacija – karinio ar civilinio krizių valdymo operacija vadovaujantis ES sutarties V antraštinės dalies 2 skyriumi;

Išslaptinimas – bet kokios slaptumo žymos panaikinimas;

Nuodugni apsauga – saugumo priemonių, kurios grupuojamos į kelis apsaugos lygius, taikymas;

Paskirtoji saugumo institucija (PSI) – valstybės narės nacionalinei saugumo institucijai (NSI) atsakinga institucija, kuri atsako už pramonės ir kitų subjektų informavimą apie nacionalinę politiką visais pramoninio saugumo klausimais ir duoda nurodymus bei padeda ją įgyvendinti. PSI funkciją gali vykdyti NSI arba kita kompetentinga institucija;

Dokumentas – fiksuota informacija, neatsižvelgiant į jos fizinę formą ar charakteristikas;

Slaptumo žymos laipsnio sumažinimas – slaptumo žymos lygio sumažinimas;

ES įslaptinta informacija (ESĮI) – žr. 2 straipsnio 1 dalį;

Įmonės patikimumą patvirtinantis pažymėjimas (ĮPPP) – NSI ar PSI administracinis patvirtinimas, kad saugumo požiūriu patalpose gali būti užtikrinta nurodyto slaptumo žymos laipsnio ESĮI tinkamo lygio apsauga;

ESĮI administravimas – visi galimi veiksmai, kurie gali būti atliekami su ESĮI per visą jos gyvavimo ciklą. Tai apima ESĮI parengimą, apdorojimą, gabenimą, slaptumo žymos laipsnio sumažinimą, išslaptinimą ir sunaikinimą. RIS atžvilgiu tai taip pat apima ESĮI rinkimą, skelbimą, perdavimą ir saugojimą;

Turėtojas – tinkamą leidimą turintis asmuo, kuris atitinka principą „būtina žinoti“ ir turi ESĮI dalį bei yra atitinkamai atsakingas už jos apsaugą;

Pramonės arba kitas subjektas – subjektas, tiekiantis prekes, vykdantis darbus arba teikiantis paslaugas; tai gali būti pramonės, prekybos, paslaugų, mokslo, mokslinių tyrimų, švietimo ar vystymo subjektas arba savarankiškai dirbantis asmuo;

Pramoninis saugumas – žr. 11 straipsnio 1 dalį;

Informacijos saugumo užtikrinimas – žr. 10 straipsnio 1 dalį;

Tarpusavio sujungimas – žr. IV priedo 32 punktą;

Įslaptintos informacijos administravimas – žr. 9 straipsnio 1 dalį;

Medžiaga – dokumentas, duomenų laikmena arba bet kokie pagaminti ar gaminami įrenginiai ar įranga;

Rengėjas – Europos Sąjungos institucija, įstaiga ar agentūra, valstybė narė, trečioji valstybė ar tarptautinė organizacija, kurios atsakomybe įslaptinta informacija buvo parengta ir (arba) pateikta naudoti Europos Sąjungos struktūrose;

Personalo patikimumas – žr. 7 straipsnio 1 dalį;

Asmens patikimumo pažymėjimas (APP) – valstybės narės kompetentingos institucijos pažyma, išduota valstybės narės kompetentingoms institucijoms užbaigus patikimumo tikrinimo procedūras ir patvirtinanti, kad asmeniui gali būti leidžiama susipažinti su iki tam tikro laipsnio slaptumo žyma (CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma) pažymėta ESĮI iki nustatytos datos;

Asmens patikimumo pažymėjimą patvirtinanti pažyma (APPPP) – kompetentingos institucijos išduota pažyma, kurioje nurodoma, kad asmens patikimumas yra patikrintas ir kad jis turi galiojantį patikimumo pažymėjimą arba paskyrimų tarnybos leidimą susipažinti su ESĮI, ir nurodomas ESĮI, su kuria tam asmeniui gali būti leista susipažinti, slaptumo žymos laipsnis (CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma), atitinkamo APP galiojimo laikas ir pačios pažymos galiojimo laikas;

Fizinis saugumas – žr. 8 straipsnio 1 dalį;

Programos / projekto saugumo instrukcijos (PRSI) – saugumo procedūrų, kurios yra taikomos konkrečiai programai / projektui siekiant standartizuoti saugumo procedūras, sąrašas. Jos gali būti tikslinamos įgyvendinant programą / projektą;

Registravimas – žr. III priedo 18 punktą;

Likutinė rizika – rizika, kuri lieka po to, kai buvo įgyvendintos saugumo priemonės, atsižvelgiant į tai, kad ne nuo visų grėsmių apsisaugoma ir ne visi pažeidžiamumo aspektai gali būti pašalinti;

Rizika – galimybė, kad tam tikros grėsmės atveju bus pasinaudota organizacijos ar sistemų vidiniu ir išoriniu pažeidžiamumu ir taip bus padaryta žala organizacijai ir jos materialiajam ar nematerialiajam turtui.

Ji įvertinama atsižvelgiant į kylančios grėsmės tikimybę ir į jos poveikį:

– **rizikos pripažinimas** – sprendimas atlikus rizikos tvarkymą pripažinti, kad vis dar yra likutinė rizika;

– **rizikos įvertinimas** – grėsmių ir pažeidžiamų sričių nustatymas bei susijusios rizikos analizės, t. y. galimumo ir poveikio analizės, atlikimas;

– **informavimas apie riziką** – RIS vartotojų bendruomenės informuotumo apie riziką didinimas, patvirtinimo institucijų informavimas apie tokią riziką ir pranešimų vykdančiosioms institucijoms teikimas;

– **rizikos tvarkymas** – rizikos silpninimas, šalinimas, mažinimas (taikant tinkamas technines, fizines, valdymo ar procedūrines priemones), perkėlimas arba stebėsena;

Saugumo aspektų paaiškinimas (SAP) – specialių sutartinių sąlygų rinkinys, kurį parengia perkančioji institucija ir kuris yra įslaptintos sutarties, pagal kurią gali būti susipažįstama su ESĮI arba tokia informacija gali būti rengiama, sudėtinė dalis – jame nurodomi saugumo reikalavimai arba sutarties dalys, kurių saugumą būtina užtikrinti;

Slaptumo žymų vadovas (SŽV) – dokumentas, kuriame aprašomi programos arba sutarties įslaptintos dalys, nurodant taikomus slaptumo žymų laipsnius. SŽV gali būti papildomas programos arba sutarties vykdymo laikotarpiu, o informacijos dalims gali būti suteiktos naujos slaptumo žymos arba jų slaptumo žymos laipsnis gali būti sumažintas; tais atvejais, kai yra parengtas SŽV, jis yra SAP dalis;

Patikimumo tikrinimas – tikrinimo procedūros, kurias, vadovaudamasi valstybėje narėje galiojančiais įstatymais ir kitais teisės aktais, atlieka kompetentinga institucija, siekdama gauti užtikrinimą, kad nėra jokios nepalankios informacijos, kuri neleistų asmeniui išduoti asmens patikimumo pažymėjimo arba leidimo, suteikiančio galimybę susipažinti su tam tikro lygio ESĮI (CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta informacija);

Darbo saugumo režimas – sąlygų, kuriomis veikia RIS, apibrėžtis, pagrįsta apdorojamos informacijos slaptumo žyma ir patikimumo laipsniais, oficialiais prieigos patvirtinimais ir naudotojams taikomu principu „būtina žinoti“. Įslaptintos informacijos apdorojimui arba perdavimui gali būti taikomi keturi darbo režimai: skirtinis režimas, aukšto lygio sistemos režimas, patalpų atskyrimo pertvaromis režimas ir daugialaipsnis režimas:

– **skirtinis režimas** – toks darbo režimas, kai visi galintys naudotis RIS asmenys turi leidimą naudotis RIS tvarkoma aukščiausio slaptumo

žymos laipsnio informacija ir pagal bendrą principą „būtina žinoti“ turi susipažinti su visa RIS tvarkoma informacija;

– **aukšto lygio sistemos režimas** – toks darbo režimas, kai visi galintys naudotis RIS asmenys turi leidimą naudotis RIS tvarkoma aukščiausio slaptumo žymos laipsnio informacija, tačiau ne visi galintys naudotis RIS asmenys turi pagal bendrą principą „būtina žinoti“ susipažinti su RIS tvarkoma informacija; patvirtinimas apie teisės susipažinti su informacija suteikimą gali būti išduodamas asmens;

– **patalpų atskyrimo pertvaromis režimas** – toks darbo režimas, kai visi galintys naudotis RIS asmenys turi leidimą naudotis RIS tvarkoma aukščiausio slaptumo žymos laipsnio informacija, tačiau ne visi galintys naudotis RIS asmenys turi oficialų leidimą susipažinti su visa RIS tvarkoma informacija; oficialus leidimas reiškia oficialų patekimo į objektą centrinį valdymą, kuris yra atskirtas nuo leidimo asmeniui savo nuožiūra suteikti prieigą;

– **daugialaipsnis režimas** – toks darbo režimas, kai ne visi galintys naudotis RIS asmenys turi leidimą naudotis RIS tvarkoma aukščiausio slaptumo žymos laipsnio informacija ir ne visi galintys naudotis RIS asmenys turi pagal bendrą principą „būtina žinoti“ susipažinti su RIS tvarkoma informacija;

Saugumo rizikos valdymo procesas – visas nebūtinai galinčių įvykti atvejų, kurie gali paveikti organizacijos arba jos naudojamų sistemų saugumą, nustatymo, kontrolės ir mažinimo procesas. Jis apima visą su rizika susijusią veiklą, įskaitant jos įvertinimą, tvarkymą, pripažinimą ir informavimą apie ją;

TEMPEST – elektromagnetinio spinduliavimo, dėl kurio neteisėtai atskleidžiama informacija, tikrinimas, tyrimas bei kontrolė ir jo šalinimo priemonės;

Grėsmė – galimas nepageidaujamas atvejis, dėl kurio gali būti padaryta žala organizacijai ar jos naudojamoms sistemoms; tokios grėsmės gali būti atsitiktinės arba tyčinės (piktybinės); jas apibūdina pavojingi elementai, galimi taikiniai ir puolimo būdai;

Pažeidžiamumas – bet kokio pobūdžio silpnumas, kuriuo gali būti naudojamasi vienos ar daugiau grėsmių atveju. Pažeidžiamumas gali atsirasti dėl neveikimo arba gali būti susijęs su kontrolės stiprumo, išsamumo ar nuoseklumo trūkumu ir gali būti techninio, procedūrinio, fizinio, organizacinio ar veiklos pobūdžio.

B priedėlis

SLAPTUMO ŽYMŲ ATITIKMENYS

ES	TRÈS SECRET UE/ ES TOP SECRET	SECRET UE/ES SECRET	CONFIDENTIEL UE/ES CONFIDENTIAL	RESTREINT UE/ES RESTRICTED
Belgija	Très Secret (Loi 11.12.1998) Zeer Geheim (Wet 11.12.1998)	Secret (Loi 11.12.1998) Geheim (Wet 11.12.1998)	Confidentiel (Loi 11.12.1998) Vertrouwelijk (Wet 11.12.1998)	([1]) pastaba
Bulgarija	Строго секретно	Секретно	Поверително	За служебно ползване
Čekija	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Danija	YDERST HEMMELIGT	HEMMELIGT	FORTROLIGT	TIL TJENESTEBRUG
Vokietija	STRENG GEHEIM	GEHEIM	VS ([2])– VERTRAULICH	VS – NUR FÜR DEN DIENSTGEBRAUCH
Estija	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Airija	Top Secret	Secret	Confidential	Restricted
Graikija	Άκρως Απόρρητο Abr: ΑΑΠ	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Ispanija	SECRETO	RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
Prancūzija	Très Secret Défense	Secret Défense	Confidentiel Défense	([3]) pastaba
Kroatija	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Italija	Segretissimo	Segreto	Riservatissimo	Riservato
Kipras	Άκρως Απόρρητο Abr: (ΑΑΠ)	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Latvija	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Lietuva	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Liuksemburgas	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux

Vengrija	Szigorúan titkos!	Titkos!	Bizalmas!	Korlátozott terjesztésű!
Malta	L-Ogħla Segretezza Top Secret	Sigriet Secret	Kunfidenzjali Confidential	Ristrett Restricted ([4])
Nyderlandai	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Austrija	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Lenkija	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugalija	Muito Secreto	Secreto	Confidencial	Reservado
Rumunija	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu
Slovėnija	STROGO TAJNO	TAJNO	ZAUPNO	INTERNO
Slovakija	Prísne tajné	Tajné	Dôverné	Vyhradené
Suomija	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Švedija ([5])	HEMLIG/TOP SECRET HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG/ SECRET HEMLIG	HEMLIG/CONFIDENTIAL HEMLIG	HEMLIG/RESTRICTED HEMLIG
Jungtinė Karalystė	UK TOP SECRET	UK SECRET	UK CONFIDENTIAL	UK RESTRICTED

([1]) Diffusion Restreinte/Beperkte Verspreiding nėra slaptumo žyma Belgijoje. Žyma RESTREINT UE/ES RESTRICTED pažymėtą informaciją Belgija tvarko ir saugo taip pat griežtai, kaip taikant nustatytus Europos Sąjungos Tarybos saugumo taisyklėse aprašytus standartus ir procedūras.

([2]) Vokietija: VS = Verschlusssache.

([3]) Prancūzijos nacionalinėje sistemoje slaptumo žyma RESTREINT nenaudojama. Žyma RESTREINT UE/ES RESTRICTED pažymėtą informaciją Prancūzija tvarko ir saugo taip pat griežtai, kaip taikant nustatytus Europos Sąjungos Tarybos saugumo taisyklėse aprašytus standartus ir procedūras.

([4]) Maltoje gali būti naudojamos žymos tiek maltiečių, tiek anglų kalba.

([5]) Švedija: viršutinėje eilutėje nurodytas slaptumo žymas naudoja gynybos institucijos, o nurodytas apatinėje eilutėje – kitos institucijos.

C priedėlis

NACIONALINIŲ SAUGUMO INSTITUCIJŲ (NSI) SĄRAŠAS

BELGIJA Autorité nationale de Sécurité SPF Affaires étrangères, Commerce extérieur et Coopération au Développement 15, rue des Petits Carmes 1000 Bruxelles Sekretoriato tel. +32 25014542 Faks. +32 25014596 El. p. nvo-ans@diplobel.fed.be	**ESTIJA** National Security Authority Department Estonian Ministry of Defence Sakala 1 15094 Tallinn Tel.: +372 7170019, +372 7170117 Faks. +372 7170213 El. p. nsa@mod.gov.ee
BULGARIJA State Commission on Information Security 90 Cherkovna Str. 1505 Sofia Tel. +359 29333600 Faks. +359 29873750 El. p. dksi@government.bg Interneto svetainė www.dksi.bg	**AIRIJA** National Security Authority Department of Foreign Affairs 76–78 Harcourt Street Dublin 2 Tel. +353 14780822 Faks. +353 14082959
ČEKIJA Národní bezpečnostní úřad (National Security Authority) Na Popelce 2/16 150 06 Praha 56 Tel. +420 257283335 Faks. +420 257283110 El. p. czech.nsa@nbu.cz Interneto svetainė www.nbu.cz	**GRAIKIJA** Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ) Διεύθυνση Ασφαλείας και Αντιπληροφοριών ΣΤΓ 1020 -Χολαργός (Αθήνα) Ελλάδα Τηλ.: +30 2106572045 (ώρες γραφείου) +30 2106572009 (ώρες γραφείου) Φαξ: +30 2106536279 +30 2106577612 Hellenic National Defence General Staff (HNDGS) Counter Intelligence and Security Directorate (NSA) 227–231 HOLARGOS STG 1020 ATHENS Tel.: +30 2106572045 +30 2106572009 Faks.: +30 2106536279 +30 2106577612

DANIJA Politiets Efterretningstjeneste (Danish Security Intelligence Service) Klausdalsbrovej 1 2860 Søborg Tel. +45 33148888 Faks. +45 33430190 Forsvarets Efterretningstjeneste (Danish Defence Intelligence Service) Kastellet 30 2100 Copenhagen Ø Tel. +45 33325566 Faks. +45 33931320	**ISPANIJA** Autoridad Nacional de Seguridad Oficina Nacional de Seguridad Avenida Padre Huidobro s/n 28023 Madrid Tel. +34 913725000 Faks. +34 913725808 El. p. nsa-sp@areatec.com
VOKIETIJA Bundesministerium des Innern Referat ÖS III 3 Alt-Moabit 101 D D-11014 Berlin Tel. +49 30186810 Faks. +49 30186811441 El. p. oesIII3@bmi.bund.de	**PRANCŪZIJA** Secrétariat général de la défense et de la sécurité nationale Sous-direction Protection du secret (SGDSN/PSD) 51 Boulevard de la Tour-Maubourg 75700 Paris 07 SP Tel. +33 171758177 Faks. +33 171758200
KROATIJA Office of the National Security Council Croatian NSA Jurjevska 34 10000 Zagreb Croatia Tel. +385 14681222 Faks. +385 14686049 www.uvns.hr	**LIUKSEMBURGAS** Autorité nationale de Sécurité Boîte postale 2379 1023 Luxembourg Tel.: +352 24782210 (centrinis) +352 24782253 (tiesioginis) Faks. +352 24782243
ITALIJA Presidenza del Consiglio dei Ministri D.I.S. - U.C.Se. Via di Santa Susanna, 15 00187 Roma Tel. +39 0661174266 Faks. +39 064885273	**VENGRIJA** Nemzeti Biztonsági Felügyelet (National Security Authority of Hungary) H-1024 Budapest, Szilágyi Erzsébet fasor 11/B Tel. +36 (1) 7952303 Faks. +36 (1) 7950344 Pašto adresas H-1357 Budapest, PO Box 2 El. p. nbf@nbf.hu Interneto svetainė www.nbf.hu

KIPRAS ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ Εθνική Αρχή Ασφάλειας (ΕΑΑ) Υπουργείο Άμυνας Λεωφόρος Εμμανουήλ Ροΐδη 4 1432 Λευκωσία, Κύπρος Τηλέφωνα: +357 22807569, +357 22807643, +357 22807764 Τηλεομοιότυπο: +357 22302351 Ministry of Defence Minister's Military Staff National Security Authority (NSA) 4 Emanuel Roidi street 1432 Nicosia Tel.: +357 22807569, +357 22807643, +357 22807764 Faks. +357 22302351 El. p. cynsa@mod.gov.cy	**MALTA** Ministry for Home Affairs and National Security P.O. Box 146 MT-Valletta Tel. +356 21249844 Faks. +356 25695321
LATVIJA National Security Authority Constitution Protection Bureau of the Republic of Latvia P.O.Box 286 LV-1001 Riga Tel. +371 67025418 Faks. +371 67025454 El. p. ndi@sab.gov.lv	**NYDERLANDAI** Ministerie van Binnenlandse Zaken en Koninkrijksrelaties Postbus 20010 2500 EA Den Haag Tel. +31 703204400 Faks. +31 703200733 Ministerie van Defensie Beveiligingsautoriteit Postbus 20701 2500 ES Den Haag Tel. +31 703187060 Faks. +31 703187522
LIETUVA Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija (The Commission for Secrets Protection Coordination of the Republic of Lithuania National Security Authority) Gedimino 40/1 LT-01110 Vilnius Tel.: +370 70666701, +370 70666702 Faks. +370 70666700 El. p. nsa@vsd.lt	**AUSTRIJA** Informationssicherheitskommission Bundeskanzleramt Ballhausplatz 2 1014 Wien Tel. +43 1531152594 Faks. +43 1531152615 El. p. ISK@bka.gv.at

LENKIJA Agencja Bezpieczeństwa Wewnętrznego – ABW (Internal Security Agency) 2A Rakowiecka St. 00–993 Warszawa Tel. +48 225857360 Faks. +48 225858509 El. p. nsa@abw.gov.pl Interneto svetainė www.abw.gov.pl	**SLOVAKIJA** Národný bezpečnostný úrad (National Security Authority) Budatínska 30 P.O. Box 16 850 07 Bratislava Tel. +421 268692314 Faks. +421 263824005 Interneto svetainė: www.nbusr.sk
PORTUGALIJA Presidência do Conselho de Ministros Autoridade Nacional de Segurança Rua da Junqueira, 69 1300–342 Lisboa Tel. +351 213031710 Faks. +351 213031711	**SUOMIJA** National Security Authority Ministry for Foreign Affairs P.O. Box 453 FI-00023 Government 1 Tel. +358 16055890 Faks. +358 916055140 El. p. NSA@formin.fi
RUMUNIJA Oficiul Registrului Național al Informațiilor Secrete de Stat (Romanian NSA – ORNISS National Registry Office for Classified Information) Strada Mureș nr. 4012275 Bucharest Tel. +40 212245830 Faks. +40 212240714 El. p. nsa.romania@nsa.ro Interneto svetainė www.orniss.ro	**ŠVEDIJA** Utrikesdepartementet (Ministry for Foreign Affairs) UD-RS S-103 39 Stockholm Tel. +46 84051000 Faks. +46 87231176 El. p. ud-nsa@foreign.ministry.se
SLOVĖNIJA Urad Vlade RS za varovanje tajnih podatkov Gregorčičeva 27 1000 Ljubljana Tel. +386 14781390 Faks. +386 14781399 El. p. gp.uvtp@gov.si	**JUNGTINĖ KARALYSTĖ** UK National Security Authority Room 335, 3rd Floor 70 Whitehall London SW1A 2AS Tel.: +44 2072765645, +44 2072765497 Faks. +44 2072765651 El. p. UK-NSA@cabinet-office.x.gsi.gov.uk

D priedėlis

SANTRUMPŲ SĄRAŠAS

Santrumpa	Reikšmė
APP	Asmens patikimumo pažymėjimas
APPP	Asmens patikimumo pažymėjimą patvirtinanti pažyma
AVSS	Apsauginės vaizdo stebėjimo sistemos
BSGP	Bendra saugumo ir gynybos politika
BUSP	Bendra užsienio ir saugumo politika
COREPER	Nuolatinių atstovų komitetas
EKSD	Europos Komisijos saugumo direktoratas
ESĮI	ES įslaptinta informacija
ESSĮ	ES specialusis įgaliotinis
ĮAS	Įsibrovimo aptikimo sistema
ĮPPP	Įmonės patikimumą patvirtinantis pažymėjimas
ISU	Informacijos saugumo užtikrinimas
ISUI	Informacijos saugumo užtikrinimo institucija
IT	Informacinė technologija
KPI	Kriptografijos patvirtinimo institucija
KPLI	Kriptografijos platinimo institucija
NSI	Nacionalinė saugumo institucija
PRSI	Programos / projekto saugumo instrukcijos
PSI	Paskirtoji saugumo institucija
RAP	Ribų apsaugos priemonė
RIS	Ryšių ir informacinės sistemos, kuriose tvarkoma ESĮI
SAI	Saugumo akreditavimo institucija
SAP	Saugumo aspektų paaiškinimai
SAV	Saugumo akreditavimo valdyba
SecOPs	Saugumo įgyvendinimo patikrinimo dokumentai ir saugios eksploatacijos taisyklės
SSRA	Sistemos saugumo reikmių aktai
SŽV	Slaptumo žymų vadovas
TEI	TEMPEST institucija
TGS	Tarybos Generalinis sekretoriatas
TKI	Tinkamos kvalifikacijos institucija

2.6. COUNCIL DECISION OF 23 SEPTEMBER 2013 ON THE SECURITY RULES FOR PROTECTING EU CLASSIFIED INFORMATION

COUNCIL DECISION

of 23 September 2013

on the security rules for protecting EU classified information

(2013/488/EU)

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 240(3) thereof,

Having regard to Council Decision 2009/937/EU of 1 December 2009 adopting the Council's Rules of Procedure ([1]), and in particular Article 24 thereof,

Whereas:

(1) In order to develop Council activities in all areas which require handling classified information, it is appropriate to establish a comprehensive security system for protecting classified information covering the Council, its General Secretariat and the Member States.

(2) This Decision should apply where the Council, its preparatory bodies and the General Secretariat of the Council (GSC) handle EU classified information (EUCI).

(3) In accordance with national laws and regulations and to the extent required for the functioning of the Council, the Member States should respect this Decision where their competent authorities, personnel or contractors handle EUCI, in order that each may be assured that an equivalent level of protection is afforded to EUCI.

(4) The Council, the Commission and the European External Action Service (EEAS) are committed to applying equivalent security standards for protecting EUCI.

(5) The Council underlines the importance of associating, where appropriate, the European Parliament and other Union institutions, bodies, offices or agencies with the principles, standards and rules for protecting classified information which are necessary in order to protect the interests of the Union and its Member States.

(6) The Council should determine the appropriate framework for sharing EUCI held by the Council with other Union institutions, bodies, offices or agencies, as appropriate, in accordance with this Decision and interinstitutional arrangements in force.

(7) Union bodies and agencies established under Title V, Chapter 2, of the Treaty on European Union (TEU), Europol and Eurojust should apply, in the context of their internal organisation, the basic principles and minimum standards laid down in this Decision for protecting EUCI, where so provided in the act establishing them.

(8) Crisis management operations established under Title V, Chapter 2, of the TEU and their personnel should apply the security rules adopted by the Council for protecting EUCI where so provided in the Council act establishing them.

(9) EU Special Representatives and the members of their teams should apply the security rules adopted by the Council for protecting EUCI where so provided in the relevant Council act.

(10) This Decision is taken without prejudice to Articles 15 and 16 of the Treaty on the Functioning of the European Union (TFEU) and to instruments implementing them.

(11) This Decision is taken without prejudice to existing practices in Member States with regard to informing their national Parliaments about the activities of the Union.

(12) In order to ensure the application of the security rules for protecting EUCI in a timely manner as regards the accession of the Republic of Croatia to the European Union, this Decision should enter into force on the date of its publication,

HAS ADOPTED THIS DECISION:

Article 1

Purpose, scope and definitions

1. This Decision lays down the basic principles and minimum standards of security for protecting EUCI.

2. These basic principles and minimum standards shall apply to the Council and the GSC and be respected by the Member States in accordance with their respective national laws and regulations, in order that each may be assured that an equivalent level of protection is afforded to EUCI.

3. For the purposes of this Decision, the definitions set out in Appendix A shall apply.

Article 2

Definition of EUCI, security classifications and markings

1. 'EU classified information' (EUCI) means any information or material designated by a EU security classification, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States.

2. EUCI shall be classified at one of the following levels:

(a) TRÈS SECRET UE/EU TOP SECRET: information and material the unauthorised disclosure of which could cause exceptionally grave prejudice to the essential interests of the European Union or of one or more of the Member States;

(b) SECRET UE/EU SECRET: information and material the unauthorised disclosure of which could seriously harm the essential interests of the European Union or of one or more of the Member States;

(c) CONFIDENTIEL UE/EU CONFIDENTIAL: information and material the unauthorised disclosure of which could harm the essential interests of the European Union or of one or more of the Member States;

(d) RESTREINT UE/EU RESTRICTED: information and material the unauthorised disclosure of which could be disadvantageous to the interests of the European Union or of one or more of the Member States.

3. EUCI shall bear a security classification marking in accordance with paragraph 2. It may bear additional markings to designate the field of activity to which it relates, identify the originator, limit distribution, restrict use or indicate releasability.

Article 3

Classification management

1. The competent authorities shall ensure that EUCI is appropriately classified, clearly identified as classified information and retains its classification level for only as long as necessary.

2. EUCI shall not be downgraded or declassified nor shall any of the markings referred to in Article 2(3) be modified or removed without the prior written consent of the originator.

3. The Council shall approve a security policy on creating EUCI which shall include a practical classification guide.

Article 4

Protection of classified information

1. EUCI shall be protected in accordance with this Decision.

2. The holder of any item of EUCI shall be responsible for protecting it in accordance with this Decision.

3. Where Member States introduce classified information bearing a national security classification marking into the structures or networks of the Union, the Council and the GSC shall protect that information in accordance with the requirements applicable to EUCI at the equivalent level as set out in the table of equivalence of security classifications contained in Appendix B.

4. An aggregate of EUCI may warrant a level of protection corresponding to a higher classification than that of its individual components.

Article 5

Security risk management

1. Risk to EUCI shall be managed as a process. This process shall be aimed at determining known security risks, defining security measures to reduce such risks to an acceptable level in accordance with the basic principles and minimum standards set out in this Decision and at applying those measures in line with the concept of defence in depth as defined in Appendix A. The effectiveness of such measures shall be continuously evaluated.

2. Security measures for protecting EUCI throughout its life-cycle shall be commensurate in particular with its security classification, the form and the volume of the information or material, the location and construction of facilities housing EUCI and the locally assessed threat of malicious and/or criminal activities, including espionage, sabotage and terrorism.

3. Contingency plans shall take account of the need to protect EUCI during emergency situations in order to prevent unauthorised access, disclosure or loss of integrity or availability.

4. Preventive and recovery measures to minimise the impact of major failures or incidents on the handling and storage of EUCI shall be included in business continuity plans.

Article 6

Implementation of this Decision

1. Where necessary, the Council, on recommendation by the Security Committee, shall approve security policies setting out measures for implementing this Decision.

2. The Security Committee may agree at its level security guidelines to supplement or support this Decision and any security policies approved by the Council.

Article 7

Personnel security

1. Personnel security is the application of measures to ensure that access to EUCI is granted only to individuals who have:
– a need-to-know,
– been security cleared to the relevant level, where appropriate, and
– been briefed on their responsibilities.

2. Personnel security clearance procedures shall be designed to determine whether an individual, taking into account his loyalty, trustworthiness and reliability, may be authorised to access EUCI.

3. All individuals in the GSC whose duties require them to have access to or handle EUCI classified CONFIDENTIEL UE/EU CONFIDENTIAL or above shall be security cleared to the relevant level before being granted access to such EUCI. Such individuals must be authorised by the GSC Appointing Authority to access EUCI up to a specified level and up to a specified date.

4. Member States' personnel referred to in Article 15(3) whose duties may require access to EUCI classified CONFIDENTIEL UE/EU CONFIDENTIAL or above shall be security cleared to the relevant level or otherwise duly authorised by virtue of their functions, in accordance with national laws and regulations, before being granted access to such EUCI.

5. Before being granted access to EUCI and at regular intervals thereafter, all individuals shall be briefed on and acknowledge their responsibilities to protect EUCI in accordance with this Decision.

6. Provisions for implementing this Article are set out in Annex I.

Article 8

Physical security

1. Physical security is the application of physical and technical protective measures to prevent unauthorised access to EUCI.

2. Physical security measures shall be designed to deny surreptitious or forced entry by an intruder, to deter, impede and detect unauthorised actions and to allow for segregation of personnel in their access to EUCI on a need-to-know basis. Such measures shall be determined based on a

risk management process.

3. Physical security measures shall be put in place for all premises, buildings, offices, rooms and other areas in which EUCI is handled or stored, including areas housing communication and information systems as defined in Article 10(2).

4. Areas in which EUCI classified CONFIDENTIEL UE/EU CONFIDENTIAL or above is stored shall be established as Secured Areas in accordance with Annex II and approved by the competent security authority.

5. Only approved equipment or devices shall be used for protecting EUCI at the level CONFIDENTIEL UE/EU CONFIDENTIAL or above.

6. Provisions for implementing this Article are set out in Annex II.

Article 9

Management of classified information

1. The management of classified information is the application of administrative measures for controlling EUCI throughout its life-cycle to supplement the measures provided for in Articles 7, 8 and 10 and thereby help deter and detect deliberate or accidental compromise or loss of such information. Such measures relate in particular to the creation, registration, copying, translation, downgrading, declassification, carriage and destruction of EUCI.

2. Information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above shall be registered for security purposes prior to distribution and on receipt. The competent authorities in the GSC and in the Member States shall establish a registry system for this purpose. Information classified TRÈS SECRET UE/EU TOP SECRET shall be registered in designated registries.

3. Services and premises where EUCI is handled or stored shall be subject to regular inspection by the competent security authority.

4. EUCI shall be conveyed between services and premises outside physically protected areas as follows:

(a) as a general rule, EUCI shall be transmitted by electronic means protected by cryptographic products approved in accordance with Article 10(6);

(b) when the means referred to in point (a) are not used, EUCI shall be carried either:

(i) on electronic media (e.g. USB sticks, CDs, hard drives) protected by cryptographic products approved in accordance with Article 10(6); or

(ii) in all other cases, as prescribed by the competent security authority in accordance with the relevant protective measures laid down in Annex III.

5. Provisions for implementing this Article are set out in Annexes III and IV.

Article 10

Protection of EUCI handled in communication and information systems

1. Information Assurance (IA) in the field of communication and information systems is the confidence that such systems will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users. Effective IA shall ensure appropriate levels of confidentiality, integrity, availability, non-repudiation and authenticity. IA shall be based on a risk management process.

2. 'Communication and Information System' (CIS) means any system enabling the handling of information in electronic form. A CIS shall comprise the entire assets required for it to operate, including the infrastructure, organisation, personnel and information resources. This Decision shall apply to CIS handling EUCI.

3. CIS shall handle EUCI in accordance with the concept of IA.

4. All CIS shall undergo an accreditation process. Accreditation shall aim at obtaining assurance that all appropriate security measures have been implemented and that a sufficient level of protection of the EUCI and of the CIS has been achieved in accordance with this Decision. The accreditation statement shall determine the maximum classification level of the information that may be handled in a CIS as well as the corresponding terms and conditions.

5. Security measures shall be implemented to protect CIS handling information classified CONFIDENTIEL UE/EU CONFIDENTIAL and

above against compromise of such information through unintentional electromagnetic emanations ('TEMPEST security measures'). Such security measures shall be commensurate with the risk of exploitation and the level of classification of the information.

6. Where the protection of EUCI is provided by cryptographic products, such products shall be approved as follows:

(a) the confidentiality of information classified SECRET UE/EU SECRET and above shall be protected by cryptographic products approved by the Council as Crypto Approval Authority (CAA), upon recommendation by the Security Committee;

(b) the confidentiality of information classified CONFIDENTIEL UE/EU CONFIDENTIAL or RESTREINT UE/EU RESTRICTED shall be protected by cryptographic products approved by the Secretary-General of the Council ('the Secretary-General') as CAA, upon recommendation by the Security Committee.

Notwithstanding point (b), within Member States' national systems, the confidentiality of EUCI classified CONFIDENTIEL UE/EU CONFIDENTIAL or RESTREINT UE/EU RESTRICTED may be protected by cryptographic products approved by a Member State's CAA.

7. During transmission of EUCI by electronic means, approved cryptographic products shall be used. Notwithstanding this requirement, specific procedures may be applied under emergency circumstances or specific technical configurations as specified in Annex IV.

8. The competent authorities of the GSC and of the Member States respectively shall establish the following IA functions:

(a) an IA Authority (IAA);

(b) a TEMPEST Authority (TA);

(c) a Crypto Approval Authority (CAA);

(d) a Crypto Distribution Authority (CDA).

9. For each system, the competent authorities of the GSC and of the Member States respectively shall establish:

(a) a Security Accreditation Authority (SAA);

(b) an IA Operational Authority.

10. Provisions for implementing this Article are set out in Annex IV.

Article 11

Industrial security

1. Industrial security is the application of measures to ensure the protection of EUCI by contractors or subcontractors in pre-contract negotiations and throughout the life-cycle of classified contracts. Such contracts shall not involve access to information classified TRÈS SECRET UE/EU TOP SECRET.

2. The GSC may entrust by contract tasks involving or entailing access to or the handling or storage of EUCI by industrial or other entities registered in a Member State or in a third State which has concluded an agreement or an administrative arrangement in accordance with point (a) or (b) of Article 13(2).

3. The GSC, as contracting authority, shall ensure that the minimum standards on industrial security set out in this Decision, and referred to in the contract, are complied with when awarding classified contracts to industrial or other entities.

4. The National Security Authority (NSA), the Designated Security Authority (DSA) or any other competent authority of each Member State shall ensure, to the extent possible under national laws and regulations, that contractors and subcontractors registered in their territory take all appropriate measures to protect EUCI in pre-contract negotiations and when performing a classified contract.

5. The NSA, DSA or any other competent security authority of each Member State shall ensure, in accordance with national laws and regulations, that contractors or subcontractors registered in the respective Member State participating in classified contracts or sub-contracts which require access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET within their facilities, either in the performance of such contracts or during the pre-contractual stage, hold a Facility Security Clearance (FSC) at the relevant classification level.

6. Contractor or subcontractor personnel who, for the performance of a classified contract, require access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET shall be granted a Personnel Security Clearance (PSC) by the respective NSA, DSA or any other competent security authority

in accordance with national laws and regulations and the minimum standards laid down in Annex I.

7. Provisions for implementing this Article are set out in Annex V.

Article 12

Sharing EUCI

1. The Council shall determine the conditions under which it may share EUCI held by it with other Union institutions, bodies, offices or agencies. An appropriate framework may be put in place to that effect, including by entering into interinstitutional agreements or other arrangements where necessary for that purpose.

2. Any such framework shall ensure that EUCI is given protection appropriate to its classification level and according to basic principles and minimum standards which shall be equivalent to those laid down in this Decision.

Article 13

Exchange of classified information with third States and international organisations

1. Where the Council determines that there is a need to exchange EUCI with a third State or international organisation, an appropriate framework shall be put in place to that effect.

2. In order to establish such a framework and define reciprocal rules on the protection of classified information exchanged:

(a) the Union shall conclude agreements with third States or international organisations on security procedures for exchanging and protecting classified information ('security of information agreements'); or

(b) the Secretary-General may enter into administrative arrangements on behalf of the GSC in accordance with paragraph 17 of Annex VI where the classification level of EUCI to be released is as a general rule no higher than RESTREINT UE/EU RESTRICTED.

3. Security of information agreements or administrative arrangements referred to in paragraph 2 shall contain provisions to ensure that when third States or international organisations receive EUCI, such information is given protection appropriate to its classification level and according to

minimum standards which are no less stringent than those laid down in this Decision.

4. The decision to release EUCI originating in the Council to a third State or international organisation shall be taken by the Council on a case-by-case basis, according to the nature and content of such information, the recipient's need-to-know and the measure of advantage to the Union. If the originator of the classified information for which release is desired is not the Council, the GSC shall first seek the originator's written consent to release. If the originator cannot be established, the Council shall assume the former's responsibility.

5. Assessment visits shall be arranged to ascertain the effectiveness of the security measures in place in a third State or international organisation for protecting EUCI provided or exchanged.

6. Provisions for implementing this Article are set out in Annex VI.

Article 14

Breaches of security and compromise of EUCI

1. A breach of security occurs as the result of an act or omission by an individual which is contrary to the security rules laid down in this Decision.

2. Compromise of EUCI occurs when, as a result of a breach of security, it has wholly or in part been disclosed to unauthorised persons.

3. Any breach or suspected breach of security shall be reported immediately to the competent security authority.

4. Where it is known or where there are reasonable grounds to assume that EUCI has been compromised or lost, the NSA or other competent authority shall take all appropriate measures in accordance with the relevant laws and regulations to:

(a) inform the originator;

(b) ensure that the case is investigated by personnel not immediately concerned with the breach in order to establish the facts;

(c) assess the potential damage caused to the interests of the Union or of the Member States;

(d) take appropriate measures to prevent a recurrence; and

(e) notify the appropriate authorities of the action taken.

5. Any individual who is responsible for a breach of the security rules laid down in this Decision may be liable to disciplinary action in accordance with the applicable rules and regulations. Any individual who is responsible for compromising or losing EUCI shall be liable to disciplinary and/or legal action in accordance with the applicable laws, rules and regulations.

Article 15

Responsibility for implementation

1. The Council shall take all necessary measures to ensure overall consistency in the application of this Decision.

2. The Secretary-General shall take all necessary measures to ensure that, when handling or storing EUCI or any other classified information, this Decision is applied in premises used by the Council and within the GSC, by GSC officials and other servants, by personnel seconded to the GSC and by GSC contractors.

3. Member States shall take all appropriate measures, in accordance with their respective national laws and regulations, to ensure that when EUCI is handled or stored, this Decision is respected by:

(a) personnel of Member States' Permanent Representations to the European Union, and national delegates attending meetings of the Council or of its preparatory bodies, or participating in other Council activities;
(b) other personnel in Member States' national administrations, including personnel seconded to those administrations, whether they serve on the territory of the Member States or abroad;
(c) other persons in the Member States duly authorised by virtue of their functions to have access to EUCI; and
(d) Member States' contractors, whether on the territory of the Member States or abroad.

Article 16

The organisation of security in the Council

1. As part of its role in ensuring overall consistency in the application of this Decision, the Council shall approve:
(a) agreements referred to in Article 13(2)(a);
(b) decisions authorising or consenting to the release of EUCI originating in or held by the Council to third States and international organisations, in accordance with the principle of originator consent;
(c) an annual assessment visit programme recommended by the Security Committee for visits to assess Member States' services and premises, Union bodies, agencies and entities which apply this Decision or the principles thereof, and for assessment visits to third States and international organisations in order to ascertain the effectiveness of measures implemented for protecting EUCI; and
(d) security policies as foreseen in Article 6(1).

2. The Secretary-General shall be the GSC's Security Authority. In that capacity, the Secretary-General shall:
(a) implement the Council's security policy and keep it under review;
(b) coordinate with Member States' NSAs on all security matters relating to the protection of classified information relevant for the Council's activities;
(c) grant GSC officials, other servants and seconded national experts authorisation for access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above in accordance with Article 7(3);
(d) as appropriate, order investigations into any actual or suspected compromise or loss of classified information held by or originating in the Council and request the relevant security authorities to assist in such investigations;
(e) undertake periodic inspections of the security arrangements for protecting classified information on GSC premises;
(f) undertake periodic visits to assess the security arrangements for protecting EUCI in Union bodies, agencies and entities which apply this Decision or the principles thereof;
(g) undertake, jointly and in agreement with the NSA concerned, periodic assessments of the security arrangements for protecting EUCI in Member States' services and premises;

(h) ensure that security measures are coordinated as necessary with the competent authorities of the Member States which are responsible for protecting classified information and, as appropriate, third States or international organisations, including on the nature of threats to the security of EUCI and the means of protection against them; and

(i) enter into the administrative arrangements referred to in Article 13(2)(b).

The Security Office of the GSC shall be at the disposal of the Secretary-General to assist in those responsibilities.

3. For the purposes of implementing Article 15(3), Member States should:

(a) designate an NSA, as listed in Appendix C, responsible for security arrangements for protecting EUCI in order that:

(i) EUCI held by any national department, body or agency, public or private, at home or abroad, is protected in accordance with this Decision;

(ii) security arrangements for protecting EUCI are periodically inspected or assessed;

(iii) all individuals employed within a national administration or by a contractor who may be granted access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above are appropriately security cleared or are otherwise duly authorised by virtue of their functions in accordance with national laws and regulations;

(iv) security programmes are set up as necessary in order to minimise the risk of EUCI being compromised or lost;

(v) security matters related to protecting EUCI are coordinated with other competent national authorities, including those referred to in this Decision; and

(vi) responses are given to appropriate security clearance requests in particular from any Union bodies, agencies, entities, operations established under Title V, Chapter 2 of the TEU, and EU Special Representatives (EUSRs) and their teams which apply this Decision or the principles thereof;

(b) ensure that their competent authorities provide information and advice to their governments, and through them to the Council, on the nature of threats to the security of EUCI and the means of protection against them.

Article 17

Security Committee

1. A Security Committee is hereby established. It shall examine and assess any security matter within the scope of this Decision and make recommendations to the Council as appropriate.

2. The Security Committee shall be composed of representatives of the Member States' NSAs and be attended by a representative of the Commission and of the EEAS. It shall be chaired by the Secretary-General or by his designated delegate. It shall meet as instructed by the Council, or at the request of the Secretary-General or of an NSA.

Representatives of Union bodies, agencies and entities which apply this Decision or the principles thereof may be invited to attend when questions concerning them are discussed.

3. The Security Committee shall organise its activities in such a way that it can make recommendations on specific areas of security. It shall establish an expert sub-area for IA issues and other expert sub-areas as necessary. It shall draw up terms of reference for such expert sub-areas and receive reports from them on their activities including, as appropriate, any recommendations for the Council.

Article 18

Replacement of previous decision

1. This Decision shall repeal and replace Council Decision 2011/292/EU ([2]).

2. All EUCI classified in accordance with Council Decision 2001/264/EC ([3]) and with Decision 2011/292/EU shall continue to be protected in accordance with the relevant provisions of this Decision.

Article 19

Entry into force

This Decision shall enter into force on the date of its publication in the *Official Journal of the European Union*.

Done at Brussels, 23 September 2013.

For the Council
The President
V. JUKNA

([1]) OJ L 325, 11.12.2009, p. 35.

([2]) Council Decision 2011/292/EU of 31 March 2011 on the security rules for protecting EU classified information (OJ L 141, 27.5.2011, p. 17).

([3]) Council Decision 2001/264/EC of 19 March 2001 adopting the Council's security regulations (OJ L 101, 11.4.2001, p. 1).

ANNEXES

ANNEX I

Personnel security

ANNEX II

Physical security

ANNEX III

Management of classified information

ANNEX IV

Protection of EUCI handled in CIS

ANNEX V

Industrial security

ANNEX VI

Exchange of classified information with third States and international organisations

ANNEX I

PERSONNEL SECURITY

I. INTRODUCTION

1. This Annex sets out provisions for implementing Article 7. It lays down criteria for determining whether an individual, taking into account his loyalty, trustworthiness and reliability, may be authorised to have access to EUCI and the investigative and administrative procedures to be followed to that effect.

II. GRANTING ACCESS TO EUCI

2. An individual shall only be granted access to classified information after:

   (a) his need-to-know has been determined;

   (b) he has been briefed on the security rules and procedures for protecting EUCI and has acknowledged his responsibilities with regard to protecting such information; and

   (c) in the case of information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above:

   – he has been granted a PSC to the relevant level or is otherwise duly authorised by virtue of his functions in accordance with national laws and regulations, or

   – in the case of GSC officials, other servants or seconded national experts, he has been given authorisation for access to EUCI by the GSC Appointing Authority in accordance with paragraphs 16 to 25 up to a specified level and up to a specified date.
3. Each Member State and the GSC shall identify the positions in their structures which require access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above and therefore require security clearance to the relevant level.

III. PERSONNEL SECURITY CLEARANCE REQUIREMENTS

4. After having received a duly authorised request, NSAs or other competent national authorities shall be responsible for ensuring that security investigations are carried out on their nationals who require access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above. Standards of investigation shall be in accordance with national laws and regulations with a view to issuing a PSC or providing an assurance for the individual to be granted authorisation for access to EUCI, as appropriate.
5. Should the individual concerned reside in the territory of another Member State or of a third State, the competent national authorities shall seek assistance from the competent authority of the State of residence in accordance with national laws and regulations. Member States shall assist one another in carrying out security investigations in accordance with national laws and regulations.
6. Where permissible under national laws and regulations, NSAs or other competent national authorities may conduct investigations on non-nationals who require access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above. Standards of investigation shall be in accordance with national laws and regulations.

Security investigation criteria

7. The loyalty, trustworthiness and reliability of an individual for the purposes of being security cleared for access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above shall be determined by means of a security investigation. The competent national authority shall make an overall assessment based on the findings of such a security investigation. The principal criteria used for that purpose include, to the extent possible under national laws and regulations, an examination of whether the individual:

   (a) has committed or attempted to commit, conspired with or aided and abetted another to commit any act of espionage, terrorism, sabotage, treason or sedition;

   (b) is, or has been, an associate of spies, terrorists, saboteurs, or of individuals reasonably suspected of being such or an associate of

representatives of organisations or foreign states, including foreign intelligence services, which may threaten the security of the Union and/or Member States unless these associations were authorised in the course of official duty;

(c) is, or has been, a member of any organisation which by violent, subversive or other unlawful means seeks, inter alia, to overthrow the government of a Member State, to change the constitutional order of a Member State or to change the form or the policies of its government;

(d) is, or has been, a supporter of any organisation described in point (c), or who is, or who has been closely associated with members of such organisations;

(e) has deliberately withheld, misrepresented or falsified information of significance, particularly of a security nature, or has deliberately lied in completing a personnel security questionnaire or during the course of a security interview;

(f) has been convicted of a criminal offence or offences;

(g) has a history of alcohol dependence, use of illegal drugs and/or misuse of legal drugs;

(h) is or has been involved in conduct which may give rise to the risk of vulnerability to blackmail or pressure;

(i) by act or through speech, has demonstrated dishonesty, disloyalty, unreliability or untrustworthiness;

(j) has seriously or repeatedly infringed security regulations; or has attempted, or succeeded in, unauthorised activity in respect of communication and information systems; and

(k) may be liable to pressure (e.g. through holding one or more non-EU nationalities or through relatives or close associates who could be vulnerable to foreign intelligence services, terrorist groups or other subversive organisations, or individuals whose aims may threaten the security interests of the Union and/or Member States).

8. Where appropriate and in accordance with national laws and regulations, an individual's financial and medical background may also be considered relevant during the security investigation.

9. Where appropriate and in accordance with national laws and regulations, a spouse's, cohabitant's or close family member's conduct and circumstances may also be considered relevant during the security investigation.

Investigative requirements for access to EUCI

Initial granting of a security clearance

10. The initial security clearance for access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET shall be based on a security investigation covering at least the last 5 years, or from age 18 to the present, whichever is the shorter, which shall include the following:

    (a) the completion of a national personnel security questionnaire for the level of EUCI to which the individual may require access; once completed, this questionnaire shall be forwarded to the competent security authority;

    (b) 312identity check/citizenship/nationality status – the individual's date and place of birth shall be verified and his identity checked. Citizenship status and/or nationality, past and present, of the individual shall be established; this shall include an assessment of any vulnerability to pressure from foreign sources, for example, due to former residence or past associations; and

    (c) national and local records check – a check shall be made of national security and central criminal records, where the latter exist, and/or other comparable governmental and police records. The records of law enforcement agencies with legal jurisdiction where the individual has resided or been employed shall be checked.

11. The initial security clearance for access to information classified TRÈS SECRET UE/EU TOP SECRET shall be based on a security investigation covering at least the last 10 years, or from age 18 to the present, whichever is the shorter. If interviews are conducted as stated in point (e), investigations shall cover at least the last 7 years, or from age 18 to the present, whichever is the shorter. In addition to the criteria indicated in paragraph 7 above, the following elements shall be investigated, to the extent possible under national laws and regulations, before granting a TRÈS SECRET UE/EU

TOP SECRET PSC; they may also be investigated before granting a CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET PSC, where required by national laws and regulations:

(a) financial status – information shall be sought on the individual's finances in order to assess any vulnerability to foreign or domestic pressure due to serious financial difficulties, or to discover any unexplained affluence;

(b) education – information shall be sought to verify the individual's educational background at schools, universities and other education establishments attended since his 18th birthday, or during a period judged appropriate by the investigating authority;

(c) employment – information covering present and former employment shall be sought, reference being made to sources such as employment records, performance or efficiency reports and to employers or supervisors;

(d) military service – where applicable, the service of the individual in the armed forces and type of discharge shall be verified; and

(e) interviews – where provided for and admissible under national law, an interview or interviews shall be conducted with the individual. Interviews shall also be conducted with other individuals who are in a position to give an unbiased assessment of the individual's background, activities, loyalty, trustworthiness and reliability. When it is national practice to ask the subject of the investigation for referrals, referees shall be interviewed unless there are good reasons for not doing so.

12. Where necessary and in accordance with national laws and regulations, additional investigations may be conducted to develop all relevant information available on an individual and to substantiate or disprove adverse information.

Renewal of a security clearance

13. After the initial granting of a security clearance and provided that the individual has had uninterrupted service with a national administration or the GSC and has a continuing need for access to EUCI, the security clearance shall be reviewed for renewal at intervals not exceeding 5 years for a TRÈS SECRET UE/EU TOP SECRET clearance and 10 years for SECRET UE/EU SECRET and CONFIDENTIEL UE/EU CONFIDENTIAL clearances, with

effect from the date of notification of the outcome of the last security investigation on which they were based. All security investigations for renewing a security clearance shall cover the period since the previous such investigation.

14. For renewing security clearances, the elements outlined in paragraphs 10 and 11 shall be investigated.
15. Requests for renewal shall be made in a timely manner taking account of the time required for security investigations. Nevertheless, where the relevant NSA or other competent national authority has received the relevant request for renewal and the corresponding personnel security questionnaire before a security clearance expires, and the necessary security investigation has not been completed, the competent national authority may, where admissible under national laws and regulations, extend the validity of the existing security clearance for a period of up to 12 months. If, at the end of this 12-month period, the security investigation has still not been completed, the individual shall be assigned to duties which do not require a security clearance.

Authorisation procedures in the GSC

16. For officials and other servants in the GSC, the GSC Security Authority shall forward the completed personnel security questionnaire to the NSA of the Member State of which the individual is a national requesting that a security investigation be undertaken for the level of EUCI to which the individual will require access.
17. Where information relevant for a security investigation becomes known to the GSC concerning an individual who has applied for a security clearance for access to EUCI, the GSC, acting in accordance with the relevant rules and regulations, shall notify the relevant NSA thereof.
18. Following completion of the security investigation, the relevant NSA shall notify the GSC Security Authority of the outcome of such an investigation, using the standard format for the correspondence prescribed by the Security Committee.

    (a) Where the security investigation results in an assurance that nothing adverse is known which would call into question the loyalty, trustworthiness and reliability of the individual, the GSC Appointing Authority may grant the individual concerned authorisation for access to EUCI up to the relevant level until a specified date.

(b) Where the security investigation does not result in such an assurance, the GSC Appointing Authority shall notify the individual concerned, who may ask to be heard by the Appointing Authority. The Appointing Authority may ask the competent NSA for any further clarification it can provide according to its national laws and regulations. If the outcome is confirmed, authorisation shall not be granted for access to EUCI.

19. The security investigation together with the results obtained shall be subject to the relevant laws and regulations in force in the Member State concerned, including those concerning appeals. Decisions by the GSC Appointing Authority shall be subject to appeals in accordance with the Staff Regulations of Officials of the European Union and the Conditions of Employment of Other Servants of the European Union, laid down in Council Regulation (EEC, Euratom, ECSC) No 259/68 ([1]) ('the Staff Regulations and Conditions of Employment').
20. National experts seconded to the GSC for a position requiring access to EUCI classified CONFIDENTIEL UE/EU CONFIDENTIAL and above shall present a valid Personnel Security Clearance Certificate (PSCC) for access to EUCI to the GSC Security Authority prior to taking up their assignment, on the basis of which the Appointing Authority shall issue an authorisation for access to EUCI.
21. The GSC will accept the authorisation for access to EUCI granted by any other Union institution, body or agency, provided it remains valid. Authorisation will cover any assignment by the individual concerned within the GSC. The Union institution, body or agency in which the individual is taking up employment will notify the relevant NSA of the change of employer.
22. If an individual's period of service does not commence within 12 months of the notification of the outcome of the security investigation to the GSC Appointing Authority, or if there is a break of 12 months in an individual's service, during which time he has not been employed in the GSC or in a position with a national administration of a Member State, this outcome shall be referred to the relevant NSA for confirmation that it remains valid and appropriate.
23. Where information becomes known to the GSC concerning a security risk posed by an individual who has authorisation for access to EUCI, the GSC, acting in accordance with the relevant rules and regulations, shall notify the relevant NSA thereof and may suspend access to EUCI or withdraw authorisation for access to EUCI.

24. Where an NSA notifies the GSC of withdrawal of an assurance given in accordance with paragraph 18(a) for an individual who has authorisation for access to EUCI, the GSC Appointing Authority may ask for any clarification the NSA can provide according to its national laws and regulations. If the adverse information is confirmed, authorisation shall be withdrawn and the individual shall be excluded from access to EUCI and from positions where such access is possible or where he might endanger security.
25. Any decision to withdraw or suspend an authorisation from a GSC official or other servant for access to EUCI and, where appropriate, the reasons for doing so shall be notified to the individual concerned, who may ask to be heard by the Appointing Authority. Information provided by an NSA shall be subject to the relevant laws and regulations in force in the Member State concerned, including those concerning appeals. Decisions by the GSC Appointing Authority shall be subject to appeals in accordance with the Staff Regulations and Conditions of Employment.

Records of security clearances and authorisations

26. Records of PSCs and authorisations granted for access to information classified as CONFIDENTIEL UE/EU CONFIDENTIAL or above shall be maintained respectively by each Member State and by the GSC. These records shall contain as a minimum the level of EUCI to which the individual may be granted access, the date the security clearance was granted and its period of validity.
27. The competent security authority may issue a PSCC showing the level of EUCI to which the individual may be granted access (CONFIDENTIEL UE/EU CONFIDENTIAL or above), the date of validity of the relevant PSC for access to EUCI or authorisation for access to EUCI and the date of expiry of the certificate itself.

Exemptions from the PSC requirement

28. Access to EUCI by individuals in Member States duly authorised by virtue of their functions shall be determined in accordance with national laws and regulations; such individuals shall be briefed on their security obligations in respect of protecting EUCI.

IV. SECURITY EDUCATION AND AWARENESS

29. All individuals who have been granted a security clearance shall acknowledge in writing that they have understood their obligations in respect of protecting EUCI and the consequences if EUCI is compromised. A record of such a written acknowledgement shall be kept by the Member State and by the GSC, as appropriate.
30. All individuals who are authorised to have access to, or required to handle EUCI, shall initially be made aware, and periodically briefed on the threats to security and must report immediately to the appropriate security authorities any approach or activity that they consider suspicious or unusual.
31. All individuals who cease to be employed in duties requiring access to EUCI shall be made aware of, and where appropriate acknowledge in writing, their obligations in respect of the continued protection of EUCI.

V. EXCEPTIONAL CIRCUMSTANCES

32. Where permissible under national laws and regulations, security clearance granted by a competent national authority of a Member State for access to national classified information may, for a temporary period pending the granting of a PSC for access to EUCI, allow access by national officials to EUCI up to the equivalent level specified in the table of equivalence in Appendix B where such temporary access is required in the interests of the Union. NSAs shall inform the Security Committee where national laws and regulations do not permit such temporary access to EUCI.
33. For reasons of urgency, where duly justified in the interests of the service and pending completion of a full security investigation, the GSC Appointing Authority may, after consulting the NSA of the Member State of whom the individual is a national and subject to the outcome of preliminary checks to verify that no adverse information is known, grant a temporary authorisation for GSC officials and other servants to access EUCI for a specific function. Such temporary authorisations shall be valid for a period not exceeding 6 months and shall not permit access to information classified TRÈS SECRET UE/EU TOP SECRET. All individuals who have been granted a

temporary authorisation shall acknowledge in writing that they have understood their obligations in respect of protecting EUCI and the consequences if EUCI is compromised. A record of such a written acknowledgement shall be kept by the GSC.

34. When an individual is to be assigned to a position that requires a security clearance at one level higher than that currently possessed by the individual, the assignment may be made on a provisional basis, provided that:

(a) the compelling need for access to EUCI at a higher level shall be justified, in writing, by the individual's superior;

(b) access shall be limited to specific items of EUCI in support of the assignment;

(c) the individual holds a valid PSC or authorisation for access to EUCI;

(d) action has been initiated to obtain authorisation for the level of access required for the position;

(e) satisfactory checks have been made by the competent authority that the individual has not seriously or repeatedly infringed security regulations;

(f) the assignment of the individual is approved by the competent authority; and

(g) a record of the exception, including a description of the information to which access was approved, shall be kept by the registry or subordinate registry responsible.

35. The above procedure shall be used for one-time access to EUCI at one level higher than that to which the individual has been security cleared. Recourse to this procedure shall not be made on a recurring basis.

36. In very exceptional circumstances, such as missions in hostile environments or during periods of mounting international tension when emergency measures require it, in particular for the purposes of saving lives, Member States and the Secretary-General may grant, where possible in writing, access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET to individuals who do not possess the requisite security clearance, provided that such permission is absolutely necessary and there are no reasonable doubts as to the loyalty, trustworthiness and

reliability of the individual concerned. A record shall be kept of this permission describing the information to which access was approved.

37. In the case of information classified TRÈS SECRET UE/EU TOP SECRET, this emergency access shall be confined to Union nationals who have been authorised access to either the national equivalent of TRÈS SECRET UE/EU TOP SECRET or information classified SECRET UE/EU SECRET.
38. The Security Committee shall be informed of cases when recourse is made to the procedure set out in paragraphs 36 and 37.
39. Where national laws and regulations of a Member State stipulate more stringent rules with respect to temporary authorisations, provisional assignments, one-time access or emergency access by individuals to classified information, the procedures foreseen in this Section shall be implemented only within any limitations set forth in the relevant national laws and regulations.
40. The Security Committee shall receive an annual report on recourse to the procedures set out in this Section.

VI. ATTENDANCE AT MEETINGS IN THE COUNCIL

41. Subject to paragraph 28, individuals assigned to participate in meetings of the Council or of Council preparatory bodies at which information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above is discussed may only do so upon confirmation of the individual's security clearance status. For delegates, a PSCC or other proof of security clearance shall be forwarded by the appropriate authorities to the GSC Security Office, or exceptionally be presented by the delegate concerned. Where applicable, a consolidated list of names may be used, giving the relevant proof of security clearance.
42. Where a PSC for access to EUCI is withdrawn for security reasons from an individual whose duties require attendance at meetings of the Council or of Council preparatory bodies, the competent authority shall inform the GSC thereof.

VII. POTENTIAL ACCESS TO EUCI

43. Couriers, guards and escorts shall be security cleared to the relevant level or otherwise appropriately investigated in accordance with national laws and regulations, be briefed on security procedures for protecting EUCI and be instructed on their duties for protecting such information entrusted to them.

([1]) Council Regulation (EEC, Euratom, ECSC) No 259/68 of 29 February 1968 laying down the Staff Regulations and the Conditions of Employment of Other Servants of the European Communities and instituting special measures temporarily applicable to officials of the Commission (OJ L 56, 4.3.1968, p. 1.).

ANNEX II

PHYSICAL SECURITY

I. INTRODUCTION

1. This Annex sets out provisions for implementing Article 8. It lays down minimum requirements for the physical protection of premises, buildings, offices, rooms and other areas where EUCI is handled and stored, including areas housing CIS.
2. Physical security measures shall be designed to prevent unauthorised access to EUCI by:

   (a) ensuring that EUCI is handled and stored in an appropriate manner;

   (b) allowing for segregation of personnel in terms of access to EUCI on the basis of their need-to-know and, where appropriate, their security clearance;

   (c) deterring, impeding and detecting unauthorised actions; and

   (d) denying or delaying surreptitious or forced entry by intruders.

II. PHYSICAL SECURITY REQUIREMENTS AND MEASURES

3. Physical security measures shall be selected on the basis of a threat assessment made by the competent authorities. The GSC and Member States shall each apply a risk management process for protecting EUCI on their premises to ensure that a commensurate level of physical protection is afforded against the assessed risk. The risk management process shall take account of all relevant factors, in particular:

   (a) the classification level of EUCI;

   (b) the form and volume of EUCI, bearing in mind that large quantities or a compilation of EUCI may require more stringent protective measures to be applied;

   (c) the surrounding environment and structure of the buildings or areas housing EUCI; and

(d) the assessed threat from intelligence services which target the Union or Member States and from sabotage, terrorist, subversive or other criminal activities.

4. The competent security authority, applying the concept of defence in depth, shall determine the appropriate combination of physical security measures to be implemented. These can include one or more of the following:

(a) a perimeter barrier: a physical barrier which defends the boundary of an area requiring protection;

(b) intrusion detection systems (IDS): an IDS may be used to enhance the level of security offered by a perimeter barrier, or in rooms and buildings in place of, or to assist, security staff;

(c) access control: access control may be exercised over a site, a building or buildings on a site or to areas or rooms within a building. Control may be exercised by electronic or electro-mechanical means, by security personnel and/or a receptionist, or by any other physical means;

(d) security personnel: trained, supervised and, where necessary, appropriately security-cleared security personnel may be employed, inter alia, in order to deter individuals planning covert intrusion;

(e) closed circuit television (CCTV): CCTV may be used by security personnel in order to verify incidents and IDS alarms on large sites or at perimeters;

(f) security lighting: security lighting may be used to deter a potential intruder, as well as to provide the illumination necessary for effective surveillance directly by security personnel or indirectly through a CCTV system; and

(g) any other appropriate physical measures designed to deter or detect unauthorised access or prevent loss of or damage to EUCI.

5. The competent authority can be authorised to conduct entry and exit searches to act as a deterrent to the unauthorised introduction of material or the unauthorised removal of EUCI from premises or buildings.
6. When EUCI is at risk from overlooking, even accidentally, appropriate measures shall be taken to counter this risk.
7. For new facilities, physical security requirements and their functional specifications shall be defined as part of the planning and design of the facilities. For existing facilities, physical security requirements shall be implemented to the maximum extent possible.

III. EQUIPMENT FOR THE PHYSICAL PROTECTION OF EUCI

8. When acquiring equipment (such as security containers, shredding machines, door locks, electronic access control systems, IDS, alarm systems) for the physical protection of EUCI, the competent security authority shall ensure that the equipment meets approved technical standards and minimum requirements.
9. The technical specifications of equipment to be used for the physical protection of EUCI shall be set out in security guidelines to be approved by the Security Committee.
10. Security systems shall be inspected at regular intervals and equipment shall be maintained regularly. Maintenance work shall take account of the outcome of inspections to ensure that equipment continues to operate at optimum performance.
11. The effectiveness of individual security measures and of the overall security system shall be re-evaluated during each inspection.

IV. PHYSICALLY PROTECTED AREAS

12. Two types of physically protected areas, or the national equivalents thereof, shall be established for the physical protection of EUCI:

    (a) Administrative Areas; and

    (b) Secured Areas (including technically Secured Areas).

    In this Decision, all references to Administrative Areas and Secured Areas, including technically Secured Areas, shall be understood as also referring to the national equivalents thereof.
13. The competent security authority shall establish that an area meets the requirements to be designated as an Administrative Area, a Secured Area or a technically Secured Area.
14. For Administrative Areas:

    (a) a visibly defined perimeter shall be established which allows individuals and, where possible, vehicles to be checked;

    (b) unescorted access shall be granted only to individuals who are duly authorised by the competent authority; and

    (c) all other individuals shall be escorted at all times or be subject to equivalent controls.

15. For Secured Areas:

(a) a visibly defined and protected perimeter shall be established through which all entry and exit are controlled by means of a pass or personal recognition system;

(b) unescorted access shall be granted only to individuals who are security-cleared and specifically authorised to enter the area on the basis of their need-to-know; and

(c) all other individuals shall be escorted at all times or be subject to equivalent controls.

16. Where entry into a Secured Area constitutes, for all practical purposes, direct access to the classified information contained in it, the following additional requirements shall apply:

(a) the level of highest security classification of the information normally held in the area shall be clearly indicated;

(b) all visitors shall require specific authorisation to enter the area, shall be escorted at all times and shall be appropriately security cleared unless steps are taken to ensure that no access to EUCI is possible.

17. Secured Areas protected against eavesdropping shall be designated technically Secured Areas. The following additional requirements shall apply:

(a) such areas shall be IDS equipped, be locked when not occupied and be guarded when occupied. Any keys shall be controlled in accordance with Section VI;

(b) all persons and material entering such areas shall be controlled;

(c) such areas shall be regularly physically and/or technically inspected as required by the competent security authority. Such inspections shall also be conducted following any unauthorised entry or suspicion of such entry; and

(d) such areas shall be free of unauthorised communication lines, unauthorised telephones or other unauthorised communication devices and electrical or electronic equipment.

18. Notwithstanding point (d) of paragraph 17, before being used in areas where meetings are held or work is being performed involving information classified SECRET UE/EU SECRET and above, and where the threat to EUCI is assessed as high, any communications devices and electrical or electronic equipment shall first be examined

by the competent security authority to ensure that no intelligible information can be inadvertently or illicitly transmitted by such equipment beyond the perimeter of the Secured Area.

19. Secured Areas which are not occupied by duty personnel on a 24-hour basis shall, where appropriate, be inspected at the end of normal working hours and at random intervals outside normal working hours, unless an IDS is in place.
20. Secured Areas and technically Secured Areas may be set up temporarily within an Administrative Area for a classified meeting or any other similar purpose.
21. Security operating procedures shall be drawn up for each Secured Area stipulating:

    (a) the level of EUCI which may be handled and stored in the area;

    (b) the surveillance and protective measures to be maintained;

    (c) the individuals authorised to have unescorted access to the area by virtue of their need-to-know and security clearance;

    (d) where appropriate, the procedures for escorts or for protecting EUCI when authorising any other individuals to access the area; and

    (e) any other relevant measures and procedures.
22. Strong rooms shall be constructed within Secured Areas. The walls, floors, ceilings, windows and lockable doors shall be approved by the competent security authority and afford protection equivalent to a security container approved for the storage of EUCI of the same classification level.

V. PHYSICAL PROTECTIVE MEASURES FOR HANDLING AND STORING EUCI

23. EUCI which is classified RESTREINT UE/EU RESTRICTED may be handled:

    (a) in a Secured Area;

    (b) in an Administrative Area provided the EUCI is protected from access by unauthorised individuals; or

    (c) outside a Secured Area or an Administrative Area provided the holder carries the EUCI in accordance with paragraphs 28 to 41 of Annex III and has undertaken to comply with compensatory measures laid down in security instructions issued by the competent security authority to ensure that EUCI is protected from access by

security authority to ensure that EUCI is protected from access by unauthorised persons.

24. EUCI which is classified RESTREINT UE/EU RESTRICTED shall be stored in suitable locked office furniture in an Administrative Area or a Secured Area. It may temporarily be stored outside a Secured Area or an Administrative Area provided the holder has undertaken to comply with compensatory measures laid down in security instructions issued by the competent security authority.
25. EUCI which is classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET may be handled:

(a) in a Secured Area;

(b) in an Administrative Area provided the EUCI is protected from access by unauthorised individuals; or

(c) outside a Secured Area or an Administrative Area provided the holder:

(i) carries the EUCI in accordance with paragraphs 28 to 41 of Annex III;

(ii) has undertaken to comply with compensatory measures laid down in security instructions issued by the competent security authority to ensure that EUCI is protected from access by unauthorised persons;

(iii) keeps the EUCI at all times under his personal control; and

(iv) in the case of documents in paper form, has notified the relevant registry of the fact.

26. EUCI which is classified CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET shall be stored in a Secured Area either in a security container or in a strong room.
27. EUCI which is classified TRÈS SECRET UE/EU TOP SECRET shall be handled in a Secured Area.
28. EUCI which is classified TRÈS SECRET UE/EU TOP SECRET shall be stored in a Secured Area under one of the following conditions:

(a) in a security container in line with paragraph 8 with at least one of the following supplementary controls:

(i) continuous protection or verification by cleared security staff or duty personnel;

(ii) an approved IDS in combination with response security personnel;

(b) in an IDS-equipped strong room in combination with response security personnel.

29. Rules governing the carriage of EUCI outside physically protected areas are set out in Annex III.

VI. CONTROL OF KEYS AND COMBINATIONS USED FOR PROTECTING EUCI

30. The competent security authority shall define procedures for managing keys and combination settings for offices, rooms, strong rooms and security containers. Such procedures shall protect against unauthorised access.

31. Combination settings shall be committed to memory by the smallest possible number of individuals needing to know them. Combination settings for security containers and strong rooms storing EUCI shall be changed:

(a) on receipt of a new container;

(b) whenever there is a change in personnel knowing the combination;

(c) whenever a compromise has occurred or is suspected;

(d) when a lock has undergone maintenance or repair; and

(e) at least every 12 months.

ANNEX III

MANAGEMENT OF CLASSIFIED INFORMATION

I. INTRODUCTION

1. This Annex sets out provisions for implementing Article 9. It lays down the administrative measures for controlling EUCI throughout its life-cycle in order to help deter and detect deliberate or accidental compromise or loss of such information.

II. CLASSIFICATION MANAGEMENT

Classifications and markings

2. Information shall be classified where it requires protection with regard to its confidentiality.
3. The originator of EUCI shall be responsible for determining the security classification level, in accordance with the relevant classification guidelines, and for the initial dissemination of the information.
4. The classification level of EUCI shall be determined in accordance with Article 2(2) and by reference to the security policy to be approved in accordance with Article 3(3).
5. The security classification shall be clearly and correctly indicated, regardless of whether the EUCI is on paper, oral, electronic or in any other form.
6. Individual parts of a given document (i.e. pages, paragraphs, sections, annexes, appendices, attachments and enclosures) may require different classifications and shall be marked accordingly, including when stored in electronic form.
7. The overall classification level of a document or file shall be at least as high as that of its most highly classified component. When information from various sources is collated, the final product shall be reviewed to determine its overall security classification level, since it may warrant a higher classification than its component parts.
8. To the extent possible, documents containing parts with different classification levels shall be structured so that parts with a different classification level may be easily identified and detached if necessary.

9. The classification of a letter or note covering enclosures shall be as high as the highest classification of its enclosures. The originator shall indicate clearly at which level it is classified when detached from its enclosures by means of an appropriate marking, e.g.:
CONFIDENTIEL UE/EU CONFIDENTIAL

Without attachment(s) RESTREINT UE/EU RESTRICTED

Markings

10. In addition to one of the security classification markings set out in Article 2(2), EUCI may bear additional markings, such as:

(a) an identifier to designate the originator;

(b) any caveats, code-words or acronyms specifying the field of activity to which the document relates, a particular distribution on a need-to-know basis or restrictions on use;

(c) releasability markings; or

(d) where applicable, the date or specific event after which it may be downgraded or declassified.

Abbreviated classification markings

11. Standardised abbreviated classification markings may be used to indicate the classification level of individual paragraphs of a text. Abbreviations shall not replace the full classification markings.
12. The following standard abbreviations may be used within EU classified documents to indicate the classification level of sections or blocks of text of less than a single page:

TRÈS SECRET UE/EU TOP SECRETV	TS-UE/EU-TS
SECRET UE/EU SECRET	S-UE/EU-S
CONFIDENTIEL UE/EU CONFIDENTIAL	C-UE/EU-C
RESTREINT UE/EU RESTRICTED	R-UE/EU-R

Creation of EUCI

13. When creating an EU classified document:

    (a) each page shall be marked clearly with the classification level;

    (b) each page shall be numbered;

    (c) the document shall bear a reference number and a subject, which is not itself classified information, unless it is marked as such;

    (d) the document shall be dated; and

    (e) documents classified SECRET UE/EU SECRET or above shall bear a copy number on every page, if they are to be distributed in several copies.
14. Where it is not possible to apply paragraph 13 to EUCI, other appropriate measures shall be taken in accordance with security guidelines to be established pursuant to Article 6(2).

Downgrading and declassification of EUCI

15. At the time of its creation, the originator shall indicate, where possible, and in particular for information classified RESTREINT UE/EU RESTRICTED, whether EUCI can be downgraded or declassified on a given date or following a specific event.
16. The GSC shall regularly review EUCI held by it to ascertain whether the classification level still applies. The GSC shall establish a system to review the classification level of EUCI which it has originated no less frequently than every five years. Such a review shall not be necessary where the originator has indicated from the outset that the information will automatically be downgraded or declassified and the information has been marked accordingly.

III. REGISTRATION OF EUCI FOR SECURITY PURPOSES

17. For every organisational entity within the GSC and Member States' national administrations in which EUCI is handled, a responsible registry shall be identified to ensure that EUCI is handled in accordance with this Decision. Registries shall be established as Secured Areas as defined in Annex II.

18. For the purposes of this Decision, registration for security purposes ('registration') means the application of procedures which record the life-cycle of material, including its dissemination and destruction.
19. All material classified CONFIDENTIEL UE/EU CONFIDENTIAL and above shall be registered in designated registries when it arrives at or leaves an organisational entity.
20. The Central Registry within the GSC shall keep a record of all classified information released by the Council and the GSC to third States and international organisations, and of all classified information received from third States or international organisations.
21. In the case of a CIS, registration procedures may be performed by processes within the CIS itself.
22. The Council shall approve a security policy on the registration of EUCI for security purposes.

TRÈS SECRET UE/EU TOP SECRET registries

23. A registry shall be designated in the Member States and in the GSC to act as the central receiving and dispatching authority for information classified TRÈS SECRET UE/EU TOP SECRET. Where necessary, subordinate registries may be designated to handle such information for registration purposes.
24. Such subordinate registries may not transmit TRÈS SECRET UE/EU TOP SECRET documents directly to other subordinate registries of the same central TRÈS SECRET UE/EU TOP SECRET registry or externally without the express written approval of the latter.

IV. COPYING AND TRANSLATING EU CLASSIFIED DOCUMENTS

25. TRÈS SECRET UE/EU TOP SECRET documents shall not be copied or translated without the prior written consent of the originator.
26. Where the originator of documents classified SECRET UE/EU SECRET and below has not imposed caveats on their copying or translation, such documents may be copied or translated on instruction from the holder.
27. The security measures applicable to the original document shall apply to copies and translations thereof.

V. CARRIAGE OF EUCI

28. Carriage of EUCI shall be subject to the protective measures set out in paragraphs 30 to 41. When EUCI is carried on electronic media, and notwithstanding Article 9(4), the protective measures set out below may be supplemented by appropriate technical countermeasures prescribed by the competent security authority so as to minimise the risk of loss or compromise.
29. The competent security authorities in the GSC and in Member States shall issue instructions on the carriage of EUCI in accordance with this Decision.

Within a building or self-contained group of buildings

30. EUCI carried within a building or self-contained group of buildings shall be covered in order to prevent observation of its contents.
31. Within a building or self-contained group of buildings, information classified TRÈS SECRET UE/EU TOP SECRET shall be carried in a secured envelope bearing only the addressee's name.

Within the Union

32. EUCI carried between buildings or premises within the Union shall be packaged so that it is protected from unauthorised disclosure.
33. The carriage of information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET within the Union shall be by one of the following means:

(a) military, government or diplomatic courier, as appropriate;

(b) hand carriage, provided that:

(i) EUCI does not leave the possession of the bearer, unless it is stored in accordance with the requirements set out in Annex II;

(ii) EUCI is not opened en route or read in public places;

(iii) individuals are briefed on their security responsibilities; and

(iv) individuals are provided with a courier certificate where necessary;

(c) postal services or commercial courier services, provided that:

(i) they are approved by the relevant NSA in accordance with national laws and regulations; and

(ii) they apply appropriate protective measures in accordance with minimum requirements to be laid down in security guidelines pursuant to Article 6(2).

In the case of carriage from one Member State to another, the provisions of point (c) shall be limited to information classified up to CONFIDENTIEL UE/EU CONFIDENTIAL.

34. Information classified RESTREINT UE/EU RESTRICTED may also be carried by postal services or commercial courier services. A courier certificate is not required for the carriage of such information.
35. Material classified CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET (e.g. equipment or machinery) which cannot be carried by the means referred to in paragraph 33 shall be transported as freight by commercial carrier companies in accordance with Annex V.
36. The carriage of information classified TRÈS SECRET UE/EU TOP SECRET between buildings or premises within the Union shall be by military, government or diplomatic courier, as appropriate.

From within the Union to the territory of a third State

37. EUCI carried from within the Union to the territory of a third State shall be packaged in such a way that it is protected from unauthorised disclosure.
38. The carriage of information classified CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET from within the Union to the territory of a third State shall be by one of the following means:

(a) military or diplomatic courier;

(b) hand carriage, provided that:

(i) the package bears an official seal, or is packaged so as to indicate that it is an official consignment and should not undergo customs or security scrutiny;

(ii) individuals carry a courier certificate identifying the package and authorising them to carry the package;

(iii) EUCI does not leave the possession of the bearer, unless it is stored in accordance with the requirements set out in Annex II;

(iv) EUCI is not opened en route or read in public places; and

(v) individuals are briefed on their security responsibilities.

39. The carriage of information classified CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET released by the Union to a third State or international organisation shall comply with the relevant provisions under a security of information Agreement or an administrative arrangement in accordance with Article 13(2) (a) or (b).
40. Information classified RESTREINT UE/EU RESTRICTED may also be carried by postal services or commercial courier services.
41. The carriage of information classified TRÈS SECRET UE/EU TOP SECRET from within the Union to the territory of a third State shall be by military or diplomatic courier.

VI. DESTRUCTION OF EUCI

42. EU classified documents which are no longer required may be destroyed, without prejudice to the relevant rules and regulations on archiving.
43. Documents subject to registration in accordance with Article 9(2) shall be destroyed by the responsible registry on instruction from the holder or from a competent authority. The logbooks and other registration information shall be updated accordingly.
44. For documents classified SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET, destruction shall be performed in the presence of a witness who shall be cleared to at least the classification level of the document being destroyed.
45. The registrar and the witness, where the presence of the latter is required shall sign a destruction certificate, which shall be filed in the registry. The registry shall keep destruction certificates of TRÈS SECRET UE/EU TOP SECRET documents for a period of at least 10 years and of documents CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET for a period of at least five years.

46. Classified documents, including those classified RESTREINT UE/EU RESTRICTED, shall be destroyed by methods which meet relevant Union or equivalent standards or which have been approved by Member States in accordance with national technical standards so as to prevent reconstruction in whole or in part.
47. The destruction of computer storage media used for EUCI shall be in accordance with paragraph 37 of Annex IV.
48. In the event of an emergency, if there is an imminent risk of unauthorised disclosure EUCI shall be destroyed by the holder in such a way that it cannot be reconstructed in whole or in part. The originator and originating registry shall be informed of the emergency destruction of registered EUCI.

VII. ASSESSMENT VISITS

49. The term 'assessment visit' shall be used hereinafter to designate any:

    (a) inspections or assessment visits in accordance with Article 9(3) and points (e), (f) and (g) of Article 16(2); or

    (b) assessment visit in accordance with Article 13(5);

    to evaluate the effectiveness of measures implemented for protecting EUCI.
50. Assessment visits shall be carried out, inter alia, to:

    (a) ensure that the required minimum standards for protecting EUCI laid down in this Decision are respected;

    (b) emphasise the importance of security and effective risk management within the entities inspected;

    (c) recommend countermeasures to mitigate the specific impact of loss of confidentiality, integrity or availability of classified information; and

    (d) reinforce security authorities' ongoing security education and awareness programmes.
51. Before the end of each calendar year, the Council shall adopt the assessment visit programme foreseen in point (c) of Article 16(1) for the following year. The actual dates for each assessment visit shall be determined in agreement with the Union body or agency, Member State, third State or international organisation concerned.

Conduct of assessment visits

52. Assessment visits shall be conducted in order to check the relevant rules, regulations and procedures in the visited entity and verify whether the entity's practices comply with the basic principles and minimum standards laid down in this Decision and in the provisions governing the exchange of classified information with that entity.
53. Assessment visits shall be conducted in two phases. Prior to the visit itself a preparatory meeting shall be organised, if necessary, with the entity concerned. After this preparatory meeting the assessment team shall establish, in agreement with the entity concerned, a detailed assessment visit programme covering all areas of security. The assessment visit team should have access to any location where EUCI is handled, in particular registries and CIS points of presence.
54. Assessment visits to Member States' national administrations, third States and international organisations shall be conducted in full cooperation with the officials of the entity, third State or international organisation being visited.
55. Assessment visits to Union bodies, agencies and entities which apply this Decision or the principles thereof shall be conducted with assistance from experts of the NSA on whose territory the body or agency is located.
56. In the case of assessment visits to Union bodies, agencies and entities which apply this Decision or the principles thereof, and to third States and international organisations, assistance and contributions from NSA experts may be requested in accordance with detailed arrangements to be agreed by the Security Committee.

Reports

57. At the end of the assessment visit the main conclusions and recommendations shall be presented to the visited entity. Thereafter, a report on the assessment visit shall be drawn up. Where corrective action and recommendations have been proposed, sufficient details shall be included in the report to support the conclusions reached. The report shall be forwarded to the appropriate authority of the visited entity.
58. For assessment visits conducted in Member States' national administrations:

    (a) the draft assessment report will be forwarded to the NSA concerned to verify that it is factually correct and that it contains no information classified higher than RESTREINT UE/EU RESTRICTED; and

(b) unless the Member State NSA in question requests general distribution to be withheld, assessment reports shall be circulated to the Security Committee The report shall be classified RESTREINT UE/EU RESTRICTED.

A regular report shall be prepared under the responsibility of the GSC Security Authority (Security Office) to highlight the lessons learned from the assessment visits conducted in Member States over a specified period and examined by the Security Committee.

59. For assessment visits of third States and international organisations, the report shall be distributed to the Security Committee. The report shall be classified at least RESTREINT UE/EU RESTRICTED. Any corrective action shall be verified during a follow-up visit and reported to the Security Committee.
60. For assessment visits to any Union bodies, agencies and entities which apply this Decision or the principles thereof, assessment visit reports shall be distributed to the Security Committee. The draft assessment visit report shall be forwarded to the agency or body concerned to verify that it is factually correct and that it contains no information classified higher than RESTREINT UE/EU RESTRICTED. Any corrective action shall be verified during a follow up visit and reported to the Security Committee.
61. The GSC Security Authority shall conduct regular inspections of organisational entities in the GSC for the purposes laid down in paragraph 50.

Checklist

62. The GSC Security Authority (Security Office) shall draw up and update a checklist of items to be verified in the course of an assessment visit. This checklist shall be forwarded to the Security Committee.
63. The information to complete the checklist shall be obtained in particular during the visit from the security management of the entity being inspected. Once completed with the detailed responses, the checklist shall be classified in agreement with the inspected entity. It shall not form part of the inspection report.

ANNEX IV

PROTECTION OF EUCI HANDLED IN CIS

I. INTRODUCTION

1. This Annex sets out provisions for implementing Article 10.
2. The following IA properties and concepts are essential for the security and correct functioning of operations on CIS:

   Authenticity:
   the guarantee that information is genuine and from bona fide sources;

   Availability:
   the property of being accessible and usable upon request by an authorised entity;

   Confidentiality:
   the property that information is not disclosed to unauthorised individuals, entities or processes;

   Integrity:
   the property of safeguarding the accuracy and completeness of information and assets;

   Non-repudiation:
   the ability to prove an action or event has taken place, so that this event or action cannot subsequently be denied.

II. INFORMATION ASSURANCE PRINCIPLES

3. The provisions set out below shall form the baseline for the security of any CIS handling EUCI. Detailed requirements for implementing these provisions shall be defined in IA security policies and security guidelines.

Security risk management

4. Security risk management shall be an integral part of defining, developing, operating and maintaining CIS. Risk management (assessment, treatment, acceptance and communication) shall be conducted as an iterative process jointly by representatives of the system owners, project authorities, operating authorities and security approval authorities, using a proven, transparent and fully understandable risk assessment process. The scope of the CIS and its assets shall be clearly defined at the outset of the risk management process.
5. The competent authorities shall review the potential threats to CIS and shall maintain up-to-date and accurate threat assessments which reflect the current operational environment. They shall constantly update their knowledge of vulnerability issues and periodically review the vulnerability assessment to keep up with the changing information technology (IT) environment.
6. The aim of security risk treatment shall be to apply a set of security measures which results in a satisfactory balance between user requirements, cost and residual security risk.
7. The specific requirements, scale and the degree of detail determined by the relevant SAA for accrediting a CIS shall be commensurate with the assessed risk, taking account of all relevant factors, including the classification level of the EUCI handled in the CIS. Accreditation shall include a formal residual risk statement and acceptance of the residual risk by a responsible authority.

Security throughout the CIS life-cycle

8. Ensuring security shall be a requirement throughout the entire CIS life-cycle from initiation to withdrawal from service.
9. The role and interaction of each actor involved in a CIS with regard to its security shall be identified for each phase of the life-cycle.
10. Any CIS, including its technical and non-technical security measures, shall be subject to security testing during the accreditation process to ensure that the appropriate level of assurance is obtained and to verify that they are correctly implemented, integrated and configured.
11. Security assessments, inspections and reviews shall be performed periodically during the operation and maintenance of a CIS and when exceptional circumstances arise.

12. Security documentation for a CIS shall evolve over its life-cycle as an integral part of the process of change and configuration management.

Best practice

13. The GSC and the Member States shall cooperate to develop best practice for protecting EUCI handled on CIS. Best practice guidelines shall set out technical, physical, organisational and procedural security measures for CIS with proven effectiveness in countering given threats and vulnerabilities.
14. The protection of EUCI handled on CIS shall draw on lessons learned by entities involved in IA within and outside the Union.
15. The dissemination and subsequent implementation of best practice shall help achieve an equivalent level of assurance for the various CIS operated by the GSC and by Member States which handle EUCI.

Defence in depth

16. To mitigate risk to CIS, a range of technical and non-technical security measures, organised as multiple layers of defence, shall be implemented. These layers shall include:

    (a) Deterrence: security measures aimed at dissuading any adversary planning to attack the CIS;

    (b) Prevention: security measures aimed at impeding or blocking an attack on the CIS;

    (c) Detection: security measures aimed at discovering the occurrence of an attack on the CIS;

    (d) Resilience: security measures aimed at limiting impact of an attack to a minimum set of information or CIS assets and preventing further damage; and

    (e) Recovery: security measures aimed at regaining a secure situation for the CIS.

    The degree of stringency of such security measures shall be determined following a risk assessment.

17. The NSA or other competent authority shall ensure that:

(a) cyber defence capabilities are implemented to respond to threats which may transcend organisational and national boundaries; and

(b) responses are coordinated and information about these threats, incidents and the related risk is shared (computer emergency response capabilities).

Principle of minimality and least privilege

18. Only the essential functionalities, devices and services to meet operational requirements shall be implemented in order to avoid unnecessary risk.
19. CIS users and automated processes shall be given only the access, privileges or authorisations they require to perform their tasks in order to limit any damage resulting from accidents, errors, or unauthorised use of CIS resources.
20. Registration procedures performed by a CIS, where required, shall be verified as part of the accreditation process.

Information Assurance awareness

21. Awareness of the risks and available security measures is the first line of defence for the security of CIS. In particular all personnel involved in the life-cycle of CIS, including users, shall understand:

(a) that security failures may significantly harm the CIS;

(b) the potential harm to others which may arise from interconnectivity and interdependency; and

(c) their individual responsibility and accountability for the security of CIS according to their roles within the systems and processes.

22. To ensure that security responsibilities are understood, IA education and awareness training shall be mandatory for all personnel involved, including senior management and CIS users.

Evaluation and approval of IT-security products

23. The required degree of confidence in the security measures, defined as a level of assurance, shall be determined following the outcome of the risk management process and in line with the relevant security policies and security guidelines.

24. The level of assurance shall be verified by using internationally recognised or nationally approved processes and methodologies. This includes primarily evaluation, controls and auditing.
25. Cryptographic products for protecting EUCI shall be evaluated and approved by a national CAA of a Member State.
26. Prior to being recommended for approval by the Council or the Secretary-General in accordance with Article 10(6), such cryptographic products shall have undergone a successful second party evaluation by an Appropriately Qualified Authority (AQUA) of a Member State not involved in the design or manufacture of the equipment. The degree of detail required in a second party evaluation shall depend on the envisaged maximum classification level of EUCI to be protected by these products. The Council shall approve a security policy on the evaluation and approval of cryptographic products.
27. Where warranted on specific operational grounds, the Council or the Secretary-General as appropriate may, upon recommendation by the Security Committee, waive the requirements under paragraphs 25 or 26 of this Annex and grant an interim approval for a specific period in accordance with the procedure laid down in Article 10(6).
28. The Council, acting upon recommendation by the Security Committee, may accept the evaluation, selection and approval process of cryptographic products of a third State or international organisation and accordingly deem such cryptographic products approved for protecting EUCI released to that third state or international organisation.
29. An AQUA shall be a CAA of a Member State that has been accredited on the basis of criteria laid down by the Council to undertake the second evaluation of cryptographic products for protecting EUCI.
30. The Council shall approve a security policy on the qualification and approval of non-cryptographic IT security products.

Transmission within Secured and Administrative Areas

31. Notwithstanding the provisions of this Decision, when transmission of EUCI is confined within Secured Areas or Administrative Areas, unencrypted transmission or encryption at a lower level may be used based on the outcome of a risk management process and subject to the approval of the SAA.

Secure interconnection of CIS

32. For the purposes of this Decision, an interconnection shall mean the direct connection of two or more IT systems for the purpose of sharing data and other information resources (e.g. communication) in a unidirectional or multidirectional way.
33. A CIS shall treat any interconnected IT system as untrusted and shall implement protective measures to control the exchange of classified information.
34. For all interconnections of CIS with another IT system the following basic requirements shall be met:

    (a) business or operational requirements for such interconnections shall be stated and approved by the competent authorities;

    (b) the interconnection shall undergo a risk management and accreditation process and shall require the approval of the competent SAAs; and

    (c) Boundary Protection Services (BPS) shall be implemented at the perimeter of all CIS.
35. There shall be no interconnection between an accredited CIS and an unprotected or public network, except where the CIS has approved BPS installed for such a purpose between the CIS and the unprotected or public network. The security measures for such interconnections shall be reviewed by the competent IAA and approved by the competent SAA.

    When the unprotected or public network is used solely as a carrier and the data is encrypted by a cryptographic product approved in accordance with Article 10, such a connection shall not be deemed to be an interconnection.
36. The direct or cascaded interconnection of a CIS accredited to handle TRÈS SECRET UE/EU TOP SECRET to an unprotected or public network shall be prohibited.

Computer storage media

37. Computer storage media shall be destroyed in accordance with procedures approved by the competent security authority.
38. Computer storage media shall be reused, downgraded or declassified in accordance with security guidelines to be established pursuant to Article 6(2).

Emergency circumstances

39. Notwithstanding the provisions of this Decision, the specific procedures described below may be applied in an emergency, such as during impending or actual crisis, conflict, war situations or in exceptional operational circumstances.
40. EUCI may be transmitted using cryptographic products which have been approved for a lower classification level or without encryption with the consent of the competent authority if any delay would cause harm clearly outweighing the harm entailed by any disclosure of the classified material and if:

    (a) the sender and recipient do not have the required encryption facility or have no encryption facility; and

    (b) the classified material cannot be conveyed in time by other means.
41. Classified information transmitted under the circumstances set out in paragraph 39 shall not bear any markings or indications distinguishing it from information which is unclassified or which can be protected by an available cryptographic product. Recipients shall be notified of the classification level, without delay, by other means.
42. Should recourse be made to paragraph 39 a subsequent report shall be made to the competent authority and to the Security Committee.

III. INFORMATION ASSURANCE FUNCTIONS AND AUTHORITIES

43. The following IA functions shall be established in the Member States and the GSC. These functions do not require single organisational entities. They shall have separate mandates. However, these functions, and their accompanying responsibilities, may be combined or integrated in the same organisational entity or split into different organisational entities, provided that internal conflicts of interests or tasks are avoided.

Information Assurance Authority

44. The IAA shall be responsible for:

(a) developing IA security policies and security guidelines and monitoring their effectiveness and pertinence;

(b) safeguarding and administering technical information related to cryptographic products;

(c) ensuring that IA measures selected for protecting EUCI comply with the relevant policies governing their eligibility and selection;

(d) ensuring that cryptographic products are selected in compliance with policies governing their eligibility and selection;

(e) coordinating training and awareness on IA;

(f) consulting with the system provider, the security actors and representatives of users in respect to IA security policies and security guidelines; and

(g) ensuring appropriate expertise is available in the expert sub-area of the Security Committee for IA issues.

TEMPEST Authority

45. The TEMPEST Authority (TA) shall be responsible for ensuring compliance of CIS with TEMPEST policies and guidelines. It shall approve TEMPEST countermeasures for installations and products to protect EUCI to a defined level of classification in its operational environment.

Crypto Approval Authority

46. The Crypto Approval Authority (CAA) shall be responsible for ensuring that cryptographic products comply with national cryptographic policy or the Council's cryptographic policy. It shall grant the approval of a cryptographic product to protect EUCI to a defined level of classification in its operational environment. As regards the Member States, the CAA shall in addition be responsible for evaluating cryptographic products.

Crypto Distribution Authority

47. The Crypto Distribution Authority (CDA) shall be responsible for:

(a) managing and accounting for EU crypto material;

(b) ensuring that appropriate procedures are enforced and channels established for accounting, secure handling, storage and distribution of all EU crypto material; and

(c) ensuring the transfer of EU crypto material to or from individuals or services using it.

Security Accreditation Authority

48. The SAA for each system shall be responsible for:

(a) ensuring that CIS comply with the relevant security policies and security guidelines, providing a statement of approval for CIS to handle EUCI to a defined level of classification in its operational environment, stating the terms and conditions of the accreditation, and criteria under which re-approval is required;

(b) establishing a security accreditation process, in accordance with the relevant policies, clearly stating the approval conditions for CIS under its authority;

(c) defining a security accreditation strategy setting out the degree of detail for the accreditation process commensurate with the required level of assurance;

(d) examining and approving security-related documentation, including risk management and residual risk statements, system-specific security requirement statements ('SSRSs'), security implementation verification documentation and security operating procedures ('SecOPs'), and ensuring that it complies with the Council's security rules and policies;

(e) checking implementation of security measures in relation to the CIS by undertaking or sponsoring security assessments, inspections or reviews;

(f) defining security requirements (e.g. personnel clearance levels) for sensitive positions in relation to the CIS;

(g) endorsing the selection of approved cryptographic and TEMPEST products used to provide security for a CIS;

(h) approving, or where relevant, participating in the joint approval of the interconnection of a CIS to other CIS; and

(i) consulting the system provider, the security actors and representatives of the users with respect to security risk management, in particular the residual risk, and the terms and conditions of the approval statement.

49. The GSC SAA shall be responsible for accrediting all CIS operating within the remit of the GSC.
50. The relevant SAA of a Member State shall be responsible for accrediting CIS and components thereof operating within the remit of a Member State.
51. A joint Security Accreditation Board (SAB) shall be responsible for accrediting CIS within the remit of both the GSC SAA and Member States' SAAs. It shall be composed of an SAA representative from each Member State and be attended by an SAA representative of the Commission. Other entities with nodes on a CIS shall be invited to attend when that system is under discussion.

    The SAB shall be chaired by a representative of the GSC SAA. It shall act by consensus of SAA representatives of institutions, Member States and other entities with nodes on the CIS. It shall make periodic reports on its activities to the Security Committee and shall notify all accreditation statements to it.

Information Assurance Operational Authority

52. The IA Operational Authority for each system shall be responsible for:

    (a) developing security documentation in line with security policies and security guidelines, in particular the SSRS including the residual risk statement, the SecOPs and the crypto plan within the CIS accreditation process;

    (b) participating in selecting and testing the system-specific technical security measures, devices and software, to supervise their implementation and to ensure that they are securely installed, configured and maintained in accordance with the relevant security documentation;

(c) participating in selecting TEMPEST security measures and devices if required in the SSRS and ensuring that they are securely installed and maintained in cooperation with the TA;

(d) monitoring implementation and application of the SecOps and, where appropriate, delegating operational security responsibilities to the system owner;

(e) managing and handling cryptographic products, ensuring the custody of crypto and controlled items and, if so required, ensuring the generation of cryptographic variables;

(f) conducting security analysis reviews and tests, in particular to produce the relevant risk reports, as required by the SAA;

(g) providing CIS-specific IA training; and

(h) implementing and operating CIS-specific security measures.

ANNEX V

INDUSTRIAL SECURITY

I. INTRODUCTION

1. This Annex sets out provisions for implementing Article 11. It lays down general security provisions applicable to industrial or other entities in pre-contract negotiations and throughout the life-cycle of classified contracts let by the GSC.
2. The Council shall approve guidelines on industrial security outlining in particular detailed requirements regarding FSCs, Security Aspects Letters (SALs), visits, transmission and carriage of EUCI.

II. SECURITY ELEMENTS IN A CLASSIFIED CONTRACT

Security classification guide (SCG)

3. Prior to launching a call for tender or letting a classified contract, the GSC, as the contracting authority, shall determine the security classification of any information to be provided to bidders and contractors, as well as the security classification of any information to be created by the contractor. For that purpose, the GSC shall prepare an SCG to be used for the performance of the contract.
4. In order to determine the security classification of the various elements of a classified contract, the following principles shall apply:

   (a) in preparing an SCG, the GSC shall take into account all relevant security aspects, including the security classification assigned to information provided and approved to be used for the contract by the originator of the information;

   (b) the overall level of classification of the contract may not be lower than the highest classification of any of its elements; and

(c) where relevant, the GSC shall liaise with the Member States' NSAs/DSAs or any other competent security authority concerned in the event of any changes regarding the classification of information created by or provided to contractors in the performance of a contract and when making any subsequent changes to the SCG.

Security aspects letter (SAL)

5. The contract-specific security requirements shall be described in a SAL. The SAL shall, where appropriate, contain the SCG and shall be an integral part of a classified contract or sub-contract.
6. The SAL shall contain the provisions requiring the contractor and/or subcontractor to comply with the minimum standards laid down in this Decision. Non-compliance with these minimum standards may constitute sufficient grounds for the contract to be terminated.

Programme/Project Security Instructions (PSI)

7. Depending on the scope of programmes or projects involving access to or handling or storage of EUCI, specific PSI may be prepared by the contracting authority designated to manage the programme or project. The PSI shall require the approval of the Member States' NSAs/DSAs or any other competent security authority participating in the PSI and may contain additional security requirements.

III. FACILITY SECURITY CLEARANCE (FSC)

8. An FSC shall be granted by the NSA or DSA or any other competent security authority of a Member State to indicate, in accordance with national laws and regulations, that an industrial or other entity can protect EUCI at the appropriate classification level (CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET) within its facilities. It shall be presented to the GSC, as the contracting authority, before a contractor or subcontractor or potential contractor or subcontractor may be provided with or granted access to EUCI.

9. When issuing an FSC, the relevant NSA or DSA shall, as a minimum:

   (a) evaluate the integrity of the industrial or other entity;

   (b) evaluate ownership, control, or the potential for undue influence that may be considered a security risk;

   (c) verify that the industrial or any other entity has established a security system at the facility which covers all appropriate security measures necessary for the protection of information or material classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET in accordance with the requirements laid down in this Decision;

   (d) verify that the personnel security status of management, owners and employees who are required to have access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET has been established in accordance with the requirements laid down in this Decision; and

   (e) verify that the industrial or any other entity has appointed a Facility Security Officer who is responsible to its management for enforcing the security obligations within such an entity.
10. Where relevant, the GSC, as the contracting authority, shall notify the appropriate NSA/DSA or any other competent security authority that an FSC is required in the pre-contractual stage or for performing the contract. An FSC or PSC shall be required in the pre-contractual stage where EUCI classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET has to be provided in the course of the bidding process.
11. The contracting authority shall not award a classified contract with a preferred bidder before having received confirmation from the NSA/DSA or any other competent security authority of the Member State in which the contractor or subcontractor concerned is registered that, where required, an appropriate FSC has been issued.
12. The NSA/DSA or any other competent security authority which has issued an FSC shall notify the GSC as contracting authority about changes affecting the FSC. In the case of a sub-contract, the NSA/DSA or any other competent security authority shall be informed accordingly.

13. Withdrawal of an FSC by the relevant NSA/DSA or any other competent security authority shall constitute sufficient grounds for the GSC, as the contracting authority, to terminate a classified contract or exclude a bidder from the competition.

IV. CLASSIFIED CONTRACTS AND SUB-CONTRACTS

14. Where EUCI is provided to a bidder at the pre-contractual stage, the invitation to bid shall contain a provision obliging the bidder which fails to submit a bid or which is not selected to return all classified documents within a specified period of time.
15. Once a classified contract or sub-contract has been awarded, the GSC, as the contracting authority, shall notify the contractor's or subcontractor's NSA/DSA or any other competent security authority about the security provisions of the classified contract.
16. When such contracts are terminated, the GSC, as the contracting authority (and/or the NSA/DSA or any other competent security authority, as appropriate, in the case of a sub-contract) shall promptly notify the NSA/DSA or any other competent security authority of the Member State in which the contractor or subcontractor is registered.
17. As a general rule, the contractor or subcontractor shall be required to return to the contracting authority, upon termination of the classified contract or sub-contract, any EUCI held by it.
18. Specific provisions for the disposal of EUCI during the performance of the contract or upon its termination shall be laid down in the SAL.
19. Where the contractor or subcontractor is authorised to retain EUCI after termination of a contract, the minimum standards contained in this Decision shall continue to be complied with and the confidentiality of EUCI shall be protected by the contractor or subcontractor.
20. The conditions under which the contractor may subcontract shall be defined in the call for tender and in the contract.
21. A contractor shall obtain permission from the GSC, as the contracting authority, before sub-contracting any parts of a classified contract. No subcontract may be awarded to industrial or other entities registered in a non-EU Member State which has not concluded a security of information Agreement with the Union.

22. The contractor shall be responsible for ensuring that all sub-contracting activities are undertaken in accordance with the minimum standards laid down in this Decision and shall not provide EUCI to a subcontractor without the prior written consent of the contracting authority.
23. With regard to EUCI created or handled by the contractor or subcontractor, the rights incumbent on the originator shall be exercised by the contracting authority.

V. VISITS IN CONNECTION WITH CLASSIFIED CONTRACTS

24. Where the GSC, contractors' or subcontractors' personnel require access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET in each other's premises for the performance of a classified contract, visits shall be arranged in liaison with the NSAs/DSAs or any other competent security authority concerned. However, in the context of specific projects, the NSAs/DSAs may also agree on a procedure whereby such visits can be arranged directly.
25. All visitors shall hold an appropriate PSC and have a 'need-to-know' for access to the EUCI related to the GSC contract.
26. Visitors shall be given access only to EUCI related to the purpose of the visit.

VI. TRANSMISSION AND CARRIAGE OF EUCI

27. With regard to the transmission of EUCI by electronic means, the relevant provisions of Article 10 and Annex IV shall apply.
28. With regard to the carriage of EUCI, the relevant provisions of Annex III shall apply, in accordance with national laws and regulations.

29. For the transport of classified material as freight, the following principles shall be applied when determining security arrangements:

(a) security shall be assured at all stages during transportation from the point of origin to the final destination;

(b) the degree of protection afforded to a consignment shall be determined by the highest classification level of material contained within it;

(c) an FSC at the appropriate level shall be obtained for companies providing transportation. In such cases, personnel handling the consignment shall be security cleared in accordance with Annex I;

(d) prior to any cross-border movement of material classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET, a transportation plan shall be drawn up by the consignor and approved by the NSA/DSAs or any other competent security authority concerned;

(e) journeys shall be point to point to the extent possible, and shall be completed as quickly as circumstances permit; and

(f) whenever possible, routes should be only through Member States. Routes through States other than Member States should only be undertaken when authorised by the NSA/DSA or any other competent security authority of the States of both the consignor and the consignee.

VII. TRANSFER OF EUCI TO CONTRACTORS LOCATED IN THIRD STATES

30. EUCI shall be transferred to contractors and subcontractors located in third States in accordance with security measures agreed between the GSC, as the contracting authority, and the NSA/DSA of the concerned third State where the contractor is registered.

VIII INFORMATION CLASSIFIED RESTREINT UE/EU RESTRICTED

31. In liaison, as appropriate, with the NSA/DSA of the Member State the GSC, as the contracting authority, shall be entitled to conduct inspections of contractors'/subcontractors' facilities on the basis of contractual provisions in order to verify that the relevant security measures for the protection of EUCI at the level RESTREINT UE/EU RESTRICTED as required under the contract have been put in place.
32. To the extent necessary under national laws and regulations, NSAs/DSAs or any other competent security authority shall be notified by the GSC as the contracting authority of contracts or subcontracts containing information classified RESTREINT UE/EU RESTRICTED.
33. An FSC or a PSC for contractors or subcontractors and their personnel shall not be required for contracts let by the GSC containing information classified RESTREINT UE/EU RESTRICTED.
34. The GSC, as the contracting authority, shall examine the responses to invitations to tender for contracts which require access to information classified RESTREINT UE/EU RESTRICTED, notwithstanding any requirement relating to FSC or PSC which may exist under national laws and regulations.
35. The conditions under which the contractor may subcontract shall be in accordance with paragraph 21.
36. Where a contract involves handling information classified RESTREINT UE/EU RESTRICTED in a CIS operated by a contractor, the GSC as contracting authority shall ensure that the contract or any subcontract specifies the necessary technical and administrative requirements regarding accreditation of the CIS commensurate with the assessed risk, taking account of all relevant factors. The scope of accreditation of such CIS shall be agreed between the contracting authority and the relevant NSA/DSA.

ANNEX VI

EXCHANGE OF CLASSIFIED INFORMATION WITH THIRD STATES AND INTERNATIONAL ORGANISATIONS

I. INTRODUCTION

1. This Annex sets out provisions for implementing Article 13.

II. FRAMEWORKS GOVERNING THE EXCHANGE OF CLASSIFIED INFORMATION

2. Where the Council determines that a long-term need exists to exchange classified information,

   – a security of information agreement shall be concluded, or

   – an administrative arrangement shall be entered into,

   in accordance with Article 13(2) and Sections III and IV and based on a recommendation from the Security Committee.
3. Where EUCI generated for the purposes of a CSDP operation is to be provided to third States or international organisations participating in such an operation, and where neither of the frameworks referred to in paragraph 2 exists, the exchange of EUCI with the contributing third State or international organisation shall be regulated, in accordance with Section V, under:

   – a framework participation agreement,

   – an ad hoc participation agreement, or

   – in the absence of either of the above, an ad hoc administrative arrangement.
4. In the absence of a framework referred to in paragraphs 2 and 3, and where a decision is taken to release EUCI to a third State or international organisation on an exceptional ad hoc basis in accordance with Section VI, written assurances shall be sought from the third State or international organisation concerned to ensure that it protects any EUCI released to it in accordance with the basic principles and minimum standards set out in this Decision.

III. SECURITY OF INFORMATION AGREEMENTS

5. Security of information agreements shall establish the basic principles and minimum standards governing the exchange of classified information between the Union and a third State or international organisation.
6. Security of information agreements shall provide for technical implementing arrangements to be agreed between the competent security authorities of the relevant Union institutions and bodies and the competent security authority of the third State or international organisation in question. Such arrangements shall take account of the level of protection provided by the security regulations, structures and procedures in place in the third State or international organisation concerned. They shall be approved by the Security Committee.
7. No EUCI shall be exchanged under a security of information agreement by electronic means unless explicitly provided for in the agreement or in corresponding technical implementing arrangements.
8. When the Council concludes a security of information agreement, a registry shall be designated in each party as the main point of entry and exit for classified information exchanges.
9. In order to assess the effectiveness of the security regulations, structures and procedures in the third State or international organisation concerned, assessment visits shall be conducted in mutual agreement with the third State or international organisation concerned. Such assessment visits shall be conducted in accordance with the relevant provisions of Annex III and shall evaluate:

   (a) the regulatory framework applicable for protecting classified information;

   (b) any specific features of the security policy and the way in which security is organised in the third State or international organisation which may have an impact on the level of classified information that may be exchanged;

   (c) the security measures and procedures actually in place; and

   (d) security clearance procedures for the level of EUCI to be released.
10. The team conducting an assessment visit on behalf of the Union shall assess whether the security regulations and procedures in the third State or international organisation in question are adequate for the protection of EUCI at a given level.

11. The findings of such visits shall be set out in a report on the basis of which the Security Committee shall determine the maximum level of EUCI which may be exchanged in hard copy, and where appropriate electronically, with the third party concerned as well as any specific conditions governing exchange with that party.
12. Every endeavour shall be made to conduct a full security assessment visit to the third State or international organisation in question before the Security Committee approves the implementing arrangements in order to establish the nature and the effectiveness of the security system in place. However, where this is not possible the Security Committee shall receive as full a report as possible from the GSC Security Office, based on the information available to it, informing the Security Committee about the security regulations applicable and the way in which security is organised in the third State or international organisation concerned.
13. The report on the assessment visit, or in the absence of such a report the report referred to in paragraph 12, shall be forwarded to, and deemed satisfactory by, the Security Committee before EUCI is actually released to the third State or international organisation in question.
14. The competent security authorities of the Union institutions and bodies shall communicate to the third State or international organisation the date as from when the Union is in a position to release EUCI under the agreement, as well as the maximum level of EUCI which may be exchanged in paper form or by electronic means.
15. Follow-up assessment visits shall be conducted as necessary, in particular if:

    (a) there is a need for the releasable level of EUCI to be raised;

    (b) the Union has been notified of fundamental changes in the third State or international organisation's security arrangements that might have an impact on how it protects EUCI; or

    (c) there has been a serious incident involving unauthorised disclosure of EUCI.

16. Once the security of information agreement is in force and classified information is exchanged with the third State or international organisation concerned, the Security Committee may decide to modify the maximum level of EUCI which may be exchanged in paper form or by electronic means, in particular in the light of any follow-up assessment visit.

IV. ADMINISTRATIVE ARRANGEMENTS

17. Where a long-term need exists to exchange information classified as a general rule no higher than RESTREINT UE/EU RESTRICTED with a third State or international organisation, and where the Security Committee has established that the party in question does not have a sufficiently developed security system for it to be possible to enter into a security of information agreement, the Secretary-General may, subject to approval by the Council, enter into an administrative arrangement on behalf of the GSC with the relevant authorities of the third State or international organisation in question.
18. Where, for urgent operational reasons, a framework for exchanging classified information needs to be put in place rapidly, exceptionally the Council may decide that an administrative arrangement be entered into for exchanging information of a higher classification level.
19. Administrative arrangements shall as a general rule take the form of an Exchange of Letters.
20. An assessment visit referred to in paragraph 9 shall be conducted and the report, or in the absence of such a report the report referred to in paragraph 12, forwarded to, and deemed satisfactory by, the Security Committee before EUCI is actually released to the third State or international organisation in question.
21. No EUCI shall be exchanged under an administrative arrangement by electronic means unless explicitly provided for in the arrangement.

V. EXCHANGE OF CLASSIFIED INFORMATION IN THE CONTEXT OF CSDP OPERATIONS

22. Framework participation agreements govern the participation of third States or international organisations in CSDP operations. Such agreements shall include provisions on the release of EUCI generated for the purposes of CSDP operations to the contributing third States or international organisations. The maximum classification level of EUCI which may be exchanged shall be RESTREINT UE/EU RESTRICTED for civilian CSDP operations and CONFIDENTIEL UE/EU CONFIDENTIAL for military CSDP operations, unless otherwise laid down in the Decision establishing each CSDP operation.
23. Ad hoc participation agreements concluded for a specific CSDP operation shall include provisions on the release of EUCI generated for the purposes of that operation to the contributing third State or international organisation. The maximum classification level of EUCI which may be exchanged shall be RESTREINT UE/EU RESTRICTED for civilian CSDP operations and CONFIDENTIEL UE/EU CONFIDENTIAL for military CSDP operations, unless otherwise laid down in the Decision establishing each CSDP operation.
24. In the absence of a security of information agreement and pending the conclusion of a participation agreement, the release of EUCI generated for the purposes of the operation to a third State or international organisation participating in the operation shall be governed by an administrative arrangement to be entered into by the High Representative or subject to a decision on ad hoc release in accordance with Section VI. EUCI shall only be exchanged under such an arrangement as long as the participation of the third State or international organisation is still envisaged. The maximum classification level of EUCI which may be exchanged shall be RESTREINT UE/EU RESTRICTED for civilian CSDP operations and CONFIDENTIEL UE/EU CONFIDENTIAL for military CSDP operations, unless otherwise laid down in the Decision establishing each CSDP operation.

25. The provisions on classified information to be included in framework participation agreements, ad hoc participation agreements and ad hoc administrative arrangements referred to in paragraphs 22 to 24 shall provide that the third State or international organisation in question shall ensure that its personnel seconded to any operation will protect EUCI in accordance with the Council's security rules and with further guidance issued by the competent authorities, including the operation's chain of command.
26. If a security of information agreement is subsequently concluded between the Union and a contributing third State or international organisation, the security of information agreement shall supersede the provisions on the exchange of classified information laid down in any framework participation agreement, ad hoc participation agreement or ad hoc administrative arrangement as far as the exchange and handling of EUCI is concerned.
27. No exchange of EUCI by electronic means shall be permitted under a framework participation agreement, ad hoc participation agreement or ad hoc administrative arrangement with a third State or international organisation, unless explicitly provided for in the agreement or arrangement in question.
28. EUCI generated for the purposes of a CSDP operation may be disclosed to personnel seconded to that operation by third States or international organisations in accordance with paragraphs 22 to 27. When authorising access to EUCI in premises or in CIS of a CSDP operation by such personnel, measures shall be applied (including recording of EUCI disclosed) to mitigate the risk of loss or compromise. Such measures shall be defined in relevant planning or mission documents.

29. In the absence of a security of information agreement, the release of EUCI, in the event of a specific and immediate operational need, to the host State on whose territory a CSDP operation is conducted, may be governed by an administrative arrangement to be entered into by the High Representative. This possibility shall be provided for in the Decision establishing the CSDP operation. EUCI released under such circumstances shall be restricted to that generated for the purposes of the CSDP operation and classified no higher than RESTREINT UE/EU RESTRICTED, unless a higher level of classification is laid down in the Decision establishing the CSDP operation. Under such an administrative arrangement, the host State shall be required to undertake to protect EUCI according to minimum standards which are no less stringent than those laid down in this Decision.
30. In the absence of a security of information agreement, the release of EUCI to relevant third States and international organisations, other than those participating in a CSDP operation, may be governed by an administrative arrangement to be entered into by the High Representative. Where appropriate, this possibility, as well as any conditions attached thereto, shall be provided for in the Decision establishing the CSDP operation. EUCI released under such circumstances shall be restricted to that generated for the purposes of the CSDP operation and classified no higher than RESTREINT UE/EU RESTRICTED, unless a higher level of classification is laid down in the Decision establishing the CSDP operation. Under such an administrative arrangement, the third State or international organisation in question shall be required to undertake to protect EUCI according to minimum standards which are no less stringent than those laid down in this Decision.
31. No implementing arrangements or assessment visits are required prior to implementing the provisions on release of EUCI in the context of paragraphs 22, 23 and 24.

VI. EXCEPTIONAL AD HOC RELEASE OF EUCI

32. Where no framework is in place in accordance with Sections III to V, and where the Council or one of its preparatory bodies determines the exceptional need to release EUCI to a third State or international organisation, the GSC shall:

    (a) to the extent possible, verify with the security authorities of the third State or international organisation concerned that its security regulations, structures and procedures are such that EUCI released to it will be protected to standards no less stringent than those laid down in this Decision; and

    (b) invite the Security Committee, on the basis of available information, to issue a recommendation regarding the confidence that can be placed in the security regulations, structures and procedures in the third State or international organisation to which the EUCI is to be released.
33. If the Security Committee issues a recommendation in favour of releasing the EUCI, the matter shall be referred to the Committee of Permanent Representatives (Coreper), which shall take a decision on its release.
34. If the Security Committee's recommendation is not in favour of releasing the EUCI:

    (a) for matters relating to CFSP/CSDP, the Political and Security Committee shall discuss the matter and formulate a recommendation for a decision by Coreper;

    (b) for all other matters, Coreper shall discuss the matter and take a decision.
35. Where deemed appropriate, and subject to the prior written consent of the originator, Coreper may decide that the classified information may be released only in part or only if downgraded or declassified beforehand, or that the information to be released shall be prepared without reference to the source or original EU classification level.
36. Following a decision to release EUCI, the GSC shall forward the document concerned, which shall bear a releasability marking indicating the third State or international organisation to which it has been released. Prior to or upon actual release, the third party in question shall undertake in writing to protect the EUCI it receives in accordance with the basic principles and minimum standards set out in this Decision.

VII. AUTHORITY TO RELEASE EUCI TO THIRD STATES OR INTERNATIONAL ORGANISATIONS

37. Where a framework exists in accordance with paragraph 2 for exchanging classified information with a third State or international organisation, the Council shall take a decision to authorise the Secretary-General to release EUCI, in accordance with the principle of originator's consent, to the third State or international organisation in question. The Secretary-General may delegate such authorisation to senior GSC officials.
38. Where a security of information agreement exists in accordance with paragraph 2, first indent, the Council may take a decision to authorise the High Representative to release EUCI originating in the Council in the area of the Common Foreign and Security Policy, after having obtained the consent of the originator of any source material contained therein, to the third State or international organisation in question. The High Representative may delegate such authorisation to senior EEAS officials or to EUSRs.
39. Where a framework exists in accordance with paragraph 2 or with paragraph 3 for exchanging classified information with a third State or international organisation, the High Representative shall be authorised to release EUCI, in accordance with the Decision establishing the CSDP operation and with the principle of originator's consent. The High Representative may delegate such authorisation to senior EEAS officials, to EU Operation, Force or Mission Commanders, or to Heads of EU Mission.

Appendices

Appendix A

Definitions

Appendix B

Equivalence of security classifications

Appendix C

List of national security authorities (NSAs)

Appendix D

List of abbreviations

Appendix A

DEFINITIONS

For the purposes of this Decision, the following definitions shall apply:
'Accreditation' means the process leading to a formal statement by the Security Accreditation Authority (SAA) that a system is approved to operate with a defined level of classification, in a particular security mode in its operational environment and at an acceptable level of risk, based on the premise that an approved set of technical, physical, organisational and procedural security measures has been implemented;
'Asset' means anything that is of value to an organisation, its business operations and their continuity, including information resources that support the organisation's mission;
'**Authorisation for access to EUCI'** means a decision by the GSC Appointing Authority taken on the basis of an assurance given by a competent authority of a Member State that a GSC official, other servant or seconded national expert may, provided his 'need-to-know' has been determined and he has been appropriately briefed on his responsibilities, be granted access to EUCI up to a specified level (CONFIDENTIEL UE/ EU CONFIDENTIAL or above) until a specified date;
'CIS life-cycle' means the entire duration of existence of a CIS, which includes initiation, conception, planning, requirements analysis, design, development, testing, implementation, operation, maintenance and decommissioning;
'Classified contract' means a contract entered into by the GSC with a contractor for the supply of goods, execution of works or provision of services, the performance of which requires or involves access to or the creation of EUCI;
'Classified subcontract' means a contract entered into by a contractor of the GSC with another contractor (i.e. the subcontractor) for the supply of goods, execution of works or provision of services, the performance of which requires or involves access to or the creation of EUCI;
'Communication and information system' (CIS) – see Article 10(2);
'Contractor' means an individual or legal entity possessing the legal capacity to undertake contracts;
'Cryptographic (Crypto) material' means cryptographic algorithms, cryptographic hardware and software modules, and products including implementation details and associated documentation and keying material;

'Cryptographic product' means a product whose primary and main functionality is the provision of security services (confidentiality, integrity, availability, authenticity, non-repudiation) through one or more cryptographic mechanisms;
'CSDP operation' means a military or civilian crisis management operation under Title V, Chapter 2, of the TEU;
'Declassification' means the removal of any security classification;
'Defence in depth' means the application of a range of security measures organised as multiple layers of defence;
'Designated Security Authority' (DSA) means an authority responsible to the National Security Authority (NSA) of a Member State which is responsible for communicating to industrial or other entities national policy on all matters of industrial security and for providing direction and assistance in its implementation. The function of DSA may be carried out by the NSA or by any other competent authority;
'Document' means any recorded information regardless of its physical form or characteristics;
'Downgrading' means a reduction in the level of security classification;
'EU classified information' (EUCI) – see Article 2(1);
'Facility Security Clearance' (FSC) means an administrative determination by an NSA or DSA that, from the security viewpoint, a facility can afford an adequate level of protection to EUCI of a specified security classification level;
'Handling' of EUCI means all possible actions to which EUCI may be subject throughout its life-cycle. It comprises its creation, processing, carriage, downgrading, declassification and destruction. In relation to CIS it also comprises its collection, display, transmission and storage;
'Holder' means a duly authorised individual with an established need-to-know who is in possession of an item of EUCI and is accordingly responsible for protecting it;
'Industrial or other entity' means an entity involved in supplying goods, executing works or providing services; this may be an industrial, commercial, service, scientific, research, educational or development entity or a self-employed individual;
'Industrial security' – see Article 11(1);
'Information Assurance' – see Article 10(1);
'Interconnection' – see Annex IV, paragraph 32;
'Management of classified information' – see Article 9(1);
'Material' means any document, data carrier or item of machinery or equipment, either manufactured or in the process of manufacture;

'Originator' means the Union institution, body or agency, Member State, third state or international organisation under whose authority classified information has been created and/or introduced into the Union's structures;

'Personnel security' – see Article 7(1);

'Personnel Security Clearance' (PSC) means a statement by a competent authority of a Member State which is made following completion of a security investigation conducted by the competent authorities of a Member State and which certifies that an individual may be granted access to EUCI up to a specified level (CONFIDENTIEL UE/EU CONFIDENTIAL or above) until a specified date;

'Personnel Security Clearance Certificate' (PSCC) means a certificate issued by a competent authority establishing that an individual is security cleared and holds a valid security clearance certificate or authorisation from the Appointing Authority for access to EUCI, and which shows the level of EUCI to which that individual may be granted access (CONFIDENTIEL UE/EU CONFIDENTIAL or above), the date of validity of the relevant PSC and the date of expiry of the certificate itself;

'Physical security' – see Article 8(1);

'Programme/Project Security Instruction' (PSI) means a list of security procedures which are applied to a specific programme/project in order to standardise security procedures. It may be revised throughout the programme/project;

'Registration' – see Annex III, paragraph 18;

'Residual risk' means the risk which remains after security measures have been implemented, given that not all threats are countered and not all vulnerabilities can be eliminated;

'Risk' means the potential that a given threat will exploit internal and external vulnerabilities of an organisation or of any of the systems it uses and thereby cause harm to the organisation and to its tangible or intangible assets. It is measured as a combination of the likelihood of threats occurring and their impact;

– **'Risk acceptance'** is the decision to agree to the further existence of a residual risk after risk treatment;

– **'Risk assessment'** consists of identifying threats and vulnerabilities and conducting the related risk analysis, i.e. the analysis of probability and impact;

– **'Risk communication'** consists of developing awareness of risks among CIS user communities, informing approval authorities such risks and reporting them to operating authorities;

– **'Risk treatment'** consists of mitigating, removing, reducing (through an appropriate combination of technical, physical, organisational or procedural measures), transferring or monitoring the risk;

'Security Aspects Letter' (SAL) means a set of special contractual conditions issued by the contracting authority which forms an integral part of any classified contract involving access to or the creation of EUCI, that identifies the security requirements or those elements of the contract requiring security protection;

'Security Classification Guide' (SCG) means a document which describes the elements of a programme or contract which are classified, specifying the applicable security classification levels. The SCG may be expanded throughout the life of the programme or contract and the elements of information may be re-classified or downgraded; where an SCG exists it shall be part of the SAL;

'Security investigation' means the investigative procedures conducted by the competent authority of a Member State in accordance with its national laws and regulations in order to obtain an assurance that nothing adverse is known which would prevent an individual from being granted a PSC or an authorisation for access to EUCI up to a specified level (CONFIDENTIEL UE/EU CONFIDENTIAL or above);

'Security mode of operation' means the definition of the conditions under which a CIS operates based on the classification of information handled and the clearance levels, formal access approvals, and need-to-know of its users. Four modes of operation exist for handling or transmitting classified information: dedicated mode, system-high mode, compartmented mode and multilevel mode:

– **'Dedicated mode'** means a mode of operation in which all individuals with access to the CIS are cleared to the highest classification level of information handled within the CIS, and with a common need-to-know for all of the information handled within the CIS;

– **'System-high mode'** means a mode of operation in which all individuals with access to the CIS are cleared to the highest classification level of information handled within the CIS, but not all individuals with access to the CIS have a common need-to-know for the information handled within the CIS; approval to access information may be granted by an individual;

– **'Compartmented mode'** means a mode of operation in which all individuals with access to the CIS are cleared to the highest classification level of information handled within the CIS, but not all individuals with access to the CIS have a formal authorisation to access all of the information handled within the CIS; formal authorisation implies a formal central management of access control as distinct from an individual's discretion to grant access;

– **'Multilevel mode'** means a mode of operation in which not all individuals with access to the CIS are cleared to the highest classification level of information handled within the CIS, and not all individuals with access to the CIS have a common need-to-know for the information handled within the CIS;

'Security risk management process' means the entire process of identifying, controlling and minimising uncertain events that may affect the security of an organisation or of any of the systems it uses. It covers the entirety of risk-related activities, including assessment, treatment, acceptance and communication;

'TEMPEST' means the investigation, study and control of compromising electromagnetic emanations and the measures to suppress them;

'Threat' means a potential cause of an unwanted incident which may result in harm to an organisation or any of the systems it uses; such threats may be accidental or deliberate (malicious) and are characterised by threatening elements, potential targets and attack methods;

'Vulnerability' means a weakness of any nature that can be exploited by one or more threats. A vulnerability may be an omission or it may relate to a weakness in controls in terms of their strength, completeness or consistency and may be of a technical, procedural, physical, organisational or operational nature.

Appendix B

EQUIVALENCE OF SECURITY CLASSIFICATIONS

EU	TRÈS SECRET UE/ EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Belgium	Très Secret (Loi 11.12.1998) Zeer Geheim (Wet 11.12.1998)	Secret (Loi 11.12.1998) Geheim (Wet 11.12.1998)	Confidentiel (Loi 11.12.1998) Vertrouwelijk (Wet 11.12.1998)	nota ([1]) below
Bulgaria	Строго секретно	Секретно	Поверително	За служебно ползване
Czech Republic	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Denmark	YDERST HEMMELIGT	HEMMELIGT	FORTROLIGT	TIL TJENESTEBRUG
Germany	STRENG GEHEIM	GEHEIM	VS ([2])– VERTRAULICH	VS – NUR FÜR DEN DIENSTGEBRAUCH
Estonia	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Ireland	Top Secret	Secret	Confidential	Restricted
Greece	Άκρως Απόρρητο Abr: ΑΑΠ	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Spain	SECRETO	RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
France	Très Secret Défense	Secret Défense	Confidentiel Défense	nota ([3]) below
Croatia	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Italy	Segretissimo	Segreto	Riservatissimo	Riservato
Cyprus	Άκρως Απόρρητο Abr: (ΑΑΠ)	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Latvia	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Lithuania	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Luxembourg	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Hungary	Szigorúan titkos!	Titkos!	Bizalmas!	Korlátozott terjesztésű!
Malta	L-Oġħla Segretezza Top Secret	Sigriet Secret	Kunfidenzjali Confidential	Ristrett Restricted ([4])

Netherlands	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Austria	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Poland	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugal	Muito Secreto	Secreto	Confidencial	Reservado
Romania	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu
Slovenia	STROGO TAJNO	TAJNO	ZAUPNO	INTERNO
Slovakia	Prísne tajné	Tajné	Dôverné	Vyhradené
Finland	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Sweden ([5])	HEMLIG/TOP SECRET HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG/SECRET HEMLIG	HEMLIG/CONFIDENTIAL HEMLIG	HEMLIG/RESTRICTED HEMLIG
United Kingdom	UK TOP SECRET	UK SECRET	UK CONFIDENTIAL	UK RESTRICTED

([1]) Diffusion Restreinte/Beperkte Verspreiding is not a security classification in Belgium. Belgium handles and protects 'RESTREINT UE/EU RESTRICTED' information in a manner no less stringent than the standards and procedures described in the security rules of the Council of the European Union.

([2]) Germany: VS = Verschlusssache.

([3]) France does not use the classification 'RESTREINT' in its national system. France handles and protects 'RESTREINT UE/EU RESTRICTED' information in a manner no less stringent than the standards and procedures described in the security rules of the Council of the European Union.

([4]) The Maltese and English markings for Malta can be used interchangeably

([5]) Sweden: the security classification markings in the top row are used by the defence authorities and the markings in the bottom row by other authorities.

Appendix C

LIST OF NATIONAL SECURITY AUTHORITIES (NSAs)

BELGIUM Autorité nationale de Sécurité SPF Affaires étrangères, Commerce extérieur et Coopération au Développement 15, rue des Petits Carmes 1000 Bruxelles Tel. Secretariat: +32 25014542 Fax +32 25014596 E-mail: nvo-ans@diplobel.fed.be	**ESTONIA** National Security Authority Department Estonian Ministry of Defence Sakala 1 15094 Tallinn Tel. +372 717 0019, +372 7170117 Fax +372 7170213 E-mail: nsa@mod.gov.ee
BULGARIA State Commission on Information Security 90 Cherkovna Str. 1505 Sofia Tel. +359 29333600 Fax +359 29873750 E-mail: dksi@government.bg Website: www.dksi.bg	**IRELAND** National Security Authority Department of Foreign Affairs 76 - 78 Harcourt Street Dublin 2 Tel. +353 14780822 Fax +353 14082959
CZECH REPUBLIC Národní bezpečnostní úřad (National Security Authority) Na Popelce 2/16 150 06 Praha 56 Tel. +420 257283335 Fax +420 257283110 E-mail: czech.nsa@nbu.cz Website: www.nbu.cz	**GREECE** Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ) Διεύθυνση Ασφαλείας και Αντιπληροφοριών ΣΤΓ 1020 -Χολαργός (Αθήνα) Ελλάδα Τηλ.: +30 2106572045 (ώρες γραφείου) +30 2106572009 (ώρες γραφείου) Φαξ: +30 2106536279 +30 2106577612 Hellenic National Defence General Staff (HNDGS) Counter Intelligence and Security Directorate (NSA) 227-231 HOLARGOS STG 1020 ATHENS Tel. +30 2106572045 +30 2106572009 Fax +30 2106536279 +30 2106577612

DENMARK Politiets Efterretningstjeneste (Danish Security Intelligence Service) Klausdalsbrovej 1 2860 Søborg Tel. +45 33148888 Fax +45 33430190 Forsvarets Efterretningstjeneste (Danish Defence Intelligence Service) Kastellet 30 2100 Copenhagen Ø Tel. +45 33325566 Fax +45 33931320	**SPAIN** Autoridad Nacional de Seguridad Oficina Nacional de Seguridad Avenida Padre Huidobro s/n 28023 Madrid Tel. +34 913725000 Fax +34 913725808 E-mail: nsa-sp@areatec.com
GERMANY Bundesministerium des Innern Referat ÖS III 3 Alt-Moabit 101 D D-11014 Berlin Tel. +49 30186810 Fax +49 30186811441 E-mail: oesIII3@bmi.bund.de	**FRANCE** Secrétariat général de la défense et de la sécurité nationale Sous-direction Protection du secret (SGDSN/PSD) 51 Boulevard de la Tour-Maubourg 75700 Paris 07 SP Tel. +33 171758177 Fax +33 171758200
CROATIA Office of the National Security Council Croatian NSA Jurjevska 34 10000 Zagreb Croatia Tel. +385 14681222 Fax +385 14686049 www.uvns.hr	**LUXEMBOURG** Autorité nationale de Sécurité Boîte postale 2379 1023 Luxembourg Tel. +352 24782210 central +352 24782253 direct Fax +352 24782243
ITALY Presidenza del Consiglio dei Ministri D.I.S. - U.C.Se Via di Santa Susanna, 15 00187 Roma Tel. +39 0661174266 Fax +39 064885273	**HUNGARY** Nemzeti Biztonsági Felügyelet (National Security Authority of Hungary) H-1024 Budapest, Szilágyi Erzsébet fasor 11/B Tel. +36 (1) 7952303 Fax +36 (1) 7950344 Postal address: H-1357 Budapest, PO Box 2 E-mail: nbf@nbf.hu Website: www.nbf.hu

CYPRUS ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ Εθνική Αρχή Ασφάλειας (ΕΑΑ) Υπουργείο Άμυνας Λεωφόρος Εμμανουήλ Ροΐδη 4 1432 Λευκωσία, Κύπρος Τηλέφωνα: +357 22807569, +357 22807643, +357 22807764 Τηλεομοιότυπο: +357 22302351 Ministry of Defence Minister's Military Staff National Security Authority (NSA) 4 Emanuel Roidi street 1432 Nicosia Tel. +357 22807569, +357 22807643, +357 22807764 Fax +357 22302351 E-mail: cynsa@mod.gov.cy	**MALTA** Ministry for Home Affairs and National Security P.O. Box 146 MT-Valletta Tel. +356 21249844 Fax +356 25695321
LATVIA National Security Authority Constitution Protection Bureau of the Republic of Latvia P.O.Box 286 LV-1001 Riga Tel. +371 67025418 Fax +371 67025454 E-mail: ndi@sab.gov.lv	**NETHERLANDS** Ministerie van Binnenlandse Zaken en Koninkrijksrelaties Postbus 20010 2500 EA Den Haag Tel. +31 703204400 Fax +31 703200733 Ministerie van Defensie Beveiligingsautoriteit Postbus 20701 2500 ES Den Haag Tel. +31 703187060 Fax +31 703187522
LITHUANIA Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija (The Commission for Secrets Protection Coordination of the Republic of Lithuania National Security Authority) Gedimino 40/1 LT-01110 Vilnius Tel. +370 706 66701, +370 706 66702 Fax +370 706 66700 E-mail: nsa@vsd.lt	**AUSTRIA** Informationssicherheitskommission Bundeskanzleramt Ballhausplatz 2 1014 Wien Tel. +43 1531152594 Fax +43 1531152615 E-mail: ISK@bka.gv.at

POLAND Agencja Bezpieczeństwa Wewnętrznego – ABW (Internal Security Agency) 2A Rakowiecka St. 00-993 Warszawa Tel. +48 225857360 Fax +48 225858509 E-mail: nsa@abw.gov.pl Website: www.abw.gov.pl	**SLOVAKIA** Národný bezpečnostný úrad (National Security Authority) Budatínska 30 P.O. Box 16 850 07 Bratislava Tel. +421 268692314 Fax +421 263824005 Website: www.nbusr.sk
PORTUGAL Presidência do Conselho de Ministros Autoridade Nacional de Segurança Rua da Junqueira, 69 1300-342 Lisboa Tel. +351 213031710 Fax +351 213031711	**FINLAND** National Security Authority Ministry for Foreign Affairs P.O. Box 453 FI-00023 Government Tel. +358 16055890 Fax +358 916055140 E-mail: NSA@formin.fi
ROMANIA Oficiul Registrului Național al Informațiilor Secrete de Stat (Romanian NSA – ORNISS National Registry Office for Classified Information) Strada Mureș nr. 4 012275 Bucharest Tel. +40 212245830 Fax +40 212240714 E-mail: nsa.romania@nsa.ro Website: www.orniss.ro	**SWEDEN** Utrikesdepartementet (Ministry for Foreign Affairs) UD-RS S 10339 Stockholm Tel. +46 84051000 Fax +46 87231176 E-mail: ud-nsa@foreign.ministry.se
SLOVENIA Urad Vlade RS za varovanje tajnih podatkov Gregorčičeva 27 1000 Ljubljana Tel. +386 14781390 Fax +386 14781399 E-mail: gp.uvtp@gov.si	**UNITED KINGDOM** UK National Security Authority Room 335, 3rd Floor 70 Whitehall London SW1A 2AS Tel. 1: +44 2072765645 Tel. 2: +44 2072765497 Fax +44 2072765651 E-mail: UK-NSA@cabinet-office.x.gsi.gov.uk

Appendix D

LIST OF ABBREVIATIONS

Acronym	Meaning
AQUA	Appropriately Qualified Authority
BPS	Boundary Protection Services
CAA	Crypto Approval Authority
CCTV	Closed Circuit Television
CDA	Crypto Distribution Authority
CFSP	Common Foreign and Security Policy
CIS	Communication and Information Systems handling EUCI
Coreper	Committee of Permanent Representatives
CSDP	Common Security and Defence Policy
DSA	Designated Security Authority
ECSD	European Commission Security Directorate
EUCI	EU Classified Information
EUSR	EU Special Representative
FSC	Facility Security Clearance
GSC	General Secretariat of the Council
IA	Information Assurance
IAA	Information Assurance Authority
IDS	Intrusion Detection System
IT	Information Technology
NSA	National Security Authority
PSC	Personnel Security Clearance
PSCC	Personnel Security Clearance Certificate
PSI	Programme/Project Security Instructions
SAA	Security Accreditation Authority
SAB	Security Accreditation Board
SAL	Security Aspects Letter
SecOPs	Security Operating Procedures
SCG	Security Classification Guide
SSRS	System-Specific Security Requirement Statement
TA	TEMPEST Authority

2.7. 2019 M. GRUODŽIO 19 D. TARYBOS SPRENDIMAS (ES) 2019/2247, KURIUO IŠ DALIES KEIČIAMAS SPRENDIMAS 2013/488/ES DĖL ES ĮSLAPTINTOS INFORMACIJOS APSAUGAI UŽTIKRINTI SKIRTŲ SAUGUMO TAISYKLIŲ

TARYBOS SPRENDIMAS (ES) 2019/2247

2019 m. gruodžio 19 d.

kuriuo iš dalies keičiamas Sprendimas 2013/488/ES dėl ES įslaptintos informacijos apsaugai užtikrinti skirtų saugumo taisyklių

EUROPOS SĄJUNGOS TARYBA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo, ypač į jos 240 straipsnio 3 dalį,

atsižvelgdama į 2009 m. gruodžio 1 d. Tarybos sprendimą 2009/937/ES, patvirtinantį Tarybos darbo tvarkos taisykles ([1]), ypač į jo 24 straipsnį,

kadangi:

(1) Tarybos sprendimo 2013/488/ES ([2]) B priedėlyje yra pateikta slaptumo žymų atitikmenų lentelė;
(2) to sprendimo C priedėlyje pateiktas nacionalinių saugumo institucijų (NSI) sąrašas;
(3) Švedija pranešė Tarybos generaliniam sekretoriatui apie savo slaptumo žymų ir NSI pasikeitimus;
(4) be to, Bulgarija, Čekija, Danija, Vokietija, Estija, Airija, Ispanija, Kroatija, Kipras, Latvija, Lietuva, Vengrija, Austrija, Lenkija, Rumunija, Slovakija, Suomija ir Jungtinė Karalystė pranešė Tarybos generaliniam sekretoriatui apie savo atitinkamų NSI pasikeitimus;
(5) todėl Sprendimas 2013/488/ES turėtų būti atitinkamai iš dalies pakeistas,

PRIĖMĖ ŠĮ SPRENDIMĄ:

1 straipsnis

Sprendimo 2013/488/ES B ir C priedėliai pakeičiami šio sprendimo I ir II prieduose esančiu tekstu.

2 straipsnis

Šis sprendimas įsigalioja jo paskelbimo dieną.

Priimta Briuselyje 2019 m. gruodžio 19 d.

Tarybos vardu

Pirmininkė

K. MIKKONEN

([1]) OL L 325, 2009 12 11, p. 35.

([2]) 2013 m. rugsėjo 23 d. Tarybos sprendimas 2013/488/ES dėl ES įslaptintos informacijos apsaugai užtikrinti skirtų saugumo taisyklių (OL L 274, 2013 10 15, p. 1).

I PRIEDAS

B priedėlis

SLAPTUMO ŽYMŲ ATITIKMENYS

ES	TRÈS SECRET UE/EU TOP SECRET	SECRET UE/ EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Belgija	Très Secret (Loi 11.12.1998) Zeer Geheim (Wet 11.12.1998)	Secret (Loi 11.12.1998) Geheim (Wet 11.12.1998)	Confidentiel (Loi 11.12.1998) Vertrouwelijk (Wet 11.12.1998)	([1]) pastaba
Bulgarija	Строго секретно	Секретно	Поверително	За служебно ползване
Čekija	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Danija	YDERST HEMMELIGT	HEMMELIGT	FORTROLIGT	TIL TJENESTEBRUG
Vokietija	STRENG GEHEIM	GEHEIM	VS ([2]) - VERTRAULICH	VS - NUR FÜR DEN DIENSTGEBRAUCH
Estija	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Airija	Top Secret	Secret	Confidential	Restricted
Graikija	Άκρως Απόρρητο Abr: ΑΑΠ	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Ispanija	SECRETO	RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
Prancūzija	Très Secret Défense	Secret Défense	Confidentiel Défense	([3]) pastaba
Kroatija	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Italija	Segretissimo	Segreto	Riservatissimo	Riservato
Kipras	Άκρως Απόρρητο Abr: (ΑΑΠ)	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Latvija	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Lietuva	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Liuksemburgas	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux

Vengrija	Szigorúan titkos!	Titkos!	Bizalmas!	Korlátozott terjesztésű!
Malta	L-Ogħla Segretezza Top Secret	Sigriet Secret	Kunfidenzjali Confidential	Ristrett Restricted ([4])
Nyderlandai	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Austrija	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Lenkija	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugalija	Muito Secreto	Secreto	Confidencial	Reservado
Rumunija	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu
Slovėnija	STROGO TAJNO	TAJNO	ZAUPNO	INTERNO
Slovakija	Prísne tajné	Tajné	Dôverné	Vyhradené
Suomija	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Švedija	Kvaliciferat hemlig	Hemlig	Konfidentiell	Begränsat hemlig
Jungtinė Karalystė	UK TOP SECRET	UK SECRET	([5]) pastaba	UK OFFICIAL SENSITIVE

([1]) Diffusion Restreinte/Beperkte Verspreiding nėra slaptumo žyma Belgijoje. Žyma RESTREINT UE/EU RESTRICTED pažymėtą informaciją Belgija tvarko ir saugo taip pat griežtai kaip taikant nustatytus Europos Sąjungos Tarybos saugumo taisyklėse aprašytus standartus ir procedūras.

([2]) Vokietija: VS = Verschlusssache.

([3]) Prancūzijos nacionalinėje sistemoje slaptumo žyma RESTREINT nenaudojama. Žyma RESTREINT UE/EU RESTRICTED pažymėtą informaciją Prancūzija tvarko ir saugo taip pat griežtai kaip taikant nustatytus Europos Sąjungos Tarybos saugumo taisyklėse aprašytus standartus ir procedūras.

([4]) Maltoje gali būti naudojamos žymos tiek maltiečių, tiek anglų kalba.

([5]) Jungtinės Karalystės nacionalinėje sistemoje žyma UK CONFIDENTIAL nebenaudojama. Žyma CONFIDENTIEL UE/EU CONFIDENTIAL pažymėtą įslaptintą informaciją Jungtinė Karalystė tvarko ir saugo laikydamasi žyma UK SECRET pažymėtai informacijai taikomų apsauginių saugumo reikalavimų.

II PRIEDAS

C PRIEDĖLIS

NACIONALINIŲ SAUGUMO INSTITUCIJŲ (NSI) SĄRAŠAS

BELGIJA Autorité nationale de Sécurité SPF Affaires étrangères, Commerce extérieur et Coopération au Développement 15, rue des Petits Carmes 1000 Bruxelles Sekretoriato tel. +32 25014542 Faks. +32 25014596 El. paštas nvo-ans@diplobel.fed.be	**ESTIJA** National Security Authority Department Estonian Foreign Intelligence Service Rahumäe tee 4B 11316 Tallinn Tel. +372 6939211 Faks. +372 6935001 El. paštas nsa@fis.gov.ee
BULGARIJA State Commission on Information Security 4 Kozloduy Str. 1202 Sofia Tel. +359 29333600 Faks. +359 29873750 El. paštas dksi@government.bg Interneto svetainė www.dksi.bg	**AIRIJA** National Security Authority Department of Foreign Affairs and Trade 76–78 Harcourt Street Dublin 2 D02 DX45 Ireland 1 tel. +353 14082842 2 tel. +353 14082724 El. paštas nsa@dfa.ie
ČEKIJA Národní bezpečnostní úřad (National Security Authority) Na Popelce 2/16 150 06 Praha 56 Tel. +420 257283335 Faks. +420 257283110 El. paštas oms@nbu.cz Interneto svetainė: www.nbu.cz	**GRAIKIJA** Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ) Διεύθυνση Ασφαλείας και Αντιπληροφοριών ΣΤΓ 1020 -Χολαργός (Αθήνα) Ελλάδα Tel.: +30 2106572045 (ώρες γραφείου), +30 2106572009 (ώρες γραφείου) Faks.: +30 2106536279, +30 2106577612 Hellenic National Defence General Staff (HNDGS) Counter Intelligence and Security Directorate (NSA) 227-231 HOLARGOS STG 1020 ATHENS Tel.: +30 2106572045, +30 2106572009 Faks.: +30 2106536279, +30 2106577612

DANIJA Politiets Efterretningstjeneste (Danish Security Intelligence Service) Klausdalsbrovej 1 2860 Søborg Tel. +45 45159007 Faks. +45 45150190 Forsvarets Efterretningstjeneste (Danish Defence Intelligence Service) Kastellet 30 2100 Copenhagen Ø Tel. +45 33325566 Faks. +45 33931320	**ISPANIJA** Autoridad Nacional de Seguridad Oficina Nacional de Seguridad Calle Argentona, 30 28023 Madrid Tel. +34 913725000 Faks. +34 913725808 El. paštas nsa-sp@areatec.com
VOKIETIJA Bundesministerium des Innern, für Bau und Heimat Section ÖS II 5 Alt-Moabit 140 D-10557 Berlin Tel. +49 30186810 Faks. +49 30186811441 1 el. paštas OESII5@bmi.bund.de 2 el. paštas PersGS@bmi.bund.de	**PRANCŪZIJA** Secrétariat général de la défense et de la sécurité nationale Sous-direction Protection du secret (SGDSN/PSD) 51 Boulevard de la Tour-Maubourg 75700 Paris 07 SP Tel. +33 171758177 Faks. +33 171758200
KROATIJA Office of the National Security Council Croatian NSA Jurjevska 34 10000 Zagreb Croatia Tel. +385 14681222 Faks. +385 14686049 El. paštas: NSACroatia@uvns.hr Interneto svetainė: www.uvns.hr	**LIUKSEMBURGAS** Autorité nationale de Sécurité Boîte postale 2379 1023 Luxembourg Tel. +352 24782210 (centrinis) Tel. +352 24782253 (tiesioginis) Faks. +352 24782243
ITALIJA Presidenza del Consiglio dei Ministri D.I.S. - U.C.Se Via di Santa Susanna, 15 00187 Roma Tel., faks. +39 064885273	**VENGRIJA** Nemzeti Biztonsági Felügyelet (National Security Authority of Hungary) 1024 Budapest, Szilágyi Erzsébet fasor 11/B Pašto adresas – 1399 Budapest, Pf. 710/50 Tel. +36 13911862 Faks. +36 13911889 El. paštas nbf@nbf.hu Interneto svetainė www.nbf.hu

KIPRAS ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ ΑΜΥΝΑΣ ΕΘΝΙΚΗ ΑΡΧΗ ΑΣΦΑΛΕΙΑΣ (ΕΑΑ) Υπουργείο Άμυνας Λεωφόρος Στροβόλου 172-174, 1432 Λευκωσία Ταχυδρομικός Κώδικας: 2048 Tel.: +357 22807569, +357 22807643, +357 22807764 Faks. +357 22302351 El. paštas cynsa@mod.gov.cy Ministry of Defence Minister's Military Staff National Security Authority (NSA) 172-174 Strovolou Avenue, 1432 Nicosia Pašto indeksas 2048 Tel.: +357 22807569, +357 22807643, +357 22807764 Faks. +357 22302351 El. paštas cynsa@mod.gov.cy	**MALTA** Ministry for Home Affairs and National Security P.O. Box 146 MT-Valletta Tel. +356 21249844 Faks. +356 25695321
LATVIJA National Security Authority Constitution Protection Bureau of the Republic of Latvia P.O.Box 286 LV-1001 Riga Tel.: +371 67025418 El. paštas: ndi@sab.gov.lv	**NYDERLANDAI** Ministerie van Binnenlandse Zaken en Koninkrijksrelaties Postbus 20010 2500 EA Den Haag Tel. +31 703204400 Faks. +31 703200733 Ministerie van Defensie Beveiligingsautoriteit Postbus 20701 2500 ES Den Haag Tel. +31 703187060 Faks. +31 703187522
LIETUVA Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija (The Commission for Secrets Protection Coordination of the Republic of Lithuania National Security Authority) Pilaitės pr. 19 LT-06264 Vilnius Tel. +370 570666128 Faks. +370 70666700 El. paštas nsa@vsd.lt	**AUSTRIJA** Informationssicherheitskommission Bundeskanzleramt Ballhausplatz 2 1010 Wien Tel. +43 153115202594 Faks. +43 153109202594 El. paštas isk@bka.gv.at

LENKIJA Agencja Bezpieczeństwa Wewnętrznego – ABW (Internal Security Agency) 2A Rakowiecka St. 00-993 Warszawa Tel. +48 225857663 Faks. +48 225858509 El. paštas nsa@abw.gov.pl Interneto svetainė www.abw.gov.pl	**SLOVAKIJA** Národný bezpečnostný úrad (National Security Authority) Budatínska 30 851 06 Bratislava Tel. +421 268691111 Faks. +421 268691700 El. paštas podatelna@nbu.gov.sk Interneto svetainė www.nbu.gov.sk
PORTUGALIJA Presidência do Conselho de Ministros Autoridade Nacional de Segurança Rua da Junqueira, 69 1300-342 Lisboa Tel.: +351 213031710 Faks.: +351 213031711	**SUOMIJA** National Security Authority Ministry for Foreign Affairs P.O. Box 453 FI-00023 Government Tel. +358 916055890 El. paštas NSA@formin.fi
RUMUNIJA Oficiul Registrului Național al Informațiilor Secrete de Stat – Romanian NSA – ORNISS National Registry Office for Classified Information Strada Mureș nr. 4 012275 Bucharest Tel. +40 212075114 Faks. +40 212240714 El. paštas nsa.romania@nsa.ro Interneto svetainė www.orniss.ro	**ŠVEDIJA** Ministry for Foreign Affairs Swedish National Security Authority 103 39 Stockholm Tel. +46 84051000 El. paštas ud-nsa@gov.se
SLOVĖNIJA Urad Vlade RS za varovanje tajnih podatkov Gregorčičeva 27 1000 Ljubljana Tel. +386 14781390 Faks. +386 14781399 El. paštas gp.uvtp@gov.si	**JUNGTINĖ KARALYSTĖ** UK National Security Authority Cabinet Office Room 335 70 Whitehall London SW1A 2AS 1 tel. +44 2072765645 2 tel. +44 2072765497 El. paštas uk-nsa@cabinetoffice.gov.uk

2.8. COUNCIL DECISION (EU) 2019/2247 OF 19 DECEMBER 2019 AMENDING DECISION 2013/488/EU ON THE SECURITY RULES FOR PROTECTING EU CLASSIFIED INFORMATION

COUNCIL DECISION (EU) 2019/2247

of 19 December 2019

amending Decision 2013/488/EU on the security rules for protecting EU classified information

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 240(3) thereof,

Having regard to Council Decision 2009/937/EU of 1 December 2009 adopting the Council's Rules of Procedure ([1]), and in particular Article 24 thereof,

Whereas:

(1) Appendix B to Council Decision 2013/488/EU ([2]) contains a table of equivalence of security classifications.
(2) Appendix C to that decision contains a list of national security authorities (NSAs).
(3) Sweden has notified the General Secretariat of the Council of changes to its security classifications and to its NSAs.
(4) Furthermore, Bulgaria, the Czechia, Denmark, Germany, Estonia, Ireland, Spain, Croatia, Cyprus, Latvia, Lithuania, Hungary, Austria, Poland, Romania, Slovakia, Finland and the United Kingdom have notified the General Secretariat of the Council of changes to their respective NSAs.

(5) Decision 2013/488/EU should therefore be amended accordingly,

HAS ADOPTED THIS DECISION:

Article 1

Appendices B and C to Decision 2013/488/EU are replaced by the text appearing respectively in Annexes 1 and 2 to this Decision.

Article 2

This Decision shall enter into force on the day of its publication.

Done at Brussels, 19 December 2019.

For the Council
The President
K. MIKKONEN

([1]) OJ L 325, 11.12.2009, p. 35.

([2]) Council Decision 2013/488/EU of 23 September 2013 on the security rules for protecting EU classified information (OJ L 274, 15.10.2013, p. 1).

ANNEX I

‘APPENDIX B

EQUIVALENCE OF SECURITY CLASSIFICATIONS

EU	TRÈS SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Belgium	Très Secret (Loi 11.12.1998) Zeer Geheim (Wet 11.12.1998)	Secret (Loi 11.12.1998) Geheim (Wet 11.12.1998)	Confidentiel (Loi 11.12.1998) Vertrouwelijk (Wet 11.12.1998)	nota (1) below
Bulgaria	Строго секретно	Секретно	Поверително	За служебно ползване
Czechia	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Denmark	YDERST HEMMELIGT	HEMMELIGT	FORTROLIGT	TIL TJENESTEBRUG
Germany	STRENG GEHEIM	GEHEIM	VS (2) - VERTRAULICH	VS - NUR FÜR DEN DIENSTGEBRAUCH
Estonia	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Ireland	Top Secret	Secret	Confidential	Restricted
Greece	Άκρως Απόρρητο Abr: ΑΑΠ	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Spain	SECRETO	RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
France	Très Secret Défense	Secret Défense	Confidentiel Défense	nota (3) below
Croatia	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Italy	Segretissimo	Segreto	Riservatissimo	Riservato
Cyprus	Άκρως Απόρρητο Abr: (ΑΑΠ)	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Latvia	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Lithuania	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Luxembourg	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Hungary	Szigorúan titkos!	Titkos!	Bizalmas!	Korlátozott terjesztésű!
Malta	L-Oghla Segretezza Top Secret	Sigriet Secret	Kunfidenzjali Confidential	Ristrett Restricted (4)

Netherlands	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Austria	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Poland	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugal	Muito Secreto	Secreto	Confidencial	Reservado
Romania	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu
Slovenia	STROGO TAJNO	TAJNO	ZAUPNO	INTERNO
Slovakia	Prísne tajné	Tajné	Dôverné	Vyhradené
Finland	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Sweden	Kvaliciferat hemlig	Hemlig	Konfidentiell	Begränsat hemlig
United Kingdom	UK TOP SECRET	UK SECRET	nota ([5]) below	UK OFFICIAL SENSITIVE

([1]) Diffusion Restreinte/Beperkte Verspreiding is not a security classification in Belgium. Belgium handles and protects "RESTREINT UE/EU RESTRICTED" information in a manner no less stringent than the standards and procedures described in the security rules of the Council of the European Union.

([2]) Germany: VS = Verschlusssache.

([3]) France does not use the classification "RESTREINT" in its national system. France handles and protects "RESTREINT UE/EU RESTRICTED" information in a manner no less stringent than the standards *and* procedures described in the security rules of the Council of the European Union.

([4]) The Maltese and English markings for Malta can be used interchangeably.

([5]) The UK no longer uses the classification "UK CONFIDENTIAL" in its national system. The UK handles and protects "CONFIDENTIEL UE/EU CONFIDENTIAL" classified information in accordance with the protective security requirements for "UK SECRET".

ANNEX II

‘APPENDIX C

LIST OF NATIONAL SECURITY AUTHORITIES (NSAs)

BELGIUM Autorité nationale de Sécurité SPF Affaires étrangères, Commerce extérieur et Coopération au Développement 15, rue des Petits Carmes 1000 Bruxelles Tel. Secretariat: +32 25014542 Fax +32 25014596 Email: nvo-ans@diplobel.fed.be	**ESTONIA** National Security Authority Department Estonian Foreign Intelligence Service Rahumäe tee 4B 11316 Tallinn Tel. +372 6939211 Fax +372 6935001 Email: nsa@fis.gov.ee
BULGARIA State Commission on Information Security 4 Kozloduy Str. 1202 Sofia Tel. +359 29333600 Fax +359 29873750 Email: dksi@government.bg Website: www.dksi.bg	**IRELAND** National Security Authority Department of Foreign Affairs and Trade 76 - 78 Harcourt Street Dublin 2 D02 DX45 Ireland Tel. 1: +353 14082842 Tel. 2: +353 14082724 Email: nsa@dfa.ie

CZECHIA Národní bezpečnostní úřad (National Security Authority) Na Popelce 2/16 150 06 Praha 56 Tel. +420 257283335 Fax +420 257283110 Email: oms@nbu.cz Website: www.nbu.cz	**GREECE** Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ) Διεύθυνση Ασφαλείας και Αντιπληροφοριών ΣΤΓ 1020 -Χολαργός (Αθήνα) Ελλάδα Τηλ.: +30 2106572045 (ώρες γραφείου) +30 2106572009 (ώρες γραφείου) Φαξ: +30 2106536279 +30 2106577612 Hellenic National Defence General Staff (HNDGS) Counter Intelligence and Security Directorate (NSA) 227-231 HOLARGOS STG 1020 ATHENS Tel. +30 2106572045 +30 2106572009 Fax +30 2106536279 +30 2106577612
DENMARK Politiets Efterretningstjeneste (Danish Security Intelligence Service) Klausdalsbrovej 1 2860 Søborg Tel. +45 45159007 Fax +45 45150190 Forsvarets Efterretningstjeneste (Danish Defence Intelligence Service) Kastellet 30 2100 Copenhagen Ø Tel. +45 33325566 Fax +45 33931320	**SPAIN** Autoridad Nacional de Seguridad Oficina Nacional de Seguridad Calle Argentona, 30 28023 Madrid Tel. +34 913725000 Fax +34 913725808 Email: nsa-sp@areatec.com
GERMANY Bundesministerium des Innern, für Bau und Heimat Section ÖS II 5 Alt-Moabit 140 D-10557 Berlin Tel. +49 30186810 Fax +49 30186811441 Email 1: OESII5@bmi.bund.de Email 2: PersGS@bmi.bund.de	**FRANCE** Secrétariat général de la défense et de la sécurité nationale Sous-direction Protection du secret (SGDSN/PSD) 51 Boulevard de la Tour-Maubourg 75700 Paris 07 SP Tel. +33 171758177 Fax +33 171758200

CROATIA Office of the National Security Council Croatian NSA Jurjevska 34 10000 Zagreb Croatia Tel. +385 14681222 Fax +385 14686049 Email: NSACroatia@uvns.hr Website: www.uvns.hr	**LUXEMBOURG** Autorité nationale de Sécurité Boîte postale 2379 1023 Luxembourg Tel. +352 24782210 central Tel. +352 24782253 direct Fax +352 24782243
ITALY Presidenza del Consiglio dei Ministri D.I.S. - U.C.Se Via di Santa Susanna, 15 00187 Roma Tel. +39 0661174266 Fax +39 064885273	**HUNGARY** Nemzeti Biztonsági Felügyelet (National Security Authority of Hungary) 1024 Budapest, Szilágyi Erzsébet fasor 11/B Postal address: 1399 Budapest, Pf. 710/50 Tel. +36 13911862 Fax +36 13911889 Email: nbf@nbf.hu Website: www.nbf.hu
CYPRUS ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ ΑΜΥΝΑΣ ΕΘΝΙΚΗ ΑΡΧΗ ΑΣΦΑΛΕΙΑΣ (ΕΑΑ) Υπουργείο Άμυνας Λεωφόρος Στροβόλου 172-174, 1432 Λευκωσία Ταχυδρομικός Κώδικας: 2048 Τηλεφωνα: +357 22807569, +357 22807643, +357 22807764 Τηλεομοιότυπ: +357 22302351 Ηλεκτρονικό Ταχυδρομείο: cynsa@mod.gov.cy Ministry of Defence Minister's Military Staff National Security Authority (NSA) 172-174 Strovolou Avenue, 1432 Nicosia Postal code: 2048 Tel. +357 22807569, +357 22807643, +357 22807764 Fax +357 22302351 Email: cynsa@mod.gov.cy	**MALTA** Ministry for Home Affairs and National Security P.O. Box 146 MT-Valletta Tel. +356 21249844 Fax +356 25695321

LATVIA National Security Authority Constitution Protection Bureau of the Republic of Latvia P.O.Box 286 LV-1001 Riga Tel. +371 67025418 Email: ndi@sab.gov.lv	**NETHERLANDS** Ministerie van Binnenlandse Zaken en Koninkrijksrelaties Postbus 20010 2500 EA Den Haag Tel. +31 703204400 Fax +31 703200733 Ministerie van Defensie Beveiligingsautoriteit Postbus 20701 2500 ES Den Haag Tel. +31 703187060 Fax +31 703187522
LITHUANIA Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija (The Commission for Secrets Protection Coordination of the Republic of Lithuania National Security Authority) Pilaitės ave. 19 LT-06264 Vilnius Tel. +370 570666128 Fax +370 70666700 Email: nsa@vsd.lt	**AUSTRIA** Informationssicherheitskommission Bundeskanzleramt Ballhausplatz 2 1010 Wien Tel. +43 153115202594 Fax +43 153109202594 Email: isk@bka.gv.at
POLAND Agencja Bezpieczeństwa Wewnętrznego – ABW (Internal Security Agency) 2A Rakowiecka St. 00-993 Warszawa Tel. +48 225857663 Fax +48 225858509 Email: nsa@abw.gov.pl Website: www.abw.g	**SLOVAKIA** Národný bezpečnostný úrad (National Security Authority) Budatínska 30 851 06 Bratislava Tel. +421 268691111 Fax +421 268691700 Email: podatelna@nbu.gov.sk Website: www.nbu.gov.sk
PORTUGAL Presidência do Conselho de Ministros Autoridade Nacional de Segurança Rua da Junqueira, 69 1300-342 Lisboa Tel. +351 213031710 Fax +351 213031711	**FINLAND** National Security Authority Ministry for Foreign Affairs P.O. Box 453 FI-00023 Government Tel. +358 916055890 Email: NSA@formin.fi

ROMANIA Oficiul Registrului Național al Informațiilor Secrete de Stat – Romanian NSA – ORNISS National Registry Office for Classified Information Strada Mureș nr. 4 012275 Bucharest Tel. +40 212075114 Fax +40 212240714 Email: nsa.romania@nsa.ro Website: www.orniss.ro	**SWEDEN** Ministry for Foreign Affairs Swedish National Security Authority 103 39 Stockholm Tel. +46 84051000 Email: ud-nsa@gov.se
SLOVENIA Urad Vlade RS za varovanje tajnih podatkov Gregorčičeva 27 1000 Ljubljana Tel. +386 14781390 Fax +386 14781399 Email: gp.uvtp@gov.si	**UNITED KINGDOM** UK National Security Authority Cabinet Office Room 335 70 Whitehall London SW1A 2AS Tel. 1: +44 2072765645 Tel. 2: +44 2072765497 Email: uk-nsa@cabinetoffice.gov.uk

2.9. 2015 M. KOVO 13 D. KOMISIJOS SPRENDIMAS (ES, EURATOMAS) 2015/443 DĖL SAUGUMO KOMISIJOJE

KOMISIJOS SPRENDIMAS (ES, Euratomas) 2015/443

2015 m. kovo 13 d.

dėl saugumo Komisijoje

EUROPOS KOMISIJA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo, ypač į jos 249 straipsnį,

atsižvelgdama į Europos atominės energijos bendrijos steigimo sutartį,

atsižvelgdama į Protokolą Nr. 7 dėl Europos Sąjungos privilegijų ir imunitetų, pridėtą prie Sutarčių, ypač į jo 18 straipsnį,

kadangi:

(1) saugumo Komisijoje tikslas, – laikantis nuoseklaus ir integruoto požiūrio į saugumą Komisijoje, suteikti asmenims, turtui ir informacijai tinkamo lygio apsaugą, kuri atitiktų nustatytus pavojus, taip pat veiksmingai ir laiku užtikrinti saugumą ir taip sudaryti Komisijai sąlygas vykdyti veiklą saugioje ir patikimoje aplinkoje;

(2) Komisija, kaip ir kitos tarptautinės organizacijos, susiduria su didelėmis grėsmėmis ir problemomis saugumo srityje, kurios visų pirma susijusios su terorizmu, kibernetiniais išpuoliais ir politiniu bei komerciniu šnipinėjimu;

(3) Europos Komisija su Belgijos, Liuksemburgo ir Italijos Vyriausybėmis sudarė susitarimus dėl pagrindinių jos darbo vietų saugumo ([1]). Šie susitarimai patvirtina, kad Komisija prisiima atsakomybę už savo saugumą;

(4) kad būtų užtikrintas asmenų, turto ir informacijos saugumas, Komisijai gali tekti imtis priemonių – pagrindinių teisių, įtvirtintų Pagrindinių teisių chartijoje ir Europos žmogaus teisių konvencijoje ir pripažintų Europos Teisingumo Teismo, apsaugos srityse;

(5) bet kokia tokia priemonė turėtų būti pateisinama intereso, kuriam apsaugoti ji skirta, svarba, taip pat būti proporcinga ir užtikrinti, kad būtų visapusiškai paisoma pagrindinių teisių, visų pirma teisių į privatumą ir duomenų apsaugą;

(6) sistemoje, kurioje laikomasi teisinės valstybės ir pagarbos pagrindinėms teisėms principų, Komisija turi siekti tinkamo savo darbuotojų, turto ir informacijos saugumo lygio, kuris jai užtikrintų galimybę vykdyti veiklą ir neribotų pagrindinių teisių labiau, nei tikrai būtina;

(7) saugumas Komisijoje grindžiamas teisėtumo, skaidrumo, proporcingumo ir atskaitomybės principais;

(8) personalo nariai, įgalioti imtis saugumo priemonių, neturėtų atsidurti nepalankioje padėtyje dėl savo veiksmų, išskyrus tuos atvejus, kai jie veikė viršydami savo įgaliojimus arba pažeisdami teisės aktus, taigi šiuo atžvilgiu šis sprendimas laikytinas tarnybiniu nurodymu, kaip apibrėžta Tarnybos nuostatuose;

(9) Komisija turėtų imtis tinkamų iniciatyvų siekdama puoselėti ir stiprinti saugumo kultūrą ir taip užtikrinti veiksmingesnį saugumą, gerinti saugumo valdymą, toliau stiprinti tinklus ir tarptautinio, Europos ir nacionalinio lygmens bendradarbiavimą su atitinkamomis institucijomis, taip pat gerinti saugumo priemonių įgyvendinimo stebėseną ir kontrolę;

(10) Europos išorės veiksmų tarnybos (EIVT) – funkciniu požiūriu savarankiškos Europos Sąjungos įstaigos – įsteigimas turėjo didelės įtakos Komisijos saugumo interesams, todėl būtina sukurti taisykles ir procedūras, kuriomis būtų reglamentuojamas EIVT ir Komisijos bendradarbiavimas saugos ir saugumo srityje, visų pirma, siekiant, kad Komisija galėtų atlikti rūpestingumo pareigą savo darbuotojų Sąjungos delegacijose atžvilgiu;

(11) Europos Sąjungos Komisijos saugumo politika turėtų būti įgyvendinama taip, kad būtų suderinama su kitais vidaus procesais ir procedūromis, kurie gali būti susiję su saugumo aspektu, be kita ko, ypač su veiklos tęstinumo valdymu, kuriuo siekiama išlaikyti ypatingos svarbos Komisijos funkcijas veiklos sutrikimo atveju, ir ARGUS procesu, skirtu daugiasektorei krizei koordinuoti;

(12) nepaisant priemonių, kurios šio sprendimo priėmimo momentu jau yra vykdomos ir apie kurias pranešta Europos duomenų apsaugos priežiūros pareigūnui ([2]), bet kokiai su asmens duomenų tvarkymu susijusiai priemonei pagal šį sprendimą taikomos 21 straipsnyje nurodytos įgyvendinimo taisyklės, kuriomis nustatomos tinkamos duomenų subjektų apsaugos priemonės;

(13) būtina, kad Komisija persvarstytų, atnaujintų ir konsoliduotų dabartinį saugumo Komisijoje reglamentavimo pagrindą;

(14) Komisijos sprendimas (94) 2129 ([3]) turėtų būti panaikintas,

PRIĖMĖ ŠĮ SPRENDIMĄ:

1 SKYRIUS

BENDROSIOS NUOSTATOS

1 straipsnis
Apibrėžtys

Šiame sprendime vartojamų terminų apibrėžtys:

1) **turtas** – visas kilnojamasis ir nekilnojamasis Komisijos turtas ir nuosavybė;

2) **Komisijos padalinys** – Komisijos generalinis direktoratas arba tarnyba, arba Komisijos nario kabinetas;

3) **ryšių ir informacinė sistema, arba RIS,** – bet kokia sistema, sudaranti sąlygas tvarkyti informaciją elektroniniu būdu, įskaitant visas priemones, kurių reikia jos veikimui užtikrinti, taip pat infrastruktūrą, organizavimą, personalą ir informacijos šaltinius;

4) **pavojų kontrolė** – bet kokia saugumo priemonė, kuria pagrįstai galima tikėtis veiksmingai kontroliuoti pavojų saugumui: užkirsti jam kelią, jį mažinti, jo išvengti arba jį perkelti;

5) **krizinė situacija** – bet kokios kilmės aplinkybė, įvykis, incidentas ar ekstremalioji situacija (arba jų seka ar derinys), keliantys didelę arba tiesioginę grėsmę saugumui Komisijoje;

6) **duomenys** – informacija tokios formos, kad ją būtų galima per-

duoti, registruoti arba tvarkyti;

7) **už saugumą atsakingas Komisijos narys** – Komisijos narys, kurio atsakomybės sričiai priklauso Žmogiškųjų išteklių ir saugumo generalinis direktoratas;

8) **asmens duomenys** – asmens duomenys, kaip apibrėžta Europos Parlamento ir Tarybos reglamento (EB) Nr. 45/2001 ([4]) 2 straipsnio a punkte;

9) **patalpos** – bet koks nekilnojamasis ar jam prilyginamas Komisijos turtas ir nuosavybė;

10) **pavojaus prevencija** – saugumo priemonės, kuriomis pagrįstai galima tikėtis sumažinti, atitolinti arba pašalinti pavojų saugumui;

11) **pavojus saugumui** – įvykio keliamos grėsmės lygio, pažeidžiamumo lygio ir galimo poveikio derinys;

12) **saugumas Komisijoje** – asmenų, turto ir informacijos saugumas Komisijoje, visų pirma, fizinė asmenų ir turto neliečiamybė, informacijos ir ryšių ir informacinių sistemų vientisumas, konfidencialumas ir prieinamumas, taip pat nevaržomas Komisijos veiklos vykdymas;

13) **saugumo priemonė** – bet kokia priemonė, kurios imamasi vadovaujantis šiuo sprendimu siekiant kontroliuoti pavojus saugumui;

14) **Tarnybos nuostatai** – Europos Sąjungos pareigūnų tarnybos nuostatai, nustatyti Tarybos reglamentu (EEB, Euratomas, EAPB) Nr. 259/68 ([5]) ir jį iš dalies keičiančiais teisės aktais;

15) **grėsmė saugumui** – bet koks įvykis arba veiksnys, galintis, kaip pagrįstai galima tikėtis, turėti neigiamos įtakos saugumui, jeigu nebus imtasi atsako ir jis nebus kontroliuojamas;

16) **tiesioginė grėsmė saugumui** – grėsmė saugumui, kylanti, kai apie tai iš anksto nežinoma arba sužinoma likus labai mažai laiko;

17) **didelė grėsmė saugumui** – grėsmė saugumui, dėl kurios, kaip pagrįstai galima tikėtis, gali būti prarasta gyvybė, patirtas sunkus sužalojimas ar žala sveikatai, padaryta didelė turtinė žala, atskleista itin slapta informacija, sutrikdytos IT sistemos arba sužlugdyti svarbūs Komisijos vykdomieji gebėjimai;

18) **pažeidžiamumas** – bet kokio pobūdžio trūkumas, kuris, kaip pagrįstai galima tikėtis, gali turėti neigiamos įtakos Komisijos saugumui, jeigu juo naudojamasi vienos ar daugiau grėsmių atveju.

2 straipsnis

Dalykas

1. Šiuo sprendimu nustatomi su saugumu Komisijoje susiję tikslai, pagrindiniai principai, organizacinė struktūra ir atsakomybė.

2. Šis sprendimas taikomas visiems Komisijos padaliniams ir visose Komisijos patalpose. Europos Sąjungos delegacijose dirbantiems Komisijos darbuotojams taikomos Europos išorės veiksmų tarnybos saugumo taisyklės ([6]).

3. Nepaisant konkrečių nuorodų dėl tam tikrų darbuotojų grupių, šis sprendimas taikomas Komisijos nariams, Komisijos darbuotojams pagal Tarnybos nuostatus ir kitų Europos Sąjungos tarnautojų įdarbinimo sąlygas, į Komisiją deleguotiems nacionaliniams ekspertams (angl. santrumpa SNE), paslaugų teikėjams ir jų darbuotojams, stažuotojams ir bet kuriam asmeniui, galinčiam patekti į Komisijos pastatus ar naudotis kitu turtu, arba informacija, kurią tvarko Komisija.

4. Šio sprendimo nuostatos nedaro poveikio Komisijos sprendimui 2002/47/EB, EAPB, Euratomas ([7]), Komisijos sprendimui 2004/563/EB, Euratomas ([8]), Komisijos sprendimui C(2006) 1623 ([9]) ir Komisijos sprendimui C(2006) 3602 ([10]).

2 SKYRIUS

PRINCIPAI

3 straipsnis

Saugumo Komisijoje principai

1. Įgyvendindama šį sprendimą Komisija laikosi Sutarčių, visų pirma, Pagrindinių teisių chartijos ir Protokolo Nr. 7 dėl Europos Sąjungos privilegijų ir imunitetų, taip pat 2 konstatuojamojoje dalyje nurodytų susitarimų ir visų galiojančių nacionalinės teisės normų bei šio sprendimo nuostatų. Jei būtina, pagal 21 straipsnio 2 dalį išleidžiamas saugumo pranešimas, kuriame pateikiamos gairės šiuo klausimu.

2. Saugumas Komisijoje grindžiamas teisėtumo, skaidrumo, proporcingumo ir atskaitomybės principais.

3. Teisėtumo principas reiškia būtinybę įgyvendinant šį sprendimą griežtai išlikti teisinės sistemos ribose ir atitikti teisinius reikalavimus.

4. Bet kurios saugumo priemonės imamasi atvirai, išskyrus atvejus, kai pagrįstai galima tikėtis, kad tai susilpnins jos poveikį. Saugumo priemonės adresatai iš anksto informuojami apie priemonės priežastis ir poveikį, nebent pagrįstai galima tikėtis, kad pateikus tokią informaciją šios priemonės poveikis susilpnės. Šiuo atveju saugumo priemonės adresatas informuojamas išnykus pavojui, kad saugumo priemonės poveikis susilpnės.

5. Komisijos padaliniai užtikrina, kad į saugumo aspektus būtų atsižvelgiama vos tik pradėjus rengti ir įgyvendinti Komisijos politiką, sprendimus, programas, projektus ir veiklą, už kurią jie yra atsakingi. Šiuo tikslu jau pačiuose ankstyviausiuose parengiamuosiuose etapuose bendru mastu įtraukiamas Žmogiškųjų išteklių ir saugumo generalinis direktoratas, o IT sistemų atveju – vyriausiasis informacijos apsaugos pareigūnas.

6. Komisija prireikus bendradarbiauja su priimančiosios valstybės ir kitų valstybių narių kompetentingomis institucijomis bei kitomis ES institucijomis, agentūromis arba įstaigomis, kai įmanoma, atsižvelgdama į priemones, kurių tos institucijos ėmėsi arba planavo imtis siekdamos spręsti atitinkamo pavojaus saugumui problemą.

4 straipsnis

Pareiga laikytis nuostatų

1. Privaloma laikytis šio sprendimo ir jo įgyvendinimo taisyklių, taip pat įgaliotųjų darbuotojų nurodytų saugumo priemonių ir nurodymų.

2. Jei saugumo taisyklių nesilaikoma, gali būti pradėtos taikyti drausminės priemonės pagal Sutartis ir Tarnybos nuostatus, taip pat darbo sutartyse numatytos sankcijos ir (arba) teisiniai veiksmai pagal nacionalinius įstatymus ir kitus teisės aktus.

3 SKYRIUS

SAUGUMO UŽTIKRINIMAS

5 straipsnis

Įgaliotieji darbuotojai

1. Tik darbuotojai, kuriems Žmogiškųjų išteklių ir saugumo generalinio direktorato generalinis direktorius yra suteikęs asmeninį įgaliojimą, atsižvelgiant į jų einamas pareigas, gali gauti teisę imtis vienos arba kelių iš šių priemonių:

1) nešiotis asmeninius ginklus;
2) atlikti 13 straipsnyje nurodytus saugumo tyrimus;
3) imtis 12 straipsnyje nurodytų saugumo priemonių, kaip nustatyta įgaliojime.

2. Šio straipsnio 1 dalyje nurodyti įgaliojimai suteikiami laikotarpiui, kuris neturi būti ilgesnis už laikotarpį, per kurį susijęs asmuo eina pareigas ar atlieka funkcijas, kurių pagrindu buvo suteiktas įgaliojimas. Įgaliojimai suteikiami laikantis 3 straipsnio 1 dalyje nustatytų galiojančių nuostatų.

3. Įgaliotiesiems darbuotojams šis sprendimas yra tarnybinis nurodymas, kaip apibrėžta Tarnybos nuostatų 21 straipsnyje.

6 straipsnis

Bendrosios saugumo priemonių nuostatos

1. Imdamasi saugumo priemonių, Komisija visų pirma, kiek praktiškai įmanoma, užtikrina, kad:

a) susijusios valstybės narės paramos ar pagalbos būtų prašoma, tik jei ta valstybė yra Europos Sąjungos valstybė narė arba (jei ji nėra narė) Europos žmogaus teisių konvencijos šalis, arba jei ji užtikrina teises, kurios yra bent jau lygiavertės šia konvencija užtikrinamoms teisėms;

b) pagal Reglamento (EB) Nr. 45/2001 9 straipsnį informacija apie asmenį būtų perduodama tik tiems duomenų gavėjams (išskyrus Bendrijos institucijas ir įstaigas), kuriems nėra taikomi nacionaliniai teisės aktai, priimti vadovaujantis Europos Parlamento ir Tarybos direktyva 95/46/EB ([11]);

c) jei asmuo kelia grėsmę saugumui, tam asmeniui būtų taikomos bet kokios saugumo priemonės; tam asmeniui taip pat gali tekti padengti patirtas išlaidas. Minėtas saugumo priemones kitiems asmenims galima taikyti, tik jei būtina kontroliuoti tiesioginę arba didelę grėsmę saugumui ir yra tenkinamos šios sąlygos:

a) nėra galimybės imtis priemonių, kurios numatytos grėsmę saugumui keliančiam asmeniui, arba jos greičiausiai bus neveiksmingos;

b) Komisija savo veiksmais negali kontroliuoti grėsmės saugumui arba negali to padaryti laiku;

c) dėl tos priemonės nekyla neproporcingas pavojus kitam asmeniui ir jo teisėms.

2. Žmogiškųjų išteklių ir saugumo generalinio direktorato Saugumo direktoratas sudaro saugumo priemonių, dėl kurių gali prireikti teisėjo nutarties pagal valstybių narių, kuriose yra Komisijos patalpų, įstatymus ir kitus teisės aktus, sąrašą.

3. Žmogiškųjų išteklių ir saugumo generalinio direktorato Saugumo direktoratas gali kreiptis į rangovą, kad šis, vadovaujant ir prižiūrint Saugumo direktoratui, atliktų su saugumu susijusias užduotis.

7 straipsnis

Su asmenimis susijusios saugumo priemonės

1. Atsižvelgiant į saugumo ir saugos reikalavimus, Komisijos patalpose esantiems asmenims suteikiama tinkamo lygio apsauga.

2. Didelių pavojų saugumui atveju Žmogiškųjų išteklių ir saugumo generalinis direktoratas Komisijos nariams ar kitiems darbuotojams suteikia tiesioginę asmens apsaugą, jeigu grėsmės vertinimas parodė, kad tokia apsauga būtina siekiant užtikrinti jų saugą ir saugumą.

3. Didelių pavojų saugumui atveju Komisija gali nurodyti evakuoti savo patalpas.

4. Avarijų ar išpuolių Komisijos patalpose aukos gauna pagalbą.

5. Siekiant užtikrinti pavojų saugumui prevenciją ir kontrolę, įgaliotieji darbuotojai gali atlikti asmenų, kurie patenka į šio sprendimo taikymo sritį, patikrinimus, kad nustatytų, ar, tokiems asmenims leidus patekti į Komisijos patalpas arba prieiti prie jos informacijos, kyla grėsmė saugumui. Tuo tikslu, laikydamiesi Reglamento (EB) Nr. 45/2001 nuostatų ir 3 straipsnio 1 dalyje nurodytų nuostatų, atitinkami įgaliotieji darbuotojai gali:

a) naudoti bet kokį Komisijai prieinamą informacijos šaltinį, atsižvelgdami į informacijos šaltinio patikimumą;
b) tinkamai pagrįstais atvejais susipažinti su asmens byla arba Komisijos turimais joje dirbančių arba ketinamų įdarbinti asmenų arba rangovo darbuotojų duomenimis.

8 straipsnis

Su fiziniu saugumu ir turtu susijusios saugumo priemonės

1. Turto saugumas užtikrinamas taikant tinkamas fizines ir technines apsaugos priemones ir atitinkamas procedūras (toliau – fizinis saugumas), kuriomis sukuriama daugiasluoksnė sistema.

2. Priemonės gali būti patvirtinamos pagal šį straipsnį siekiant apsaugoti asmenis arba informaciją Komisijoje, taip pat apsaugoti turtą.

3. Fiziniam saugumui keliami šie tikslai:

– užkirsti kelią smurto aktams, nukreiptiems prieš Komisijos narius arba asmenis, kurie patenka į šio sprendimo taikymo sritį;
– užkirsti kelią neskelbtinos arba įslaptintos informacijos šnipinėjimui ir slaptam pasiklausymui;
– užkirsti kelią vagystėms, vandalizmo aktams, sabotažui ir kitiems smurto veiksmams, kuriais siekiama gadinti ar naikinti Komisijos pastatus ir turtą;
– sudaryti sąlygas tirti ir nagrinėti saugumo incidentus, be kita ko, tikrinant patekimo į patalpas ir išvykimo iš jų kontrolės žurnalų failus, apsauginių vaizdo stebėjimo sistemų (AVSS) duomenis, telefono skambučių įrašus ir panašius duomenis, kaip nurodyta šio sprendimo 22 straipsnio 2 dalyje, taip pat kitus informacijos šaltinius.

4. Fizinis saugumas apima:

– prieigos suteikimo politiką, taikomą bet kuriam asmeniui ar transporto priemonei, kuriems būtina patekti į Komisijos patalpas, įskaitant automobilių stovėjimo aikšteles;

– prieigos kontrolės sistemą, kurią sudaro apsaugos darbuotojai, techninė įranga ir priemonės, informacinės sistemos arba visų tų elementų derinys.

5. Siekiant užtikrinti fizinį saugumą, galima imtis šių veiksmų:

– registruoti asmenų, transporto priemonių, prekių ir įrangos patekimą į Komisijos patalpas ir išvykimą iš jų;
– tikrinti asmens tapatybę jos patalpose;
– vaizdo arba techninėmis priemonėmis tikrinti transporto priemones, prekes ir įrangą;
– užkirsti kelią leidimo neturintiems asmenims, transporto priemonėms ir prekėms patekti į Komisijos patalpas.

9 straipsnis

Su informacija susijusios saugumo priemonės

1. Informacijos saugumas susijęs su visa Komisijos tvarkoma informacija.

2. Siekiant užtikrinti informacijos saugumą, nepriklausomai nuo informacijos formos, skaidrumo, proporcingumo, atskaitomybės ir veiksmingumo principai derinami su būtinybe apsaugoti informaciją nuo neteisėtos prieigos prie jos, neteisėto jos naudojimo, atskleidimo, pakeitimo ar sunaikinimo.

3. Informacijos saugumo tikslas – apsaugoti jos konfidencialumą, vientisumą ir prieinamumą.

4. Įslaptinant informacinius išteklius ir rengiant proporcingas saugumo priemones, procedūras bei standartus, įskaitant pavojų mažinančias priemones, pasitelkiami rizikos valdymo procesai.

5. Šie bendrieji principai, kuriais grindžiamas informacijos saugumas, visų pirma taikomi:

a) Europos Sąjungos įslaptintai informacijai (toliau – ESĮI), t. y. bet kuriai informacijai arba medžiagai, kuriai suteikta ES slaptumo žyma ir kurią neteisėtai atskleidus galėtų būti padaryta tam tikro dydžio žala Europos Sąjungos arba vienos ar kelių valstybių narių interesams;

b) neskelbtinai neįslaptintai informacijai, t. y. informacijai arba medžiagai, kurią Komisija privalo apsaugoti dėl Sutartyse ir priimtuose jų įgyvendinimo aktuose nustatytų teisinių prievolių ir (arba) dėl jos neskelbtinumo. Neskelbtina neįslaptinta informacija apima (bet neapsiriboja) informaciją ar medžiagą, kuriai taikoma tarnybinės paslapties saugojimo prievolė, kaip nurodyta SESV 339 straipsnyje, informaciją, kuri susijusi su interesais, saugomais Europos Parlamento ir Tarybos reglamento (EB) Nr. 1049/2001 ([12]) 4 straipsniu kartu su atitinkama Europos Sąjungos Teisingumo Teismo praktika, arba asmens duomenis, patenkančius į Reglamento (EB) Nr. 45/2001 taikymo sritį.

6. Neskelbtinai neįslaptintai informacijai taikomos jos tvarkymo ir saugojimo taisyklės. Ji teikiama tik tiems asmenims, kuriems „būtina žinoti“. Jei būtina, siekiant veiksmingai apsaugoti tokios informacijos konfidencialumą, ji pažymima slaptumo žyma ir jai taikomi Žmogiškųjų išteklių ir saugumo generalinio direktorato generalinio direktoriaus patvirtinti atitinkami jos tvarkymo nurodymai. Ryšių ir informacinėse sistemose tvarkoma arba laikoma tokia informacija taip pat yra saugoma laikantis Sprendimo C(2006) 3602 nuostatų, jo įgyvendinimo taisyklių ir atitinkamų standartų.

7. Bet kokiam asmeniui, neteisėtai atskleidusiam ar praradusiam ESĮI arba neskelbtiną neįslaptintą informaciją, kuri taip identifikuojama pagal jos tvarkymo ir laikymo taisykles, gali būti taikomos drausminės priemonės pagal Tarnybos nuostatus. Tos drausminės priemonės nedaro poveikio bet kokiems tolesniems valstybių narių kompetentingų nacionalinių institucijų teisiniams ar baudžiamojo proceso veiksmams pagal jų įstatymus ir kitus teisės aktus ir sutartinėms teisių gynimo priemonėms.

10 straipsnis

Su ryšių ir informacinėmis sistemomis susijusios saugumo priemonės

1. Visos Komisijos naudojamos ryšių ir informacinės sistemos (toliau – RIS) atitinka Komisijos informacinių sistemų saugumo politiką, nustatytą Sprendime C(2006) 3602, jo įgyvendinimo taisyklėse ir atitinkamuose saugumo standartuose.

2. Komisijos tarnybos, turinčios, administruojančios ar valdančios

RIS, kitoms Europos Sąjungos institucijoms, agentūroms, įstaigoms arba kitoms organizacijoms suteikia prieigą prie tų sistemų, tik jei tos Europos Sąjungos institucijos, agentūros, įstaigos arba kitos organizacijos gali pagrįstai patikinti, kad jų IT sistemos apsaugotos lygiu, atitinkančiu Komisijos informacinių sistemų saugumo politiką, nustatytą Sprendime C(2006) 3602, jo įgyvendinimo taisyklėse ir atitinkamuose saugumo standartuose. Komisija stebi, kaip laikomasi reikalavimų, o rimto jų pažeidimo atveju arba jei jų ir toliau nesilaikoma, turi teisę uždrausti prieigą.

11 straipsnis

Kibernetinio saugumo teismo ekspertizė

Žmogiškųjų išteklių ir saugumo generalinis direktoratas visų pirma yra atsakingas už techninės teismo ekspertizės atlikimą bendradarbiaujant su kompetentingais Komisijos padaliniais, kai atliekami 13 straipsnyje nurodyti saugumo tyrimai, susiję su kontržvalgyba, duomenų nutekėjimu, kibernetiniais išpuoliais ir informacinių sistemų saugumu.

12 straipsnis

Su asmenimis ir objektais susijusios saugumo priemonės

1. Siekiant užtikrinti saugumą Komisijoje ir užkirsti kelią pavojams bei juos kontroliuoti, pagal 5 straipsnį įgalioti darbuotojai, vadovaudamiesi 3 straipsnyje nustatytais principais, imasi, be kita ko, vienos ar kelių iš šių apsaugos priemonių:

a) incidentų ar elgesio, dėl kurių gali būti pradėtos administracinės, drausminės, civilinės ar baudžiamosios procedūros, atveju užtikrina įvykio vietos ir įrodymų, įskaitant patekimo į patalpas ir išvykimo iš jų kontrolės žurnalų failus ir AVSS vaizdinę medžiagą, apsaugą;
b) ribotų priemonių, susijusių su asmenimis, keliančiais grėsmę saugumui, įskaitant nurodymą asmenims palikti Komisijos patalpas, asmenų palydėjimą iš Komisijos patalpų, draudimą asmenims patekti į Komisijos patalpas tam tikru laikotarpiu, kuris nustatomas remiantis kriterijais, nustatytinais įgyvendinimo taisyklėse;
c) ribotų priemonių, susijusių su grėsmę saugumui keliančiais objektais, įskaitant objektų perkėlimą, konfiskavimą ir šalinimą;

d) Komisijos patalpų, įskaitant čia esančius biurus, kratų;
e) RIS ir įrangos, telefonų ir telekomunikacijų srauto duomenų, registracijos failų, vartotojų paskyrų ir kt. patikrų;
f) kitų panašaus poveikio specialių saugumo priemonių, kuriomis siekiama pavojų saugumui prevencijos arba kontrolės, visų pirma atsižvelgiant į Komisijos, kaip savininkės ar darbdavės, teises pagal galiojančius nacionalinius įstatymus.

2. Esant išskirtinėms aplinkybėms, Žmogiškųjų išteklių ir saugumo generalinio direktorato Saugumo direktorato personalo nariai, įgalioti pagal 5 straipsnį, gali imtis visų būtinų skubių priemonių, griežtai laikydamiesi 3 straipsnyje išdėstytų principų. Po to, kai buvo imtasi tų priemonių, jie kuo skubiau apie tai informuoja Saugumo direktorato direktorių, kuris Žmogiškųjų išteklių ir saugumo generalinio direktorato generalinio direktoriaus prašo atitinkamo įgaliojimo, kuriuo patvirtinamos priemonės, kurių buvo imtasi, ir suteikiamas leidimas bet kokiems tolesniems veiksmams, taip pat prireikus palaiko ryšį su kompetentingomis nacionalinėmis institucijomis.

3. Saugumo priemonės pagal šį straipsnį dokumentais įforminamos tada, kai jų imamasi, arba – tiesioginio pavojaus ar krizinės situacijos atveju – per protingą terminą po to, kai jų buvo imtasi. Pastaruoju atveju į dokumentus taip pat turi būti įtraukti elementai, kuriais remiantis įvertinta, ar būta tiesioginio pavojaus arba krizinės situacijos. Šie dokumentai gali būti glausti, tačiau turėtų būti sudaryti taip, kad asmuo, kuriam taikyta priemonė, galėtų pasinaudoti savo teisėmis į gynybą ir asmens duomenų apsaugą pagal Reglamentą (EB) Nr. 45/2001 ir kad būtų sudarytos sąlygos patikrinti priemonės teisėtumą. Informacija apie personalo nariui skirtas konkrečias saugumo priemones nėra jo asmens bylos dalis.

4. Imdamasi saugumo priemonių pagal b punktą, Komisija taip pat užtikrina, kad susijusiam asmeniui būtų suteikiama galimybė susisiekti su advokatu arba patikėtiniu ir būti informuotam apie teisę kreiptis į Europos duomenų apsaugos priežiūros pareigūną.

13 straipsnis

Tyrimai

1. Nedarant poveikio Tarnybos nuostatų 86 straipsniui ir IX priedui ir bet kokiam specialiam Komisijos ir EIVT susitarimui, pavyzdžiui, 2014 m. gegužės 28 d. Europos Komisijos Žmogiškųjų išteklių ir sau-

gumo generalinio direktorato ir Europos išorės veiksmų tarnybos pasirašytam susitarimui dėl rūpestingumo pareigos Komisijos darbuotojų Europos Sąjungos delegacijose atžvilgiu, saugumo tyrimai gali būti atliekami:

a) incidentų, turinčių įtakos saugumui Komisijoje, įskaitant įtariamą nusikalstamą veiką, atveju;
b) neskelbtinos neįslaptintos informacijos, ESĮI arba Euratomo įslaptintos informacijos galimo nutekėjimo, netinkamo naudojimo arba neteisėto atskleidimo atveju;
c) kontržvalgybos ir kovos su terorizmu aplinkybėmis;
d) rimtų kibernetinių incidentų atveju.

2. Sprendimą atlikti saugumo tyrimą priima Žmogiškųjų išteklių ir saugumo generalinio direktorato generalinis direktorius; jis taip pat gauna tyrimo ataskaitą.

3. Saugumo tyrimus atlieka tik paskirti Žmogiškųjų išteklių ir saugumo generalinio direktorato personalo nariai, tinkamai įgalioti pagal 5 straipsnį.

4. Įgaliotieji darbuotojai naudojasi su saugumo tyrimu susijusiomis teisėmis savarankiškai, kaip nurodyta įgaliojime, ir turi 12 straipsnyje išvardytas teises.

5. Įgaliotieji darbuotojai, turintys kompetenciją atlikti saugumo tyrimus, gali rinkti informaciją iš visų prieinamų šaltinių, susijusių su bet kokiomis administracinėmis ar baudžiamosiomis veikomis, kurios vykdytos Komisijos patalpose arba kuriose kaip tokių veikų aukos arba vykdytojai dalyvavo 2 straipsnio 3 dalyje nurodyti asmenys.

6. Žmogiškųjų išteklių ir saugumo generalinis direktoratas prireikus apie tai informuoja priimančiosios valstybės narės arba bet kurios kitos susijusios valstybės narės kompetentingas institucijas, visų pirma, jei per tyrimą nustatyta įvykdytos nusikalstamos veikos požymių. Atsižvelgdamas į tai, Žmogiškųjų išteklių ir saugumo generalinis direktoratas (jei tinka arba būtina) gali teikti paramą priimančiosios valstybės narės arba bet kurios kitos susijusios valstybės narės institucijoms.

7. Rimtų kibernetinių incidentų atveju Informatikos generalinis direktoratas glaudžiai bendradarbiauja su Žmogiškųjų išteklių ir saugumo generaliniu direktoratu, kad padėtų spręsti visus techninius klausimus. Žmogiškųjų išteklių ir saugumo generalinis direktoratas, konsultuodamasis su Informatikos generaliniu direktoratu, nusprendžia, jei tikslinga, informuoti priimančiosios valstybės arba bet kurios kitos susijusios vals-

tybės narės kompetentingas institucijas. Teikiant paramą kitoms susijusioms ES institucijoms ir agentūroms, naudojamasi Europos institucijų, įstaigų ir agentūrų Kompiuterinių incidentų tyrimo tarnybos (CERT-ES) incidentų koordinavimo paslaugomis.

8. Saugumo tyrimai įforminami dokumentais.

14 straipsnis

Kompetencijos sričių, susijusių su saugumo tyrimais ir kitų rūšių tyrimais, atskyrimas

1. Jei Žmogiškųjų išteklių ir saugumo generalinio direktorato Saugumo direktoratas atlieka 13 straipsnyje nurodytus saugumo tyrimus ir jei šie tyrimai patenka į Europos kovos su sukčiavimu tarnybos (OLAF) arba Komisijos tyrimų ir drausmės tarnybos (IDOC) kompetencijos sritį, jis iškart užmezga ryšį su tomis įstaigomis, visų pirma tam, kad nebūtų pakenkta tolesniems OLAF arba IDOC veiksmams. Žmogiškųjų išteklių ir saugumo generalinio direktorato Saugumo direktoratas prireikus kviečia OLAF arba IDOC dalyvauti atliekant tyrimą.

2. 13 straipsnyje nurodyti saugumo tyrimai nedaro poveikio OLAF ir IDOC įgaliojimams, nustatytiems tas įstaigas reglamentuojančiose taisyklėse. Atliekant OLAF ar IDOC inicijuotus tyrimus, Žmogiškųjų išteklių ir saugumo generalinio direktorato Saugumo direktorato gali būti paprašyta teikti techninę pagalbą.

3. Žmogiškųjų išteklių ir saugumo generalinio direktorato Saugumo direktorato gali būti paprašyta padėti OLAF darbuotojams patekti į Komisijos patalpas pagal Europos Parlamento ir Tarybos reglamento (ES, Euratomas) Nr. 883/2013 ([13]) 3 straipsnio 5 dalį ir 4 straipsnio 4 dalį, kad jiems būtų sudarytos sąlygos atlikti savo užduotis. Saugumo direktoratas apie tokius pagalbos prašymus informuoja Generalinį sekretorių ir Žmogiškųjų išteklių ir saugumo generalinio direktorato generalinį direktorių arba, jei toks tyrimas atliekamas Komisijos patalpose, kuriose yra jos narių arba Generalinis sekretorius, Komisijos pirmininką ir už žmogiškuosius išteklius atsakingą Komisijos narį.

4. Nedarant poveikio Tarnybos nuostatų 22a straipsniui, jei bylą galima priskirti tiek Žmogiškųjų išteklių ir saugumo generalinio direktorato Saugumo direktorato, tiek IDOC kompetencijos sričiai, Saugumo direktoratas, pagal 13 straipsnį pranešdamas apie tai Žmogiškųjų išteklių

generaliniam direktoriui, kuo ankstesniu etapu informuoja, ar yra priežasčių, dėl kurių į šią bylą reikėtų įtraukti IDOC. Laikoma, kad toks etapas pasiektas, kai išnyksta tiesioginė grėsmė saugumui. Sprendimą šiuo klausimu priima Žmogiškųjų išteklių ir saugumo generalinio direktorato generalinis direktorius.

5. Jei bylą galima priskirti tiek Žmogiškųjų išteklių ir saugumo generalinio direktorato Saugumo direktorato, tiek OLAF kompetencijos sričiai, Saugumo direktoratas nedelsdamas praneša apie tai Žmogiškųjų išteklių ir saugumo generalinio direktorato generaliniam direktoriui ir kuo ankstesniu etapu informuoja apie tai OLAF generalinį direktorių. Laikoma, kad toks etapas pasiektas, kai išnyksta tiesioginė grėsmė saugumui.

15 straipsnis

Saugumo patikrinimai

1. Žmogiškųjų išteklių ir saugumo generalinis direktoratas vykdo saugumo patikrinimus, siekdamas nustatyti, ar Komisijos tarnybos ir asmenys laikosi šio sprendimo ir jo įgyvendinimo taisyklių, ir parengti rekomendacijas, kai manoma, kad tai būtina.

2. Žmogiškųjų išteklių ir saugumo generalinis direktoratas prireikus vykdo saugumo patikrinimus, saugumo stebėseną arba vertinamuosius vizitus, kad patikrintų, ar remiantis saugumo taisyklėmis, normomis ir standartais, kurie yra bent jau lygiaverčiai Komisijos taisyklėms, yra tinkamai užtikrinamas Komisijos darbuotojų, turto ir informacijos saugumas, už kurį atsako kitos Europos Sąjungos institucijos, agentūros ar įstaigos, taip pat valstybės narės, trečiosios valstybės ar tarptautinės organizacijos. Prireikus, laikantis geranoriško administracijų bendradarbiavimo principo, į minėtus saugumo patikrinimus taip pat įtraukiami patikrinimai, atliekami tada, kai įslaptinta informacija keičiamasi su kitomis Europos Sąjungos institucijomis, įstaigomis ir agentūromis, taip pat valstybėmis narėmis, trečiosiomis valstybėmis ar tarptautinėmis organizacijomis.

3. Komisijos darbuotojų Europos Sąjungos delegacijose atžvilgiu šis straipsnis įgyvendinamas *mutatis mutandis*, nedarant poveikio bet kokiam specialiam Komisijos ir EIVT susitarimui, pavyzdžiui, 2014 m. gegužės 28 d. Europos Komisijos Žmogiškųjų išteklių ir saugumo generalinio direktorato ir Europos išorės veiksmų tarnybos pasirašytam susitarimui dėl rūpestingumo pareigos Komisijos darbuotojų Europos Sąjungos

delegacijose atžvilgiu.

16 straipsnis

Parengties lygiai ir krizinių situacijų valdymas

1. Žmogiškųjų išteklių ir saugumo generalinis direktoratas atsako už tai, kad būtų parengtos parengties lygių priemonės, tinkamos grėsmėms ir incidentams, turintiems įtakos saugumui Komisijoje, numatyti ir reaguoti į juos, taip pat už priemones, būtinas krizinėms situacijoms valdyti.

2. 1 dalyje nurodytos parengties lygių priemonės atitinka grėsmės saugumui lygį. Parengties lygiai nustatomi glaudžiai bendradarbiaujant su kitų Europos Sąjungos institucijų, agentūrų ir įstaigų, taip pat valstybės (-ių) narės (-ių), kurioje (-iose) yra Komisijos patalpų, kompetentingomis tarnybomis.

3. Žmogiškųjų išteklių ir saugumo generalinis direktoratas yra parengties lygių ir krizinių situacijų valdymo ryšių punktas.

4 SKYRIUS

ORGANIZACINĖ STRUKTŪRA

17 straipsnis

Bendroji Komisijos tarnybų atsakomybė

1. Šiame sprendime nurodyta Komisijos atsakomybė tenka Žmogiškųjų išteklių ir saugumo generaliniam direktoratui, kuriam vadovauja ir už kurį atsako už saugumą atsakingas Komisijos narys.

2. Specialios su kibernetiniu saugumu susijusios priemonės nustatytos Sprendime (2006) 3602.

3. Atsakomybė už šio sprendimo ir jo taisyklių įgyvendinimą ir už kasdienį jų laikymąsi gali būti perduota kitiems Komisijos padaliniams, jeigu decentralizuotas saugumo užtikrinimas yra daug veiksmingesnis ir padeda sutaupyti daug išlaidų arba laiko dėl, pavyzdžiui, atitinkamų tarnybų geografinės padėties.

4. Jei taikoma 3 dalis, Žmogiškųjų išteklių ir saugumo generalinis di-

rektoratas ir prireikus Informatikos generalinis direktoratas sudaro su atskirais Komisijos padaliniais susitarimus, kuriais nustatomos aiškios funkcijos ir atsakomybė už saugumo politikos įgyvendinimą ir stebėjimą.

18 straipsnis

Žmogiškųjų išteklių ir saugumo generalinis direktoratas

1. Žmogiškųjų išteklių ir saugumo generalinis direktoratas visų pirma atsako už:

1) Komisijos saugumo politikos, įgyvendinimo taisyklių ir saugumo pranešimų rengimą;
2) informacijos rinkimą siekiant įvertinti grėsmes ir pavojus saugumui ir visus aspektus, kurie gali turėti įtakos saugumui Komisijoje;
3) kovos su elektroniniu sekimu priemonių ir visų Komisijos darbo vietų apsaugos užtikrinimą, deramai atsižvelgiant į grėsmės vertinimus ir Komisijos interesus pažeidžiančios neteisėtos veiklos įrodymus;
4) pagalbos tarnybos veiklą 24 valandas per parą / 7 dienas per savaitę, Komisijos tarnyboms ir darbuotojams kreipiantis bet kokiu su sauga ir saugumu susijusiu klausimu;
5) saugumo priemonių, kuriomis siekiama mažinti grėsmes saugumui, įgyvendinimą ir tinkamų RIS kūrimą bei priežiūrą siekiant tenkinti Komisijos veiklos poreikius, visų pirma šiose srityse: fizinės prieigos kontrolės, saugumo leidimų administravimo ir neskelbtinos informacijos bei ES įslaptintos informacijos tvarkymo;
6) informuotumo didinimą, treniruočių ir pratybų organizavimą, mokymų ir konsultacijų visais saugumo Komisijoje klausimais teikimą siekiant puoselėti saugumo kultūrą ir burti personalą, kuris būtų tinkamai parengtas saugumo srityje.

2. Žmogiškųjų išteklių ir saugumo generalinis direktoratas, nedarydamas poveikio kitų Komisijos tarnybų kompetencijai ir atsakomybei, užtikrina išorės ryšių palaikymą:

1) su kitų Sąjungos institucijų, agentūrų ir įstaigų saugumo padaliniais – klausimais, susijusiais su asmenų, turto ir informacijos saugumu Komisijoje;
2) su valstybių narių, trečiųjų šalių ir tarptautinių organizacijų bei įstaigų saugumo, žvalgybos ir grėsmės vertinimo tarnybomis, įskaitant nacionalines saugumo institucijas, – klausimais, turinčiais įtakos asmenų, turto ir informacijos saugumui Komisijoje;

3) su policija ir kitomis pagalbos tarnybomis – visais įprastais ar kritiniais klausimais, turinčiais įtakos Komisijos saugumui;
4) su kitų Europos Sąjungos institucijų, agentūrų ir įstaigų, taip pat valstybių narių ir trečiųjų šalių saugumo institucijomis reaguojant į kibernetinius išpuolius, kurie galėtų daryti poveikį saugumui Komisijoje;
5) dėl žvalgybos informacijos, susijusios su terorizmo ir šnipinėjimo veiklos keliama grėsme saugumui Komisijoje, gavimo, vertinimo ir sklaidos;
6) dėl klausimų, susijusių su įslaptinta informacija, kaip nurodyta išsamiau Komisijos sprendime (ES, Euratomas) 2015/444 ([14]).

3. Žmogiškųjų išteklių ir saugumo generalinis direktoratas atsako už saugų pagal šį straipsnį vykdomą informacijos perdavimą, įskaitant asmens duomenų perdavimą.

19 straipsnis

Komisijos saugumo ekspertų grupė (ComSEG)

Įsteigiama Komisijos saugumo ekspertų grupė, kuriai suteikiami įgaliojimai prireikus patarti Komisijai klausimais, susijusiais su jos vidaus saugumo politika ir ypač ES įslaptintos informacijos apsauga.

20 straipsnis

Vietos saugumo pareigūnai (VSP)

1. Kiekvienas Komisijos padalinys ar kabinetas skiria vietos saugumo pareigūną (VSP), kuris veikia kaip pagrindinis tarnybos asmuo ryšiams su Žmogiškųjų išteklių ir saugumo generaliniu direktoratu visais saugumo Komisijoje klausimais. Jei tikslinga, gali būti skiriamas vienas ar daugiau VSP pavaduotojų. VSP turi būti pareigūnas arba laikinasis darbuotojas.

2. Kaip pagrindinis savo Komisijos padalinio ar kabineto asmuo ryšiams saugumo klausimais, vietos saugumo pareigūnas Žmogiškųjų išteklių ir saugumo generaliniam direktoratui ir savo vadovybei ataskaitas saugumo savo Komisijos padalinyje klausimais teikia reguliariai, o apie saugumo incidentus, įskaitant atvejus, kai galėjo būti atskleista ESĮI arba neskelbtina neįslaptinta informacija, praneša nedelsdamas.

3. Jei klausimai yra susiję su ryšių ir informacinių sistemų saugumu, VSP palaiko ryšius su savo Komisijos padalinio vietos informatikos saugumo pareigūnu (VISP), kurio funkcijos ir pareigos nustatytos Sprendime C(2006) 3602.

4. VSP prisideda prie saugumo mokymų ir informuotumo saugumo klausimais didinimo veiklos, skirtos konkretiems Komisijos padalinyje dirbančių darbuotojų, rangovų ir kitų asmenų poreikiams tenkinti.

5. Didelių ar tiesioginių pavojų saugumui arba ekstremaliųjų situacijų atvejais Žmogiškųjų išteklių ir saugumo generalinio direktorato prašymu vietos saugos pareigūnui gali būti skiriamos konkrečios užduotys. Žmogiškųjų išteklių ir saugumo generalinis direktoratas apie tas konkrečias užduotis informuoja VSP vietos generalinio direktorato generalinį direktorių arba žmogiškųjų išteklių direktorių.

6. VSP pareigos nedaro poveikio vietos informatikos saugumo pareigūnų (VISP), sveikatos ir saugos vadovų ir registracijos kontrolės pareigūnų (RKP) funkcijoms bei pareigoms arba bet kokioms kitoms pareigybėms, kurioms tenka su saugumu ar sauga susijusi atsakomybė. VSP palaiko su jais ryšius tam, kad būtų užtikrintas nuoseklus ir darnus požiūris į saugumą ir sklandus keitimasis informacija saugumo Komisijoje klausimais.

7. Teikdamas informaciją tiesioginei vadovybei, VSP tiesiogiai bendrauja su savo generaliniu direktoriumi arba tarnybos vadovu. VSP turi saugumo leidimą susipažinti su ESĮI, pažymėta bent jau SECRET UE/ES SECRET lygio slaptumo žyma.

8. Kad būtų skatinamas keitimasis informacija ir geriausios praktikos pavyzdžiais, Žmogiškųjų išteklių ir saugumo generalinis direktoratas ne rečiau kaip du kartus per metus rengia VSP konferencijas. VSP dalyvavimas šiose konferencijose privalomas.

5 SKYRIUS

ĮGYVENDINIMAS

21 straipsnis

Įgyvendinimo taisyklės ir saugumo pranešimai

1. Prireikus, visapusiškai laikantis vidaus darbo tvarkos taisyklių, šio sprendimo įgyvendinimo taisyklės priimamos atskiru Komisijos sprendimu dėl įgaliojimų suteikimo už saugumo reikalus atsakingam Komisijos nariui.

2. Gavęs įgaliojimus pagal pirmiau minėtą Komisijos sprendimą, už saugumo reikalus atsakingas Komisijos narys gali rengti saugumo pranešimus, kuriuose nustatomos saugumo gairės ir geriausios praktikos pavyzdžiai šio sprendimo ir jo įgyvendinimo taisyklių taikymo srityje.

3. Visapusiškai laikydamasi vidaus darbo tvarkos taisyklių, Komisija pirmoje ir antroje šio straipsnio dalyse minėtas užduotis atskiru sprendimu dėl įgaliojimų perdavimo gali pavesti Žmogiškųjų išteklių ir saugumo generalinio direktorato generaliniam direktoriui.

6 SKYRIUS

KITOS IR BAIGIAMOSIOS NUOSTATOS

22 straipsnis

Asmens duomenų tvarkymas

1. Asmens duomenis, būtinus šiam sprendimui įgyvendinti, Komisija tvarko pagal Reglamentą (EB) Nr. 45/2001.

2. Nepaisant priemonių, kurios šio sprendimo priėmimo momentu jau yra vykdomos ir apie kurias pranešta Europos duomenų apsaugos priežiūros pareigūnui ([15]), bet kokiai priemonei, susijusiai su asmens duomenų (pavyzdžiui, duomenų, susijusių su patekimo į patalpas ir išvykimo iš jų registracijos žurnalais, AVSS įrašais, telefono skambučių budinčioms tarnyboms ir išsiuntimo centrams įrašais ir panašiais duome-

nimis, kurių reikia saugumo arba atsako į krizę tikslais) tvarkymu pagal šį sprendimą taikomos 21 straipsnyje nurodytos įgyvendinimo taisyklės, kuriomis nustatomos tinkamos duomenų subjektų apsaugos priemonės.

3. Žmogiškųjų išteklių ir saugumo generalinio direktorato generalinis direktorius yra atsakingas už bet kokio asmens duomenų tvarkymo, vykdomo įgyvendinant šį sprendimą, saugumą.

4. Tos įgyvendinimo taisyklės ir procedūros priimamos pasikonsultavus su duomenų apsaugos pareigūnu ir Europos duomenų apsaugos priežiūros pareigūnu pagal Reglamentą (EB) Nr. 45/2001.

23 straipsnis

Skaidrumas

Apie šį sprendimą ir jo įgyvendinimo taisykles informuojami Komisijos darbuotojai ir visi asmenys, kuriems jie taikomi.

24 straipsnis

Ankstesnių sprendimų panaikinimas

Sprendimas (94) 2129 panaikinamas.

25 straipsnis

Įsigaliojimas

Šis sprendimas įsigalioja kitą dieną po jo paskelbimo *Europos Sąjungos oficialiajame leidinyje*.

Priimta Briuselyje 2015 m. kovo 13 d.

Komisijos vardu

Pirmininkas

Jean-Claude JUNCKER

([1]) Žr. 2004 m. gruodžio 31 d. „Arrangement entre le Gouvernement belge et le Parlement européen, le Conseil, la Commission, le Comité économique et social européen, le Comité des régions, la Banque européenne d'investissement en matière de sécurité", 2007 m. sausio 20 d.

„Accord de sécurité signé entre la Commission et le Gouvernement luxembourgeois“ ir 1959 m. liepos 22 d. „Accordo tra il Governo italiano e la Commissione europea dell‘energia atomica (Euratomas) per l‘istituzione di un Centro comune di ricerche nucleari di competenza generale“.

([2]) DPO-914.2, DPO-93.7, DPO-153.3, DPO-870.3, DPO-2831.2, DPO-1162.4, DPO-151.3, DPO-3302.1, DPO-508.6, DPO-2638.3, DPO-544.2, DPO-498.2, DPO-2692.2, DPO-2823.2.

([3]) 1994 m. rugsėjo 8 d. Komisijos sprendimas C(94) 2129 dėl Saugumo tarnybos uždavinių.

([4]) 2000 m. gruodžio 18 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 45/2001 dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo (OL L 8, 2001 1 12, p. 1).

([5]) 1968 m. vasario 29 d. Tarybos reglamentas (EEB, Euratomas, EAPB) Nr. 259/68, nustatantis Europos Bendrijų pareigūnų tarnybos nuostatus ir kitų Europos Bendrijų tarnautojų įdarbinimo sąlygas bei Komisijos pareigūnams laikinai taikomas specialias priemones (Kitų tarnautojų įdarbinimo sąlygos) (OL L 56, 1968 3 4, p. 1).

([6]) 2013 m. balandžio 19 d. Europos Sąjungos vyriausiojo įgaliotinio užsienio reikalams ir saugumo politikai sprendimas 2013/C 190/01 dėl Europos išorės veiksmų tarnybos saugumo taisyklių (OL C 190, 2013 6 29, p. 1).

([7]) 2002 m. sausio 23 d. Komisijos sprendimas 2002/47/EB, EAPB, Euratomas, iš dalies keičiantis jos darbo tvarkos taisykles (OL L 21, 2002 1 24, p. 23), kurio priede pateiktos nuostatos dėl dokumentų tvarkymo.

([8]) 2004 m. liepos 7 d. Komisijos sprendimas 2004/563/EB, Euratomas, iš dalies keičiantis jos darbo tvarkos taisykles (OL L 251, 2004 7 27, p. 9), kurio priede pateiktos nuostatos dėl elektroninių ir skaitmeninių dokumentų.

([9]) 2006 m. balandžio 21 d. Sprendimas C(2006) 1623 dėl visiems Europos Komisijos darbuotojams taikomos suderintos sveikatos ir saugos darbe politikos.

([10]) 2006 m. rugpjūčio 16 d. Sprendimas C(2006) 3602 dėl Europos Komisijos naudojamų informacinių sistemų saugumo.

([11]) 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (OL L 281, 1995 11 23, p. 31).

([12]) 2001 m. gegužės 30 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 1049/2001 dėl galimybės visuomenei susipažinti su Europos Parlamento, Tarybos ir Komisijos dokumentais (OL L 145, 2001 5 31, p. 43).

([13]) 2013 m. rugsėjo 11 d. Europos Parlamento ir Tarybos reglamentas (ES, Euratomas) Nr. 883/2013 dėl Europos kovos su sukčiavimu tarnybos (OLAF) atliekamų tyrimų ir kuriuo panaikinami Europos Parlamento ir Tarybos reglamentas (EB) Nr. 1073/1999 ir Tarybos reglamentas (Euratomas) Nr. 1074/1999 (OL L 248, 2013 9 18, p. 1).

([14]) 2015 m. kovo 13 d. Komisijos sprendimas (ES, Euratomas) 2015/444 dėl ES įslaptintos informacijos apsaugai užtikrinti skirtų saugumo taisyklių (žr. šio Oficialiojo leidinio p. 53).

([15]) DPO-914.2, DPO-93.7, DPO-153.3, DPO-870.3, DPO-2831.2, DPO-1162.4, DPO-151.3, DPO-3302.1, DPO-508.6, DPO-2638.3, DPO-544.2, DPO-498.2, DPO-2692.2, DPO-2823.2.

2.10. COMMISSION DECISION (EU, EURATOM) 2015/443 OF 13 MARCH 2015 ON SECURITY IN THE COMMISSION

COMMISSION DECISION (EU, Euratom) 2015/443

of 13 March 2015

on Security in the Commission

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 249 thereof,

Having regard to the Treaty establishing the European Atomic Energy Community,

Having regard to the Protocol No 7 on the Privileges and Immunities of the European Union annexed to the Treaties, and in particular Article 18 thereof,

Whereas:

(1) The objective of security within the Commission is to enable the Commission to operate in a safe and secure environment by establishing a coherent, integrated approach as regards its security, providing appropriate levels of protection for persons, assets and information commensurate with identified risks, and ensuring efficient and timely delivery of security.

(2) The Commission, like other international bodies, faces major threats and challenges in the field of security, in particular as regards terrorism, cyberattacks and political and commercial espionage.

(3) The European Commission has entered into instruments on security matters for its principal sites with the governments of Belgium, Luxembourg and Italy ([1]). These instruments confirm that the Commission is responsible for its security.

(4) In order to ensure security of persons, assets and information, the Commission may need to take measures in areas protected by fundamental rights as enshrined in the Charter of Fundamental Rights and in the European Convention on Human Rights and as recognised by the European Court of Justice.

(5) Any such measure should therefore be justified by the importance of the interest it is designed to protect, be proportionate and ensure full respect for fundamental rights, including especially the rights of privacy and data protection.

(6) Within a system committed to the rule of law and the respect of fundamental rights, the Commission has to strive for an appropriate level of security for its staff, assets and information that ensures it can carry out its operations, while not limiting fundamental rights beyond what is strictly necessary.

(7) Security in the Commission shall be based on the principles of legality, transparency, proportionality and accountability.

(8) Members of staff mandated to take security measures should not be placed at any disadvantage because of their actions unless they acted outside the scope of their mandate or in violation of the law, and hence in this respect this Decision is to be considered as a service instruction within the meaning of the Staff Regulations.

(9) The Commission should take appropriate initiatives to foster and strengthen its security culture, ensuring a more efficient delivery of security, improving its security governance, further intensifying networks and cooperation with relevant authorities at international, European and national level, and improving monitoring and control of the implementation of security measures.

(10) The establishment of the European External Action Service (EEAS) as a functionally autonomous body of the Union has had a significant impact on the Commission's security interests, and hence requires that rules and procedures for cooperation as regards safety and security be established between the EEAS and the Commission, in particular with regard to the fulfilment of the Commission's duty-of-care responsibilities towards Commission staff in Union Delegations.

(11) The security policy of the Commission should be implemented in a manner which is consistent with other internal processes and procedures that may involve a security element. These include, in particular, Business Continuity Management which aims at preserving the critical functions of the Commission in case of an operational disruption, and the ARGUS process for multisectoral crisis coordination.

(12) Notwithstanding the measures already in place at the time of adoption of this Decision and notified to the European Data Protection Supervisor ([2]), any measure under this Decision involving the processing of personal data shall be subject to implementing rules in accordance with Article 21, which shall lay down appropriate safeguards for data subjects.

(13) Therefore, there is a need for the Commission to review, update, and consolidate the existing regulatory basis for security at the Commission.

(14) The Commission Decision C(94) 2129 ([3]) should therefore be repealed,

HAS ADOPTED THIS DECISION:

CHAPTER 1

GENERAL PROVISIONS

Article 1

Definitions

For the purposes of this Decision the following definitions apply:

(1) **'assets'** means all movable and immovable property and possessions of the Commission;

(2) **'Commission department'** means a Commission Directorate-General or service, or a Cabinet of a Member of the Commission;

(3) **'Communication and Information System'** or 'CIS' means any system enabling the handling of information in electronic form, including all assets required for its operation, as well as the infrastructure, organisation, personnel and information resources;

(4) **'Control of risks'** shall mean any security measure that can reasonably be expected to effectively control a risk to security by its prevention, mitigation, avoidance or transfer;

(5) **'crisis situation'** means a circumstance, event, incident or emergency (or a succession or combination thereof) posing a major or an immediate threat to security in the Commission regardless of its origin;

(6) **'data'** means information in a form that allows it to be communicated, recorded or processed;

(7) **'Member of the Commission responsible for security'** means a Member of the Commission under whose authority the Directorate-General for Human Resources and Security falls;

(8) **'personal data'** means personal data as defined in Article 2(a) of Regulation (EC) No 45/2001 of the European Parliament and of the Council ([4]);

(9) **'premises'** shall mean any immovable or assimilated property and possessions of the Commission;

(10) **'prevention of risk'** shall mean security measures that can reasonably be expected to impede, delay or stop a risk to security;

(11) **'risk to security'** means the combination of the threat level, the level of vulnerability and the possible impact of an event;

(12) **'security in the Commission'** means the security of persons, assets and information in the Commission, and in particular the physical integrity of persons and assets, the integrity, confidentiality and availability of information and communication and information systems, as well as the unobstructed functioning of Commission operations;

(13) **'security measure'** means any measure taken in accordance with this Decision for purposes of controlling risks to security;

(14) **'Staff Regulations'** means the Staff Regulations of officials of the European Union, as laid down by Regulation (EEC, Euratom, ECSC) No 259/68 of the Council ([5]) and its amending acts;

(15) **'threat to security'** means an event or agent that can reasonably be expected to adversely affect security if not responded to and controlled;

(16) **'immediate threat to security'** means a threat to security which occurs with no or with extremely short advance warning; and

(17) **'major threat to security'** means a threat to security that can reasonably be expected to lead to loss of life, serious injury or harm, significant damage to property, compromise of highly sensitive information, disruption of IT systems or of essential operational capacities of the Commission;

(18) **'vulnerability'** means a weakness of any nature that can reasonably be expected to adversely affect security in the Commission, if exploited by one or more threats.

Article 2

Subject matter

1. This Decision sets out the objectives, basic principles, organisation and responsibilities regarding security at the Commission.

2. This Decision shall apply to all Commission departments and in all premises of the Commission. Commission staff working in Union Delegations shall be subject to the security rules for the European External Action Service ([6]).

3. Notwithstanding any specific indications concerning particular groups of staff, this Decision shall apply to the Members of the Commission, to Commission staff under the scope of the Staff Regulations and of the Conditions of Employment of other servants of the European Union, to national experts seconded to the Commission (SNEs), to service providers and their staff, to trainees and to any individual with access to Commission buildings or other assets, or to information handled by the Commission.

4. The provisions of this Decision shall be without prejudice to Commission Decision 2002/47/EC, ECSC, Euratom ([7]) and Commission Decision 2004/563/EC, Euratom ([8]), Commission Decision C(2006) 1623 ([9]) and Commission Decision C(2006) 3602 ([10]).

CHAPTER 2

PRINCIPLES

Article 3

Principles for security in the Commission

1. In implementing this Decision, the Commission shall comply with the Treaties and in particular the Charter of Fundamental Rights and Protocol No 7 on the Privileges and Immunities of the European Union, with the instruments referred to in recital 2 with any applicable rules of national law as well as with the terms of the present Decision. If necessary, a security notice in the sense of Article 21(2) providing guidance in this respect shall be issued.

2. Security in the Commission shall be based on the principles of legality, transparency, proportionality and accountability.

3. The principle of legality indicates the need to stay strictly within the legal framework in implementing this Decision and the need to conform to the legal requirements.

4. Any security measure shall be taken overtly unless this can reasonably be expected to impair its effect. Addressees of a security measure shall be informed in advance of the reasons for and the impact of the measure, unless the effect of the measure can reasonably be expected to be impaired by providing such information. In this case, the addressee of the security measure shall be informed after the risk of impairing the effect of the security measure has ceased.

5. Commission departments shall ensure that security issues are taken into account from the start of the development and implementation of Commission policies, decisions, programmes, projects and activities for which they are responsible. In order to do so, they shall involve the Directorate-General for Human Resources and Security in general and the Chief Information Security Officer of the Commission as regards IT systems from the earliest stages of preparation.

6. The Commission shall, where appropriate, seek cooperation with the competent authorities of the host state, of other Member States and of other EU institutions, agencies or bodies, where feasible, taking account

of the measures taken or planned by those authorities to address the risk to security concerned.

Article 4

Obligation to comply

1. Compliance with this Decision and its implementing rules and with the security measures and the instructions given by mandated staff shall be mandatory.

2. Non-compliance with the security rules may trigger liability to disciplinary action in accordance with the Treaties, the Staff Regulations, to contractual sanctions and/or to legal action under national laws and regulations.

CHAPTER 3

DELIVERING SECURITY

Article 5

Mandated staff

1. Only staff authorised on the basis of a nominative mandate conferred to them by the Director-General for Human Resources and Security, given their current duties, may be entrusted with the power to take one or several of the following measures:
(1) Carry side arms;
(2) Conduct security inquiries as referred to in Article 13;
(3) Take security measures as referred to in Article 12 as specified in the mandate.

2. The mandates referred to in paragraph 1 shall be conferred for a duration which shall not exceed the period during which the person concerned hold the post or function in respect of which the mandate has been conferred. They shall be conferred in compliance with the applicable provisions set out in Article 3(1).

3. As regards mandated staff, this Decision constitutes a service instruction within the meaning of Article 21 of the Staff Regulations.

Article 6

General provisions regarding security measures

1. When taking security measures, the Commission shall in particular ensure so far as reasonably possible, that:

(a) it only seeks support or assistance from the state concerned, provided that that state either is a Member State of the European Union or, if not, party to the European Convention on Human Rights, or guarantees rights which are at least equivalent to the rights guaranteed in this Convention;

(b) it shall only transfer information on an individual to recipients, other than Community institutions and bodies, which are not subject to national law adopted pursuant to Directive 95/46/EC of the European Parliament and of the Council ([11]), in accordance with Article 9 of Regulation (EC) No 45/2001;

(c) where an individual poses a threat to security, any security measure shall be directed against that individual and that individual may be subjected to bearing the incurring costs. Those security measures may only be directed against other individuals if an immediate or major threat to security must be controlled and the following conditions are fulfilled:

(a) the envisaged measures against the individual posing the threat to security cannot be taken or are not likely to be effective;

(b) the Commission cannot control the threat to security by its own actions or cannot do so in a timely manner;

(c) the measure does not constitute a disproportionate danger for the other individual and his rights.

2. The Security Directorate of the Directorate-General for Human Resources and Security shall establish an overview of security measures which may require an order by a judge in accordance with the laws and regulations of the Member States hosting Commission premises.

3. The Security Directorate of the Directorate-General for Human Resources and Security may turn to a contractor to carry out, under the direction and supervision of the Security Directorate, tasks relating to security.

Article 7

Security measures regarding persons

1. An appropriate level of protection shall be afforded to persons in the premises of the Commission, taking into account security and safety requirements.

2. In case of major risks to security, the Directorate-General for Human Resources and Security shall provide close protection for Members of the Commission or other staff where a threat assessment has indicated that such protection is needed to ensure their safety and security.

3. In case of major risks to security, the Commission may order the evacuation of its premises.

4. Victims of accidents or attacks within Commission premises shall receive assistance.

5. In order to prevent and control risks to security, mandated staff may carry out background checks of persons falling under the scope of this Decision, so as to determine whether giving such persons access to Commission premises or information presents a threat to security. For that purpose, and in compliance with Regulation (EC) No 45/2001 and provisions referred to under Article 3(1), the mandated staff concerned may:

(a) use any source of information available to the Commission, taking into account the reliability of the source of information;

(b) access the personnel file or data the Commission holds with regard to individuals it employs or intends to employ, or for contractors' staff when duly justified.

Article 8

Security measures regarding physical security and assets

1. Security of assets shall be ensured by applying appropriate physical and technical protective measures and corresponding procedures, hereinafter called 'physical security', creating a multi-layered system.

2. Measures may be adopted pursuant to this Article in order to protect persons or information in the Commission as well as to protect assets.

3. Physical security shall have the following objectives:

– preventing acts of violence directed against Members of the Commission or persons falling within the scope of this Decision,
– preventing espionage and eavesdropping on sensitive or classified information,
– preventing theft, acts of vandalism, sabotage and other violent actions aimed at damaging or destroying Commission buildings and assets,
– enabling investigation and inquiry into security incidents including through checks on access and exit control log files, CCTV coverage, telephone call recordings and similar data as referred to in Article 22(2) hereunder and other information sources.

4. Physical security shall include:

– an access policy applicable to any person or vehicle requiring access to Commission premises, including the parking lots,
– an access control system comprising guards, technical equipment and measures, information systems or a combination of all of those elements.

5. In order to ensure physical security, the following actions may be taken:

– recording entry to and exit from Commission premises of persons, vehicles, goods and equipment,
– identity controls at its premises,
– inspection of vehicles, goods and equipment by visual or technical means,
– preventing unauthorised persons, vehicles and goods, from entering Commission premises.

Article 9

Security measures regarding information

1. Security of information covers all information handled by the Commission.

2. Security of information, regardless of its form, shall balance transparency, proportionality, accountability and efficiency with the need to protect information from unauthorised access, use, disclosure, modification or destruction.

3. Security of information shall be aimed at protecting confidentiality, integrity and availability.

4. Risk management processes shall therefore be used to classify information assets and to develop proportionate security measures, procedures and standards, including mitigating measures.

5. These general principles underlying security of information shall be applied in particular as regards:

(a) 'European Union Classified Information' (hereafter 'EUCI'), that is to say any information or material designated by an EU security classification, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States;

(b) 'Sensitive non-classified information', that is to say information or material the Commission must protect because of legal obligations laid down in the Treaties or in acts adopted in implementation thereof, and/or because of its sensitivity. Sensitive non-classified information includes, but is not limited to, information or material covered by the obligation of professional secrecy, as referred to in Article 339 TFEU, information covered by the interests protected in Article 4 of Regulation (EC) No 1049/2001 of the European Parliament and of the Council ([12]) read in conjunction with the relevant case-law of the Court of Justice of the European Union or personal data within the scope of Regulation (EC) No 45/2001.

6. Sensitive non-classified information shall be subject to rules regarding its handling and storage. It shall only be released to those individuals who have a 'need-to-know'. When deemed necessary for the effective protection of its confidentiality, it shall be identified by a security marking and corresponding handling instructions approved by the Director-General for Human Resources and Security. When handled or stored on Communication and Information Systems, such information shall be protected also in compliance with Decision C(2006) 3602, its implementing rules and corresponding standards.

7. Any individual who is responsible for compromising or losing EUCI or sensitive non-classified information, which is identified as such in the rules regarding its handling and storage, may be liable to disciplinary action in accordance with the Staff Regulations. That disciplinary action shall be without prejudice to any further legal or criminal proceedings by the competent national authorities of the Member States in accordance with their laws and regulations and to contractual remedies.

Article 10

Security measures regarding Communication and Information Systems

1. All Communication and Information Systems (‘CIS’) used by the Commission shall comply with the Commission‘s Information Systems Security Policy, as set out in Decision C(2006) 3602, its implementing rules and corresponding security standards.

2. Commission services owning, managing or operating CIS shall only allow other Union institutions, agencies, bodies or other organisations to have access to those systems provided that those Union institutions, agencies, bodies or other organisations can provide reasonable assurance that their IT systems are protected at a level equivalent to the Commission's Information Systems Security Policy as set out in Decision C(2006) 3602, its implementing rules and corresponding security standards. The Commission shall monitor such compliance, and in case of serious non-compliance or continued failure to comply, be entitled to prohibit access.

Article 11

Forensic analysis regarding cyber-security

The Directorate-General for Human Resources and Security shall in particular be responsible for conducting forensic technical analysis in cooperation with the competent Commission departments in support of the security inquiries referred to in Article 13, related to counterintelligence, data leakage, cyberattacks and information systems security.

Article 12

Security measures regarding persons and objects

1. In order to ensure the security in the Commission and to prevent and control risks, staff mandated in accordance with Article 5 may, in compliance with the principles set out in Article 3, take inter alia one or more of the following security measures:

(a) securing of scenes and evidence, including access and exit control log files, CCTV images, in case of incidents or conduct that may lead to administrative, disciplinary, civil or criminal procedures;
(b) limited measures concerning persons posing a threat to security, including ordering persons to leave the Commission's premises, escorting persons from the Commission's premises, banning persons from the Commission's premises for a period of time, the latter defined in accordance with criteria to be defined in implementing rules;
(c) limited measures concerning objects posing a threat to security including removal, seizure and disposal of objects;
(d) searching of Commission premises, including of offices, within such premises;
(e) searching of CIS and equipment, telephone and telecommunications traffic data, log files, user accounts, etc.;
(f) other specific security measures with similar effect in order to prevent or control risks to security, in particular in the context of the Commission's rights as a landlord or as an employer in accordance with the applicable national laws.

2. Under exceptional circumstances, staff members of the Security Directorate of the Directorate-General for Human Resources and Security, mandated in accordance with Article 5, may take any urgent measures needed, in strict compliance with the principles laid down in Article 3. As soon as possible after having taken those measures, they shall inform the Director of the Security Directorate, who shall seek the appropriate mandate from the Director-General for Human Resources and Security, confirming the measures taken and authorising any further necessary actions and shall liaise, where appropriate with the competent national authorities.

3. Security measures pursuant to this Article shall be documented at the time they are taken or, in the event of an immediate risk or a crisis situation, within reasonable delay after they are taken. In the latter case, the documentation must also include the elements on which the assessment regarding the existence of an immediate risk or a crisis situation was based. The documentation can be concise, but should be constituted in such a way as to allow the person subjected to the measure to exercise his rights of defence and of protection of personal data in accordance with Regulation (EC) No 45/2001, and to allow a scrutiny

as to the legality of the measure. No information about specific security measures addressed to a member of staff shall be part of the person's personnel file.

4. When taking security measures pursuant to point (b), the Commission shall in addition guarantee that the individual concerned is given the opportunity to contact a lawyer or a person of his confidence and be made aware of their right to have recourse to the European Data Protection Supervisor.

Article 13

Inquiries

1. Without prejudice to Article 86 and Annex IX of the Staff Regulations and to any special arrangement between the Commission and the EEAS, such as the special arrangement signed on 28 May 2014 between the Directorate General for Human Resources and Security of the European Commission and the European External Action Service on the duty of care towards Commission staff posted in Union Delegations, security inquiries may be conducted:

(a) in case of incidents affecting security at the Commission, including suspected criminal offences;
(b) in case of potential leakage, mishandling or compromise of sensitive non-classified information, EUCI or Euratom Classified Information;
(c) in the context of counter-intelligence and counter-terrorism;
(d) in case of serious cyber-incidents.

2. The decision to conduct a security inquiry shall be taken by the Director-General for Human Resources and Security who will also be the recipient of the inquiry report.

3. Security inquiries shall be conducted only by dedicated members of staff of the Directorate-General for Human Resources and Security, duly mandated in accordance with Article 5.

4. The mandated staff shall exercise their powers of security inquiry independently, as specified in the mandate and shall have the powers listed in Article 12.

5. Mandated staff having the competence to conduct security inquiries may gather information from all available sources related to any administrative or criminal offences committed within the Commission premises or involving persons referred to in Article 2(3) either as victim

or perpetrator of such offences.

6. The Directorate-General for Human Resources and Security shall inform the competent authorities of the host Member State or any other Member State concerned, where appropriate, and in particular if the inquiry has given rise to indications of a criminal act having been perpetrated. In this context, the Directorate-General for Human Resources and Security may, where appropriate or required, provide support to the authorities of the host Member State or any other Member State concerned.

7. In the case of serious cyber-incidents the Directorate-General for Informatics shall collaborate closely with the Directorate-General for Human Resources and Security to provide support on all technical matters. The Directorate-General for Human Resources and Security shall decide, in consultation with the Directorate-General for Informatics, when it is appropriate to inform the competent authorities of the host country or any other Member State concerned. The incident coordination services of Computer Emergency Response Team for the European institutions, bodies and agencies ('CERT-EU') will be used as regards support to other EU institutions and agencies that may be affected.

8. Security inquiries shall be documented.

Article 14

Delineation of competences with regard to security inquiries and other types of investigations

1. Where the Security Directorate of the Directorate-General for Human Resources and Security conducts security inquiries, as referred to in Article 13, and if these enquiries fall within the competences of the European Anti-Fraud Office (OLAF) or the Investigation and Disciplinary Office of the Commission (IDOC), it shall liaise with those bodies at once with a view, in particular, not to compromise later steps by either OLAF or IDOC. Where appropriate, the Security Directorate of the Directorate-General for Human Resources and Security shall invite OLAF or IDOC to be involved in the investigation.

2. The security enquiries, as referred to in Article 13, shall be without prejudice to the powers of OLAF and IDOC as laid down in the rules governing those bodies. The Security Directorate of the Directorate-

General for Human Resources and Security may be requested to provide technical assistance for inquiries initiated by OLAF or IDOC.

3. The Security Directorate of the Directorate-General for Human Resources and Security may be asked to assist OLAF's agents when they access Commission premises in accordance with Articles 3(5) and 4(4) of Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council ([13]), in order to facilitate their tasks. The Security Directorate informs of such requests for assistance the Secretary-General and the Director-General of the Directorate-General for Human Resources and Security or, if such investigation is carried out on premises of the Commission occupied by its Members or by the Secretary-General, the President of the Commission and the Commissioner in charge of Human Resources.

4. Without prejudice to Article 22(a) of the Staff Regulations, where a case may fall within the competence of both the Security Directorate of the Directorate-General for Human Resources and Security and IDOC, the Security Directorate shall, when it reports to the Director-General of Human Resources in compliance with Article 13 at the earliest possible stage advise whether there are grounds that justify that IDOC is seized with the matter. This stage shall in particular be considered to have been reached when an immediate threat to security has come to an end. The Director-General of Human Resources and Security shall decide on the matter.

5. Where a case may fall within the competence of both the Security Directorate of the Directorate-General for Human Resources and Security and OLAF, the Security Directorate shall without delay report to the Director-General of Human Resources and Security and shall inform the Director-General of OLAF at the earliest possible stage. This stage shall in particular be considered to have been reached when an immediate threat to security has come to an end.

Article 15

Security inspections

1. The Directorate-General for Human Resources and Security shall undertake security inspections in order to verify compliance by Commission services and individuals with this Decision and its

implementing rules and to formulate recommendations when deemed necessary.

2. Where appropriate, the Directorate-General for Human Resources and Security shall undertake security inspections or security monitoring or assessment visits to verify whether the security of Commission staff, assets and information falling under the responsibility of other Union institutions, agencies or bodies, Member States, third states or international organisations, is appropriately protected in accordance with security rules, regulations and standards which are at least equivalent to those of the Commission. Where appropriate and in the spirit of good cooperation between administrations, those security inspections shall also include inspections conducted in the context of the exchange of classified information with other Union institutions, bodies and agencies, Member States or with third states or international organisations.

3. This Article shall be implemented, mutatis mutandis, for Commission staff in Union Delegations, without prejudice to any special arrangement between the Commission and the EEAS, such as the special arrangement signed on 28 May 2014 between the Directorate General for Human Resources and Security of the European Commission and the European External Action Service on the duty of care towards Commission staff posted in Union Delegations.

Article 16

Alert states and management of crisis situations

1. The Directorate-General for Human Resources and Security shall be responsible for putting in place appropriate alert state measures in anticipation of or in response to threats and incidents affecting security at the Commission, and for measures required for managing crisis situations.

2. The alert state measures referred to in paragraph 1 shall be commensurate with the level of threat to security. The alert states levels shall be defined in close cooperation with the competent services of other Union institutions, agencies and bodies, and of the Member State or Member States hosting Commission premises.

3. The Directorate-General for Human Resources and Security shall be the contact point for alert states and management of crisis situations.

CHAPTER 4

ORGANISATION

Article 17

General responsibilities of Commission services

1. The responsibilities of the Commission referred to in this Decision shall be exercised by the Directorate-General for Human Resources and Security under the authority and responsibility of the Member of the Commission responsible for security.

2. The specific arrangements as regards cyber-security are defined in Decision C(2006) 3602.

3. The responsibilities for implementing this Decision and its implementing rules and for day-to-day compliance may be delegated to other Commission departments, whenever decentralised delivery of security offers significant efficiency, resource or time savings, for instance because of the geographical location of the services concerned.

4. Where paragraph 3 applies, the Directorate-General for Human Resources and Security, and where appropriate the Director-General for Informatics, shall conclude arrangements with individual Commission departments establishing clear roles and responsibilities for the implementation and monitoring of security policies.

Article 18

The Directorate-General for Human Resources and Security

1. The Directorate-General for Human Resources and Security shall in particular be responsible for:

(1) developing the Commission's security policy, implementing rules and security notices;

(2) gathering information in view of assessing threats and risks to security and on all issues which may affect security in the Commission;

(3) providing counter electronic surveillance and protection to all the sites of the Commission, taking due account of threat assessments and evidence of unauthorised activities against the Commission's interests;
(4) providing a 24-hour/7-day emergency service for Commission services and staff for any safety- and security-related issues;
(5) implementing security measures aimed at mitigating risks to security and developing and maintaining appropriate CIS to cover its operational needs, particularly in the domains of physical access control, administration of security authorisations and handling of sensitive and EU classified information;
(6) raising awareness, organising exercises and drills and providing training and advice on all issues related to security at the Commission, in view of promoting a security culture and creating a pool of personnel appropriately trained in security matters.

2. The Directorate-General for Human Resources and Security shall, without prejudice to other Commission services' competences and responsibilities, ensure external liaison:
(1) with the security departments of the other Union institutions, agencies and bodies on issues relating to the security of the persons, assets and information in the Commission;
(2) with security, intelligence and threat assessment services, including national security authorities, of the Member States, of third countries and international organisations and bodies on issues affecting the security of persons, assets and information in the Commission;
(3) with police and other emergency services on all routine and emergency issues affecting the Commission's security;
(4) with the security authorities of other Union institutions, of agencies and bodies, of the Member States and of third countries in the field of response to cyberattacks with a potential impact on security in the Commission;
(5) regarding the receipt, assessment and distribution of intelligence concerning threats posed by terrorist and espionage activities affecting security in the Commission;
(6) regarding issues relating to classified information, as specified further in the Commission Decision (EU, Euratom) 2015/444 ([14]).

3. The Directorate-General for Human Resources and Security shall be responsible for the secure transmission of information performed under this Article, including the transmission of personal data.

Article 19

The Commission Security Expert Group (ComSEG)

A Commission Security Expert Group shall be established, with the mandate to advise the Commission, where appropriate, on matters relating to its internal security policy and more particularly on protection of EU classified information.

Article 20

Local Security Officers (LSOs)

1. Each Commission department or Cabinet shall appoint a Local Security Officer (LSO), who shall act as the principal point of contact between their service and the Directorate-General for Human Resources and Security on all matters related to security in the Commission. Where appropriate one or more deputy LSO may be appointed. The LSO shall be an official or a temporary agent.

2. As the main point of contact on security within his Commission department or Cabinet, the LSO shall, at regular intervals, report to the Directorate-General for Human Resources and Security and to his hierarchy on security issues involving his Commission department and, immediately, on any security incidents, including those where EUCI or sensitive non-classified information may have been compromised.

3. For matters related to security of communication and information systems, the LSO shall liaise with the Local Informatics Security Officer (LISO) of his Commission department, whose role and responsibilities are laid down in Decision C(2006) 3602.

4. He shall contribute to security training and awareness activities addressing the specific needs of staff, contractors and other individuals working under the authority of his Commission department.

5. The LSO may be assigned specific tasks in cases of major or immediate risks to security or of emergencies at the request of the Directorate-General for Human Resources and Security. The Director-General or the Director for Human Resources of the local Directorate-

General of the LSO shall be informed about those specific tasks by the Directorate-General for Human Resources and Security.

6. The responsibilities of the LSO shall be without prejudice to the role and responsibilities assigned to Local Informatics Security Officers (LISOs), Health and Safety Managers, Registry Control Officers (RCOs) or any other function implying security or safety-related responsibilities. The LSO shall liaise with them in order to ensure a coherent and consistent approach to security and an efficient flow of information on matters related to security at the Commission.

7. The LSO shall have direct access to his Director-General or Head of Service, while informing his direct hierarchy. He shall hold a security authorisation to access EUCI, at least up to the level of SECRET UE/EU SECRET.

8. In order to promote the exchange of information and best practices, the Directorate-General for Human Resources and Security shall organise at least twice a year a LSO conference. Attendance by LSOs at these conferences shall be mandatory.

CHAPTER 5

IMPLEMENTATION

Article 21

Implementing rules and security notices

1. As necessary, the adoption of the implementing rules for this Decision will be the subject of a separate empowerment decision of the Commission in favour of the Member of the Commission responsible for security matters, in full compliance with the internal rules of procedure.

2. After being empowered following the abovementioned Commission decision, the Member of the Commission responsible for security matters may develop security notices setting out security guidelines and best practices within the scope of this Decision and its implementing rules.

3. The Commission may delegate the tasks mentioned in the first and second paragraph of this Article to the Director-General for Human

Resources and Security by a separate delegation decision, in full compliance with the internal rules of procedure.

CHAPTER 6

MISCELLANEOUS AND FINAL PROVISIONS

Article 22

Processing of personal data

1. The Commission shall process personal data needed for implementing this Decision in accordance with Regulation (EC) No 45/2001.

2. Notwithstanding the measures already in place at the time of adoption of this Decision and notified to the European Data Protection Supervisor ([15]), any measure under this Decision involving the processing of personal data, such as relating to access and exit logs, CCTV recordings, recordings of telephone calls to duty offices or dispatch centres and similar data, which are required for reasons of security or crisis response, shall be subject to implementing rules in accordance with Article 21, which shall lay down appropriate safeguards for data subjects.

3. The Director-General of the Directorate-General for Human Resources and Security shall be responsible for the security of any processing of personal data undertaken in the context of this Decision.

4. Those implementing rules and procedures shall be adopted after consultation of the Data Protection Officer and the European Data Protection Supervisor in accordance with Regulation (EC) No 45/2001.

Article 23

Transparency

This Decision and its implementing rules shall be brought to the attention of Commission staff and to all individuals to whom they apply.

Article 24

Repeal of previous decisions

Decision C(94) 2129 is repealed.

Article 25

Entry into force

This Decision shall enter into force on the day following that of its publication in the *Official Journal of the European Union*.

Done at Brussels, 13 March 2015.

For the Commission
The President
Jean-Claude JUNCKER

---

(1) Cf. the 'Arrangement entre le Gouvernement belge et le Parlement européen, le Conseil, la Commission, le Comité économique et social européen, le Comité des régions, la Banque européenne d'investissement en matière de sécurité' of 31 December 2004, the 'Accord de sécurité signé entre la Commission et le Gouvernement luxembourgeois' of 20 January 2007, and the 'Accordo tra il Governo italiano e la Commissione europea dell'energia atomica (Euratom) per l'istituzione di un Centro comune di ricerche nucleari di competenza generale' of 22 July 1959.

(2) DPO-914.2, DPO-93.7, DPO-153.3, DPO-870.3, DPO-2831.2, DPO-1162.4, DPO-151.3, DPO-3302.1, DPO-508.6, DPO-2638.3, DPO-544.2, DPO-498.2, DPO-2692.2, DPO-2823.2.

(3) Commission Decision C(94) 2129 of 8 September 1994 on the tasks of the Security Office.

(4) Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).

(5) Regulation (EEC, Euratom, ECSC) No 259/68 of the Council of 29 February 1968 laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Communities and instituting special measures temporarily applicable to officials of the Commission (Conditions of Employment of Other Servants) (OJ L 56, 4.3.1968, p. 1).

(6) Decision of the High Representative of the Union for Foreign Affairs and Security Policy 2013/C 190/01 of 19 April 2013 on the security rules for the European External Action Service (OJ C 190, 29.6.2013, p. 1).

(7) Commission Decision 2002/47/EC, ECSC, Euratom of 23 January 2002 amending its Rules of Procedure (OJ L 21, 24.1.2002, p. 23) annexing the provisions on document management.

([8]) Commission Decision 2004/563/EC, Euratom of 7 July 2004 amending its Rules of Procedure (OJ L 251, 27.7.2004, p. 9) annexing the provisions on electronic and digitised documents.

([9]) C(2006) 1623 of 21 April 2006 establishing a harmonised policy for health and safety at work for all European Commission staff.

([10]) C(2006) 3602 of 16 August 2006 concerning the security of information systems used by the European Commission.

([11]) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

([12]) Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43).

([13]) Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No 1073/1999 of the European Parliament and of the Council and Council Regulation (Euratom) No 1074/1999 (OJ L 248, 18.9.2013, p. 1).

([14]) Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the Security rules for protecting EU classified information (see page 53 of this Official Journal).

([15]) DPO-914.2, DPO-93.7, DPO-153.3, DPO-870.3, DPO-2831.2, DPO-1162.4, DPO-151.3, DPO-3302.1, DPO-508.6, DPO-2638.3, DPO-544.2, DPO-498.2, DPO-2692.2, DPO-2823.2.

2.11. 2015 M. KOVO 13 D. KOMISIJOS SPRENDIMAS (ES, EURATOMAS) 2015/444 DĖL ES ĮSLAPTINTOS INFORMACIJOS APSAUGAI UŽTIKRINTI SKIRTŲ SAUGUMO TAISYKLIŲ

KOMISIJOS SPRENDIMAS (ES, Euratomas) 2015/444

2015 m. kovo 13 d.

dėl ES įslaptintos informacijos apsaugai užtikrinti skirtų saugumo taisyklių

EUROPOS KOMISIJA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo, ypač į jos 249 straipsnį,

atsižvelgdama į Europos atominės energijos bendrijos steigimo sutartį, ypač į jos 106 straipsnį,

atsižvelgdama į Protokolą Nr. 7 dėl Europos Sąjungos privilegijų ir imunitetų, pridėtą prie Sutarčių, ypač į jo 18 straipsnį,

kadangi:

(1) atsižvelgiant į institucinius, organizacinius, veiklos ir technologinius pokyčius, reikia peržiūrėti ir atnaujinti Komisijos taikomas saugumo nuostatas, kurių tikslas – apsaugoti Europos Sąjungos įslaptintą informaciją (ESĮI);

(2) Europos Komisija su Belgijos, Liuksemburgo ir Italijos Vyriausybėmis sudarė susitarimus ([1]) dėl pagrindinių jos darbo vietų saugumo;

(3) Komisija, Taryba ir Europos išorės veiksmų tarnyba yra įsipareigojusios taikyti lygiaverčius ESĮI apsaugą užtikrinančius saugumo standartus;

(4) svarbu, kad Europos Parlamentas ir kitos Europos Sąjungos institucijos, agentūros, įstaigos ar organai atitinkamais atvejais prisidėtų prie įslaptintos informacijos apsaugos principų, standartų ir taisyklių, būtinų siekiant apsaugoti Europos Sąjungos ir jos valstybių narių interesus, taikymo;

(5) ESĮI kylančios rizikos valdymas yra procesas. Šio proceso tikslas – nustatyti žinomą saugumo riziką, apibrėžti saugumo priemones tokiai rizikai sumažinti iki priimtino lygio pagal šiame sprendime išdėstytus pagrindinius principus ir būtiniausius standartus ir taikyti šias priemones laikantis nuodugnios apsaugos sąvokos. Periodiškai atliekamas tokių priemonių efektyvumo vertinimas;

(6) fizinis saugumas, skirtas įslaptintai informacijai apsaugoti Komisijoje – tai fizinių ir techninių apsaugos priemonių taikymas siekiant užkirsti kelią leidimo neturintiems asmenims susipažinti su ESĮI;

(7) ESĮ valdymas – administracinių ESĮI kontrolės visą jos gyvavimo ciklą priemonių taikymas siekiant papildyti šio sprendimo 2, 3 ir 5 skyriuose numatytas priemones ir tokiu būdu atgrasyti nuo sąmoningo ar atsitiktinio tokios informacijos neteisėto atskleidimo arba praradimo, nustatyti tokius atvejus ir pašalinti jų padarinius. Tokios priemonės visų pirma yra susijusios su ESĮI rengimu, saugojimu, registravimu, kopijavimu, vertimu, slaptumo mažinimu, išslaptinimu, gabenimu ir sunaikinimu ir papildo bendrąsias Komisijos dokumentų tvarkymo taisykles (Sprendimai 2002/47/EB, EAPB, Euratomas ([2]) ir 2004/563/EB, Euratomas ([3]));

(8) šio sprendimo nuostatos nedaro poveikio:

a) Reglamentui (Euratomas) Nr. 3 ([4]);

b) Europos Parlamento ir Tarybos reglamentui (EB) Nr. 1049/2001 ([5]);

c) Europos Parlamento ir Tarybos reglamentui (EB) Nr. 45/2001 ([6]);

d) Tarybos reglamentui (EEB, Euratomas) Nr. 354/83 ([7]),

PRIĖMĖ ŠĮ SPRENDIMĄ:

1 SKYRIUS

PAGRINDINIAI PRINCIPAI IR BŪTINIAUSI STANDARTAI

1 straipsnis

Apibrėžtys

Šiame sprendime vartojamų terminų apibrėžtys:

1) **Komisijos padalinys** – Komisijos generalinis direktoratas, tarnyba arba Komisijos nario kabinetas;

2) **kriptografinė medžiaga** – kriptografiniai algoritmai, techninės ir programinės kriptografinės įrangos moduliai, priemonės, apimančios vykdymo informaciją bei susijusius dokumentus ir raktų duomenis;

3) **išslaptinimas** – bet kokios saugumo žymos panaikinimas;

4) **nuodugni apsauga** – saugumo priemonių, kurios grupuojamos į kelis apsaugos lygius, taikymas;

5) **dokumentas** – bet kokios fizinės formos ir charakteristikų užregistruota informacija;

6) **slaptumo mažinimas** – aukštesnio slaptumo lygio keitimas žemesniu slaptumo lygiu;

7) **ESĮI tvarkymas** – visi galimi veiksmai, kurie gali būti atliekami su ESĮI per visą jos gyvavimo ciklą. Tai apima ESĮI rengimą, registravimą, apdorojimą, gabenimą, slaptumo mažinimą, išslaptinimą ir sunaikinimą. Ryšių ir informacinių sistemų (RIS) atžvilgiu tai taip pat apima ESĮI rinkimą, skelbimą, perdavimą ir saugojimą;

8) **turėtojas** – tinkamą leidimą turintis asmuo, kuriam „būtina žinoti“ ir kuris turi ESĮI dalį bei yra atitinkamai atsakingas už jos apsaugą;

9) **įgyvendinimo taisyklės** – taisyklės arba saugumo pranešimai, priimti pagal Komisijos sprendimo (ES, Euratomas) 2015/443 ([8]) 5 skyrių;

10) **medžiaga** – terpė, duomenų laikmena arba pagaminti ar gaminami įrenginiai ar įranga;

11) **rengėjas** – Europos Sąjungos institucija, agentūra ar įstaiga, vals-

tybė narė, trečioji valstybė ar tarptautinė organizacija, kurios atsakomybe įslaptinta informacija buvo parengta ir (arba) pateikta naudoti Europos Sąjungos struktūrose;

12) **patalpos** – bet koks nekilnojamasis ar panašus Komisijos turtas ir nuosavybė;

13) **saugumo rizikos valdymo procesas** – visas nebūtinai galinčių įvykti įvykių, kurie gali paveikti organizacijos arba jos naudojamų sistemų saugumą, nustatymo, kontrolės ir padarinių mažinimo procesas. Jis apima visą su rizika susijusią veiklą, įskaitant jos įvertinimą, valdymą, pripažinimą ir informavimą apie ją;

14) **tarnybos nuostatai** – Europos Sąjungos pareigūnų tarnybos nuostatai ir kitų Europos Sąjungos tarnautojų įdarbinimo sąlygos, nustatyti Tarybos reglamentu (EEB, Euratomas, EAPB) Nr. 259/68 ([9]);

15) **grėsmė** – galima nepageidaujamo incidento, dėl kurio gali būti padaryta žala organizacijai ar jos naudojamoms sistemoms, priežastis. Tokios grėsmės gali būti atsitiktinės arba tyčinės (piktybinės); jas apibūdina pavojingi elementai, galimi taikiniai ir puolimo būdai;

16) **pažeidžiamumas** – bet kokio pobūdžio trūkumas, kuriuo gali būti naudojamasi vienos ar daugiau grėsmių atveju. Pažeidžiamumas gali atsirasti dėl neveikimo arba gali būti susijęs su negriežta, neišsamia arba nenuoseklia kontrole ir gali būti techninio, procedūrinio, fizinio, organizacinio ar veiklos pobūdžio.

2 straipsnis

Dalykas ir taikymo sritis

1. Šis sprendimas nustato pagrindinius ESĮI apsaugai užtikrinti skirtus saugumo principus ir būtiniausius standartus.

2. Šis sprendimas taikomas visiems Komisijos padaliniams ir visose Komisijos patalpose.

3. Nepaisant konkrečių nuorodų dėl tam tikrų darbuotojų grupių, šis sprendimas taikomas Komisijos nariams, Komisijos darbuotojams pagal Tarnybos nuostatus ir kitų Europos Bendrijų tarnautojų įdarbinimo sąlygas, į Komisiją deleguotiems nacionaliniams ekspertams (SNE), paslaugų teikėjams ir jų darbuotojams, stažuotojams ir bet kuriam asmeniui, galinčiam patekti į Komisijos pastatus ar naudotis kitu turtu, arba infor-

macijai, kurią tvarko Komisija.

4. Šio sprendimo nuostatos nedaro poveikio Sprendimui 2002/47/EB, EAPB, Euratomas, ir Sprendimui 2004/563/EB, Euratomas.

3 straipsnis

ESĮI, slaptumo žymų ir kitų žymų apibrėžtis

Europos Sąjungos įslaptinta informacija (ESĮI) – bet kuri informacija arba medžiaga, kuriai suteikta ES slaptumo žyma ir kurią neteisėtai atskleidus galėtų būti padaryta tam tikro dydžio žala Europos Sąjungos arba vienos ar kelių valstybių narių interesams.

2. ESĮI žymima viena iš šių slaptumo žymų:

a) **TRES SECRET UE/ES TOP SECRET** – informacija ir medžiaga, kurią neteisėtai atskleidus galėtų būti padaryta ypač didelė žala Europos Sąjungos arba vienos ar kelių valstybių narių esminiams interesams;

b) **SECRET UE/ES SECRET** – informacija ir medžiaga, kurią neteisėtai atskleidus galėtų būti rimtai pakenkta Europos Sąjungos arba vienos ar kelių valstybių narių esminiams interesams;

c) **CONFIDENTIEL UE/ES CONFIDENTIAL** – informacija ir medžiaga, kurią neteisėtai atskleidus galėtų būti pakenkta Europos Sąjungos arba vienos ar kelių valstybių narių esminiams interesams;

d) **RESTREINT UE/ES RESTRICTED** – informacija ir medžiaga, kurios neteisėtas atskleidimas galėtų būti nepalankus Europos Sąjungos arba vienos ar kelių valstybių narių interesams.

3. ESĮI žymima slaptumo žyma pagal 2 dalį. Ji gali būti žymima papildoma žyma, kuri yra ne slaptumo žyma, bet skirta veiklos sričiai, su kuria ji yra susijusi, nurodyti, įslaptintos informacijos rengėjui įvardyti, jos platinimui ir naudojimui apriboti ar suteikimui nurodyti.

4 straipsnis

Įslaptinimo valdymas

1. Kiekvienas Komisijos narys arba kiekviena Komisijos tarnyba užtikrina, kad jos parengta ESĮI būtų žymima tinkama slaptumo žyma, būtų aiškiai nurodoma, kad tai yra ESĮI, ir jai būtų suteikta slaptumo žyma tik

tokiam laikotarpiui, kuris yra būtinas.

2. Nedarant poveikio 26 straipsniui, be išankstinio įslaptintos informacijos rengėjo raštiško sutikimo ESĮI slaptumas nemažinamas arba ji neišslaptinama, o 3 straipsnio 2 dalyje nurodytos žymos nekeičiamos arba nepanaikinamos.

3. Jei reikia, remiantis 60 straipsniu nustatomos ESĮI tvarkymo įgyvendinimo taisyklės, įskaitant praktinį slaptumo žymų vadovą.

5 straipsnis

Įslaptintos informacijos apsauga

1. ESĮI saugoma laikantis šio sprendimo ir jo įgyvendinimo taisyklių.

2. Bet kokios ESĮI turėtojas yra atsakingas už jos apsaugą pagal šį sprendimą ir jo įgyvendinimo taisykles, laikantis 4 skyriuje nustatytų taisyklių.

3. Valstybėms narėms nacionaline slaptumo žyma pažymėtą įslaptintą informaciją perdavus į Komisijos struktūras ar tinklus, Komisija tą informaciją saugo laikydamasi reikalavimų, taikomų lygiaverčio slaptumo žymos lygio ESĮI, kaip nustatyta I priede pateiktoje slaptumo žymų atitikmenų lentelėje.

4. ESĮI visumos atveju gali būti reikalaujama užtikrinti apsaugos lygį, atitinkantį aukštesnį slaptumo žymos lygį nei jos atskirų komponentų slaptumo žymos.

6 straipsnis

Saugumo rizikos valdymas

1. ESĮI apsaugai užtikrinti skirtos saugumo priemonės visą savo gyvavimo ciklą turi atitikti jos slaptumo žymos lygį, informacijos ar medžiagos formą ir kiekį, patalpų, kuriose laikoma ESĮI, vietos ir konstrukcijos reikalavimus ir turi būti parenkamos atsižvelgiant į vietos lygiu įvertintą piktavališkos ir (arba) nusikalstamos veiklos, įskaitant šnipinėjimą, sabotažą ar terorizmą, keliamą grėsmę.

2. Nenumatytų atvejų planuose turi būti atsižvelgiama į poreikį apsaugoti ESĮI ekstremaliosios padėties atvejais siekiant užkirsti kelią galimybei neteisėtai susipažinti su šia informacija, ją atskleisti ar prarasti jos

vientisumą arba galimybę ja naudotis.

3. Visų tarnybų veiklos tęstinumo planuose numatomos prevencinės ir atstatymo priemonės siekiant sumažinti didelių klaidų ar incidentų poveikį ESĮI administravimui ir saugojimui.

7 straipsnis

Šio sprendimo įgyvendinimas

1. Jei reikia, remiantis 60 straipsniu nustatomos įgyvendinimo taisyklės, skirtos šiam sprendimui papildyti ar sustiprinti.

2. Komisijos tarnybos imasi visų būtinų jų atsakomybės sričiai priklausančių priemonių, siekdamos užtikrinti, kad tvarkant arba saugant ESĮI ar kitą įslaptintą informaciją būtų laikomasi šio sprendimo ir atitinkamų įgyvendinimo taisyklių.

3. Saugumo priemonės, kurių imamasi įgyvendinant šį sprendimą, turi atitikti Komisijos saugumo principus, nustatytus Sprendimo (ES, Euratomas) 2015/443 3 straipsnyje.

4. Žmogiškųjų išteklių ir saugumo generalinio direktorato generalinis direktorius Žmogiškųjų išteklių ir saugumo generaliniame direktorate įsteigia Komisijos saugumo instituciją. Komisijos saugumo institucija atlieka pareigas, jai paskirtas šiuo sprendimu ir jo įgyvendinimo taisyklėmis.

5. Kiekvieno Komisijos padalinio vietos saugumo pareigūnas (VSP), nurodytas Sprendimo (ES, Euratomas) 2015/443 20 straipsnyje, yra bendrai atsakingas už ESĮI apsaugą pagal šį sprendimą ir, glaudžiai bendradarbiaudamas su Žmogiškųjų išteklių ir saugumo generaliniu direktoratu, atlieka šias užduotis:

a) administruoja prašymus darbuotojams išduoti saugumo leidimus;
b) prisideda prie saugumo mokymų ir teikia informaciją;
c) prižiūri padalinio registracijos kontrolės pareigūno (RKP) veiklą;
d) praneša apie saugumo pažeidimus ir neteisėto ESĮI atskleidimo atvejus;
e) saugo atsarginius raktus ir visų kodų sąrašą;
f) atlieka kitas su ESĮI apsauga susijusias arba įgyvendinimo taisyklėse nustatytas užduotis.

8 straipsnis

ESĮI saugumo pažeidimai ir neteisėtas atskleidimas

1. Saugumo pažeidimu laikomas šiame sprendime ir jo įgyvendinimo taisyklėse nustatytoms saugumo taisyklėms priešingas asmens veikimas arba neveikimas.

2. Laikoma, kad ESĮI neteisėtai atskleista, jeigu pažeidus saugumo taisykles ji visa arba jos dalis yra atskleista susipažinti su ja leidimo neturintiems asmenims.

3. Apie visus saugumo pažeidimus arba įtariamus saugumo pažeidimus nedelsiant pranešama Komisijos saugumo institucijai.

4. Tais atvejais, kai žinoma arba yra pagrįstų priežasčių manyti, kad ESĮI buvo neteisėtai atskleista arba prarasta, remiantis Sprendimo (ES, Euratomas) 2015/443 13 straipsniu atliekamas saugumo tyrimas.

5. Imamasi visų tinkamų priemonių, siekiant:

a) informuoti įslaptintos informacijos rengėją;
b) užtikrinti, kad siekiant nustatyti faktus tokį atvejį nagrinėtų su pažeidimu tiesiogiai nesusijęs personalas;
c) įvertinti galimą Europos Sąjungos ar valstybių narių interesams padarytą žalą;
d) imtis atitinkamų priemonių, kad būtų užkirstas kelias pažeidimui pasikartoti;
e) atitinkamas institucijas informuoti apie atliktus veiksmus.

6. Bet kuriam asmeniui, kuris pažeidė šiame sprendime nustatytas saugumo taisykles, gali būti taikomos drausminės priemonės vadovaujantis Tarnybos nuostatais. Asmeniui, kuris atsakingas už ESĮI neteisėtą atskleidimą ar praradimą, taikomos drausminės ir (arba) teisinės priemonės pagal taikomus įstatymus, taisykles ir kitus teisės aktus.

2 SKYRIUS

PERSONALO SAUGUMAS

9 straipsnis

Apibrėžtys

Šiame skyriuje vartojamų terminų apibrėžtys:

1) **Leidimas susipažinti su ESĮI** – remiantis valstybės narės kompetentingos institucijos patvirtinimu Komisijos priimtas saugumo institucijos sprendimas, kad Komisijos pareigūnui, kitam tarnautojui arba deleguotajam nacionaliniam ekspertui iki nustatytos datos gali būti leidžiama susipažinti su ESĮI, pažymėta nurodyto lygio slaptumo žyma (iki CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio lygio slaptumo žyma), jei nustatyta, kad asmeniui „būtina žinoti“ ir jis buvo tinkamai informuotas apie savo atsakomybę; laikoma, kad asmuo, kuriam taikoma ši apibrėžtis, yra asmuo, turintis leidimą susipažinti su įslaptinta informacija.

2) **Darbuotojo saugumo leidimas** – priemonių taikymas, siekiant užtikrinti, kad galimybė susipažinti su ESĮI būtų suteikta tik asmenims:

a) kuriems „būtina žinoti“;
b) kurie atitinkamais atvejais turi leidimus susipažinti su tam tikro lygio slaptumo žyma pažymėta įslaptinta informacija;
c) kurie yra informuoti apie savo pareigas.

3) **Asmens patikimumo pažymėjimas (APT)** – valstybės narės kompetentingos institucijos patvirtinimas, kuris pateikiamas valstybės narės kompetentingoms institucijoms baigus patikimumo patikrinimą ir kuriuo pažymima, kad atitinkamam asmeniui, nustačius, kad jam „būtina žinoti“ ir jis buvo tinkamai informuotas apie savo atsakomybę, gali būti suteikiamas leidimas iki nurodytos datos susipažinti su nurodyto lygio slaptumo žyma (iki CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio lygio slaptumo žyma) pažymėta ESĮI.

4) **Asmens patikimumo pažymėjimą patvirtinanti pažyma (APPPP)** – kompetentingos institucijos išduota pažyma, kurioje nurodoma, kad asmuo turi galiojantį patikimumo pažymėjimą arba Komisijos saugumo institucijos išduotą saugumo leidimą, ir nurodomas ESĮI, su kuria tam asmeniui gali būti leista susipažinti, slaptumo žymos lygis (CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnis), atitinka-

mo asmens patikimumo pažymėjimo arba leidimo galiojimo laikas ir pačios pažymos galiojimo laikas.

5) **Patikimumo patikrinimas** – tyrimo procedūros, kurias, vadovaudamasi valstybėje narėje galiojančiais įstatymais ir kitais teisės aktais, atlieka kompetentinga institucija, siekdama gauti užtikrinimą, kad nėra jokios nepalankios informacijos, kuri neleistų asmeniui išduoti jo patikimumo pažymėjimo, suteikiančio galimybę susipažinti su nurodyto lygio (iki CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio) ESĮI.

10 straipsnis

Pagrindiniai principai

1. Leidimas susipažinti su ESĮI asmeniui suteikiamas tik po to, kai:
1) nustatoma, kad jam „būtina žinoti“;
2) jis buvo informuotas apie ESĮI apsaugai užtikrinti skirtas saugumo taisykles bei atitinkamus saugumo standartus ir gaires ir patvirtino savo pareigą saugoti tokią informaciją;
3) jam dėl jo atliekamų funkcijų išduotas atitinkamo lygio saugumo leidimas susipažinti su įslaptinta informacija, pažymėta CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio lygio slaptumo žyma, arba jam išduoti kiti tinkami leidimai pagal nacionalinius įstatymus ir kitus teisės aktus.

2. Visi asmenys, kuriems dėl jų pareigų gali reikėti susipažinti su CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio lygio slaptumo žyma pažymėta ESĮI, prieš susipažindami su tokia ESĮI gauna atitinkamo lygio saugumo leidimus. Atitinkamas asmuo raštu sutinka dalyvauti jo patikimumo pažymėjimo išdavimo procedūroje. To nepadaręs asmuo negali būti paskirtas į pareigas, jam negali būti patikėtos funkcijos arba užduotys, kurias vykdant reikėtų susipažinti su CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio lygio slaptumo žyma pažymėta įslaptinta informacija.

3. Asmens patikimumo pažymėjimo išdavimo procedūrų tikslas – nustatyti, ar asmeniui, atsižvelgiant į jo lojalumą ir patikimumą, gali būti leidžiama susipažinti su ESĮI.

4. Asmens lojalumas ir patikimumas, prieš suteikiant jam asmens patikimumo pažymėjimą, leisiantį susipažinti su CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymė-

ta informacija, nustatomas vykdant patikimumo patikrinimą, kurį atlieka valstybės narės kompetentingos tarnybos, laikydamosi nacionalinių įstatymų ir kitų teisės aktų.

5. Komisijos saugumo institucija yra atsakinga tik už ryšių palaikymą su nacionalinėmis saugumo institucijomis (toliau – NSI) arba kitomis kompetentingomis nacionalinėmis institucijomis visais patikimumo tikrinimo klausimais. Visus Komisijos tarnybų ir jų darbuotojų ryšius su NSI ir kitomis kompetentingomis institucijomis palaiko Komisijos saugumo institucija.

11 straipsnis

Saugumo leidimų išdavimo tvarka

1. Kiekvienas Komisijos generalinis direktorius arba tarnybos vadovas nustato, kurias pareigybes užimantys jo padalinio darbuotojai atlikdami savo pareigas privalo susipažinti su įslaptinta informacija, pažymėta CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio lygio slaptumo žyma, ir kuriems reikia išduoti saugumo leidimą.

2. Kai žinoma, kad asmuo bus paskirtas į pareigas, kurias atliekant reikės turėti galimybę susipažinti su CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio lygio slaptumo žyma pažymėta įslaptinta informacija, atitinkamo Komisijos padalinio VSP praneša apie tai Komisijos saugumo institucijai, o ji tam asmeniui perduoda patikimumo pažymėjimo klausimyną, parengtą tos valstybės narės, kurios pilietis yra paskirtasis Europos Sąjungos institucijų darbuotojas, nacionalinės saugumo institucijos. Asmuo raštu sutinka dalyvauti patikimumo pažymėjimo išdavimo procedūroje ir kuo greičiau grąžinti užpildytą klausimyną Komisijos saugumo institucijai.

3. Komisijos saugumo institucija nusiunčia užpildytą asmens patikimumo pažymėjimo klausimyną valstybės narės, kurios pilietis yra paskirtasis Europos Sąjungos institucijų darbuotojas, NSI, prašydama atlikti patikimumo patikrinimą, skirtą gauti leidimui naudotis tam tikro slaptumo žymos lygio ESĮI, su kuria asmeniui reikės susipažinti.

4. Jei Komisijos saugumo institucija sužino patikimumui patikrinti svarbios informacijos apie asmenį, kuris pateikė prašymą išduoti patikimumo pažymėjimą, laikydamasi atitinkamų taisyklių ir teisės aktų, ji apie tai praneša atitinkamai NSI.

5. Užbaigusi patikimumo patikrinimą ir kaip įmanoma greičiau po to, kai gauna atitinkamos NSI patikimumo patikrinimo bendro vertinimo išvadas, Komisijos saugumo institucija:

a) atitinkamam asmeniui gali suteikti leidimą susipažinti su ESĮI ir leisti susipažinti su iki atitinkamo lygio slaptumo žyma pažymėta ESĮI iki nustatytos datos, bet ne ilgiau kaip 5 metus, jei patikimumo patikrinimo rezultatai užtikrintai rodo, kad neturima jokios nepalankios informacijos, kuri leistų abejoti asmens lojalumu ir patikimumu;

b) jei patikimumo patikrinimo rezultatai nėra tokie užtikrinantys, laikydamasi atitinkamų taisyklių ir teisės aktų apie tai praneša atitinkamam asmeniui, kuris gali prašyti, kad Komisijos saugumo institucija jį išklausytų; Komisijos saugumo institucija gali prašyti kompetentingos NSI pateikti daugiau paaiškinimų, kuriuos ji gali pateikti pagal savo nacionalinius įstatymus ir kitus teisės aktus. Jei patikimumo patikrinimo rezultatai pasitvirtina, leidimas susipažinti su ESĮI neišduodamas.

6. Patikimumo patikrinimui bei gautiems rezultatams taikomi atitinkamoje valstybėje narėje galiojantys įstatymai ir kiti teisės aktai, įskaitant su apskundimu susijusius įstatymus ir kitus teisės aktus. Komisijos saugumo institucijos sprendimai gali būti apskųsti pagal Tarnybos nuostatus.

7. Komisija pripažįsta kitos Europos Sąjungos institucijos, įstaigos ar agentūros išduotą leidimą susipažinti su ESĮI, su sąlyga, kad jis tebegalioja. Leidimas galioja visoms užduotims, kurias tas asmuo vykdo Komisijoje, o Europos Sąjungos institucija, įstaiga ar agentūra, kurioje asmuo pradeda dirbti, praneša atitinkamai NSI apie darbdavio pasikeitimą.

8. Jeigu asmens tarnyba neprasideda per 12 mėnesių nuo patikimumo patikrinimo rezultatų pranešimo Komisijos saugumo institucijai arba jeigu asmens tarnyboje daroma 12 mėnesių pertrauka ir tuo laikotarpiu jis nedirba Komisijoje arba kitoje Europos Sąjungos institucijoje, įstaigoje ar agentūroje arba valstybės narės nacionalinėje administracinėje įstaigoje, Komisijos saugumo institucija apie tai praneša atitinkamai NSI ir prašo patvirtinti, kad patikimumo pažymėjimas tebegalioja ir yra tinkamas.

9. Jei Komisijos saugumo institucija sužino, kad galiojantį saugumo leidimą turintis asmuo kelia saugumo riziką, Saugumo institucija, laikydamasi atitinkamų taisyklių ir teisės aktų, apie tai praneša atitinkamai

NSI.

10. Kai NSI informuoja Komisijos saugumo instituciją apie tai, kad pagal 5 dalies a punktą suteiktas užtikrinimas dėl asmens, turinčio leidimą susipažinti su ESĮI, panaikinamas, Komisijos saugumo institucija gali paprašyti pateikti paaiškinimą, kurį NSI gali pateikti pagal nacionalinius įstatymus ir kitus teisės aktus. Jei atitinkama NSI patvirtina nepalankią informaciją, saugumo leidimas panaikinamas, o asmeniui neleidžiama susipažinti su ESĮI ir užimti pareigų, kurias eidamas jis galėtų susipažinti su ta informacija arba sukelti pavojų saugumui.

11. Apie sprendimą panaikinti arba sustabdyti asmens, kuriam taikomas šis sprendimas, leidimą susipažinti su ESĮI ir atitinkamais atvejais tokio panaikinimo arba sustabdymo priežastis pranešama atitinkamam asmeniui, kuris gali prašyti, kad Komisijos saugumo institucija jį išklausytų. NSI teikiama informacija reglamentuojama atitinkamoje valstybėje narėje galiojančiais įstatymais ir kitais teisės aktais. Komisijos saugumo institucijos šiuo klausimu priimti sprendimai gali būti apskųsti pagal Tarnybos nuostatus.

12. Komisijos padaliniai užtikrina, kad į juos deleguoti nacionaliniai ekspertai, siekiantys eiti pareigas, kurioms reikia turėti saugumo leidimą susipažinti su ESĮI, prieš pradėdami tarnybą Komisijos saugumo institucijai pateiktų pagal nacionalinius įstatymus ir kitus teisės aktus galiojantį asmens patikimumo pažymėjimą (APP) arba asmens patikimumo pažymėjimą patvirtinančią pažymą (APPPP), kuria remdamasi Komisijos saugumo institucija išduoda saugumo leidimą susipažinti su tokio slaptumo laipsnio ESĮI, koks nurodytas nacionaliniame patikimumo pažymėjime; toks leidimas galioja ne ilgiau nei jų paskyrimo laikotarpis.

13. Komisijos nariai, kurie dėl savo atliekamų pareigų pagal Sutartį gali susipažinti su ESĮI, informuojami apie jų saugumo įsipareigojimus ESĮI apsaugos srityje.

14. Remiantis šiuo sprendimu, patikimumo pažymėjimų ir leidimų susipažinti su ESĮI registrai saugomi Komisijos saugumo institucijoje. Šiuose registruose nurodomas bent jau ESĮI, su kuria tam asmeniui gali būti leista susipažinti, slaptumo žymos lygis, patikimumo pažymėjimo išdavimo data ir jo galiojimo laikas.

15. Komisijos saugumo institucija gali išduoti APPPP, kurioje nurodomas ESĮI, su kuria tam asmeniui gali būti leista susipažinti, slaptumo žymos lygis (CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštes-

nio lygio slaptumo žyma), atitinkamo leidimo susipažinti su ESĮI galiojimo laikas ir pačios pažymos galiojimo laikas.

16. Po to, kai patikimumo pažymėjimas suteiktas pirmą kartą ir jeigu asmuo nuolat dirbo Europos Komisijoje arba kitoje Europos Sąjungos institucijoje, įstaigoje ar agentūroje bei jam reikia nuolat dirbti su ESĮI, saugumo leidimas susipažinti su ESĮI peržiūrimas siekiant jį atnaujinti paprastai kas penkerius metus skaičiuojant nuo paskutinio patikimumo patikrinimo, kuriuo remiantis buvo išduotas pažymėjimas, rezultatų pranešimo datos.

17. Komisijos saugumo institucija gali pratęsti turimo saugumo leidimo galiojimo laikotarpį ne ilgiau kaip 12 mėnesių, jeigu per du mėnesius nuo prašymo atnaujinti leidimą ir su juo susijusio asmens patikimumo pažymėjimo klausimyno pateikimo dienos iš atitinkamos NSI ar kitos kompetentingos nacionalinės institucijos negauta nepalankios informacijos. Jeigu pasibaigus šiam 12 mėnesių laikotarpiui atitinkama NSI ar kita kompetentinga nacionalinė institucija Komisijos saugumo institucijai nepraneša apie savo nuomonę, asmeniui skiriamos tokios užduotys, kurioms atlikti saugumo leidimas nereikalingas.

12 straipsnis

Saugumo leidimo informaciniai susitikimai

1. Visi asmenys, kuriems išduoti leidimai susipažinti su įslaptinta informacija, dalyvauja Komisijos saugumo institucijos rengiamame saugumo leidimo informaciniame susitikime, po kurio raštu patvirtina suprantantys savo įsipareigojimus saugoti ESĮI ir ESĮI neteisėto atskleidimo pasekmes. Komisijos saugumo institucija užregistruoja tokius rašytinius patvirtinimus.

2. Visi asmenys, kuriems leidžiama susipažinti su ESĮI arba kurie turi dirbti su ESĮI, yra iš pat pradžių informuojami ir paskui reguliariai informuojami apie grėsmes saugumui; jie turi nedelsdami pranešti Komisijos saugumo institucijai apie bet kokius bandymus užmegzti kontaktą ar veiklą, kurie, jų nuomone, yra įtartini ar neįprasti.

3. Visi asmenys, nebeeinantys pareigų, kurias einant jiems reikia susipažinti su ESĮI, yra informuojami apie jų įsipareigojimus toliau saugoti ESĮI slaptumą ir atitinkamais atvejais jie tai patvirtina raštu.

13 straipsnis

Laikini saugumo leidimai

1. 1. Esant išskirtinėms aplinkybėms, kurios tinkamai pagrįstos tarnybos interesais, ir laukiant išsamaus patikimumo patikrinimo pabaigos, Komisijos saugumo institucija, pasikonsultavusi su valstybės narės, kurios pilietis yra atitinkamas asmuo, NSI ir atsižvelgusi į preliminaraus patikrinimo, ar nėra žinomos ir susijusios nepalankios informacijos apie asmenį, rezultatus, gali jam išduoti laikiną leidimą susipažinti su ESĮI konkrečiai funkcijai atlikti, nepažeisdama asmens patikimumo pažymėjimų pratęsimo nuostatų. Tokie laikini leidimai susipažinti su ESĮI galioja vieną ne ilgesnį kaip šešių mėnesių laikotarpį ir nesuteikia teisės susipažinti su slaptumo žyma TRES SECRET UE/EU TOP SECRET pažymėta informacija

2. Pagal 12 straipsnio 1 dalies nuostatas susipažinę su informacija, visi asmenys, kuriems išduotas laikinas leidimas, raštu patvirtina, kad jie supranta įsipareigojimus saugoti ESSĮ ir ESĮI neteisėto atskleidimo pasekmes. Komisijos saugumo institucija užregistruoja tokius rašytinius patvirtinimus.

14 straipsnis

Dalyvavimas Komisijos rengiamuose susitikimuose, kuriuose naudojama įslaptinta informacija

1. Komisijos padaliniai, atsakingi už susitikimų, kuriuose naudojama CONFIDENTIEL UE/ES CONFIDENTIAL ar aukštesnio lygio slaptumo žyma pažymėta įslaptinta informacija, rengimą, per savo VSP arba per susitikimo rengėją iš anksto praneša Komisijos saugumo institucijai apie tokių susitikimų datas, laiką, vietą ir dalyvius.

2. Laikantis 11 straipsnio 13 dalies nuostatų, asmenys, paskirti dalyvauti Komisijos rengiamuose susitikimuose, kuriuose naudojama CONFIDENTIEL UE/ES CONFIDENTIAL ar aukštesnio lygio slaptumo žyma pažymėta informacija, dalyvauti gali tik tuomet, jei patvirtinama, kad jų patikimumas patikrintas arba jie turi saugumo leidimą. Tokiuose susitikimuose, kuriuose naudojama įslaptinta informacija, neleidžiama dalyvauti asmenims, kurie Komisijos saugumo institucijai nepateikia APPPP arba kito patikimumo pažymėjimo įrodymo, taip pat

saugumo leidimų neturintiems Komisijos darbuotojams.

3. Prieš rengdamas susitikimą, kuriame naudojama įslaptinta informacija, susitikimo rengėjas arba susitikimą rengiančio Komisijos padalinio VSP paprašo, kad išorės dalyviai Komisijos saugumo institucijai pateiktų APPPP ar kitą patikimumo pažymėjimo įrodymą. Komisijos saugumo institucija informuoja VSP arba susitikimo rengėją apie gautus APPPP ar kitus patikimumo pažymėjimų įrodymus. Jei taikoma, gali būti naudojamas suvestinis pavardžių sąrašas, kuriame pateikiami atitinkami įrodymai apie patikimumo pažymėjimą.

4. Jei kompetentingos institucijos praneša Komisijos saugumo institucijai, kad asmuo, kuris eidamas savo pareigas turi dalyvauti Komisijos rengiamuose susitikimuose, nebeturi asmens patikimumo pažymėjimo, Komisijos saugumo institucija apie tai praneša Komisijos padalinio, atsakingo už rengiamą susitikimą, VSP.

15 straipsnis

Galima prieiga prie ESĮI

Kurjeriams, apsaugos darbuotojams ir lydintiems asmenims išduodamas atitinkamo lygio saugumo leidimas arba jie yra kitaip deramai patikrinami vadovaujantis nacionaliniais įstatymais ir kitais teisės aktais, informuojami apie ESĮI apsaugai užtikrinti skirtas saugumo procedūras ir jiems išdėstomos jų pareigos, susijusios su jiems patikėtos tokios informacijos apsauga.

3 SKYRIUS

FIZINIS SAUGUMAS, SKIRTAS ĮSLAPTINTAI INFORMACIJAI APSAUGOTI

16 straipsnis

Pagrindiniai principai

1. Fizinio saugumo priemonės skirtos sutrukdyti įsibrauti slaptai arba įsiveržti jėga, atgrasyti nuo neteisėtų veiksmų, sutrukdyti jiems bei juos nustatyti ir sudaryti sąlygas suskirstyti personalą pagal tai, kas gali susipažinti su ESĮI, vadovaujantis principu „būtina žinoti“. Tokios priemonės nustatomos remiantis rizikos valdymo procesu ir laikantis šio sprendimo bei jo įgyvendinimo taisyklių.

2. Visų pirma fizinio saugumo priemonėmis siekiama užkirsti kelią leidimo neturintiems asmenims susipažinti su ESĮI:

a) užtikrinant, kad ESĮI būtų tinkamai tvarkoma ir saugoma;
b) sudarant sąlygas suskirstyti personalą pagal tai, kas gali susipažinti su ESĮI, remiantis principu „būtina žinoti“ ir atitinkamais atvejais – darbuotojų saugumo leidimais;
c) atgrasant nuo neteisėtų veiksmų, sutrukdant jiems bei juos nustatant;
d) sutrukdant asmenims įsibrauti slaptai ar įsiveržti jėga arba juos užlaikant.

3. Fizinio saugumo priemonės taikomos visose patalpose, pastatuose, kabinetuose, salėse ir kitose zonose, kuriose tvarkoma arba saugoma ESĮI, įskaitant zonas, kuriose įrengtos 5 skyriuje nurodytos ryšių ir informacinės sistemos.

4. Zonos, kuriose saugoma CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio lygio slaptumo žyma pažymėta ESĮI, įrengiamos kaip saugumo zonos laikantis šio skyriaus nuostatų ir patvirtinamos Komisijos saugumo akreditavimo institucijos.

5. CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio lygio slaptumo žyma pažymėtos ESĮI apsaugai naudojama tik Komisijos saugumo institucijos patvirtinta įranga ar prietaisai.

17 straipsnis

Fizinio saugumo reikalavimai ir priemonės

1. Fizinio saugumo priemonės nustatomos remiantis grėsmių įvertinimu, kurį atlieka Komisijos saugumo institucija, prireikus konsultuodamasi su kitais Komisijos padaliniais, kitomis ES institucijomis, agentūromis arba įstaigomis ir (arba) kompetentingomis valstybių narių institucijomis. ESĮI apsaugai užtikrinti savo patalpose Komisija taiko rizikos valdymo procesą, kad užtikrintų, jog, atsižvelgiant į įvertintą riziką, būtų taikoma atitinkamo lygio fizinė apsauga. Rizikos valdymo procese atsižvelgiama į visus svarbius veiksnius, visų pirma:

a) ESĮI slaptumo žymos lygį;
b) ESĮI formą ir kiekį, atsižvelgiant į tai, kad dideliam ESĮI kiekiui ar rinkiniui apsaugoti gali reikėti taikyti griežtesnes apsaugos priemones;
c) pastatus ar zonas, kuriose laikoma ESĮI, supančią aplinką ir jų struktūrą;
d) įvertintą žvalgybos tarnybų, kurių veikla nukreipta prieš Europos Sąjungą, jos institucijas, įstaigas ar agentūras arba prieš valstybes nares, keliamą grėsmę ir grėsmę dėl sabotažo, terorizmo, ardomosios arba kitų rūšių nusikalstamos veikos.

2. Komisijos saugumo institucija, taikydama nuodugnios apsaugos sąvoką, nustato tinkamas įgyvendintinas fizinio saugumo priemones. Tuo tikslu Komisijos saugumo institucija parengia būtiniausius standartus, normas ir kriterijus, nustatytus įgyvendinimo taisyklėse.

3. Komisijos saugumo institucijai leidžiama apieškoti įeinančius ir išeinančius asmenis siekiant atgrasyti, kad į patalpas arba pastatus be leidimo nebūtų įnešama medžiaga arba iš jų be leidimo nebūtų išnešama ESĮI.

4. Iškilus pavojui, kad ESĮI bus pamatyta, netgi atsitiktinai, atitinkami Komisijos padaliniai imasi tinkamų Komisijos saugumo institucijos nustatytų priemonių siekiant išvengti šio pavojaus.

5. Naujos infrastruktūros atveju fizinio saugumo reikalavimai ir jos funkcinės specifikacijos apibrėžiami infrastruktūros planavimo ir projektavimo metu konsultuojantis su Komisijos saugumo institucija. Esamų infrastruktūrų fizinio saugumo reikalavimai įgyvendinami laikantis įgyvendinimo taisyklėse nustatytų būtiniausių standartų, normų ir kriterijų.

18 straipsnis

ESĮI fizinei apsaugai skirta įranga

1. ESĮI fizinės apsaugos tikslais nustatomos dviejų tipų fiziškai apsaugotos zonos:
a) administracinės zonos;
b) saugios zonos (įskaitant techniniu požiūriu saugias zonas).

2. Komisijos saugumo akreditavimo institucija nustato, ar zona atitinka reikalavimus, kad būtų laikoma administracine zona, saugia zona ar techniniu požiūriu saugia zona.

3. Administracinių zonų atveju:
a) nustatomas aiškiai apribotas plotas, kad būtų galima tikrinti asmenis ir, jei įmanoma, transporto priemones;
b) į šias zonas įeiti nelydimiems leidžiama tik tiems asmenims, kuriems Komisijos saugumo institucija ar bet kuri kita kompetentinga institucija suteikė tinkamą leidimą;
c) visi kiti asmenys visą laiką lydimi arba jiems turi būti taikomos lygiavertės kontrolės priemonės.

4. Saugių zonų atveju:
a) nustatomas aiškiai apribotas ir saugomas plotas, per kurį kiekvienas įėjimas ir išėjimas yra kontroliuojamas naudojantis leidimų arba asmens atpažinimo sistema;
b) į zoną įeiti nelydimiems leidžiama tik tiems asmenims, kurių patikimumas patikrintas ir kurie turi specialų leidimą įeiti į zoną, nes jiems „būtina žinoti“;
c) visi kiti asmenys turi būti visą laiką lydimi arba jiems turi būti taikomos lygiavertės kontrolės priemonės.

5. Tais atvejais, kai įėjus į saugią zoną galima visais praktiniais tikslais tiesiogiai susipažinti su joje laikoma įslaptinta informacija, taikomi tokie papildomi reikalavimai:
a) aiškiai nurodomas paprastai zonoje laikomos informacijos aukščiausio slaptumo žymos lygis;
b) visi lankytojai privalo turėti specialų leidimą, suteikiantį teisę įeiti į zoną, turi būti visą laiką lydimi ir jų patikimumas turi būti tinkamai patikrinamas, nebent imtasi priemonių užtikrinti, kad nebūtų įmanoma susipažinti su ESĮI.

6. Nuo pasiklausymo apsaugotos saugios zonos klasifikuojamos kaip techniniu požiūriu saugios zonos. Taikomi šie papildomi reikalavimai:

a) tokiose zonose įdiegiama įsibrovimo aptikimo sistema (ĮAS) ir, kai jose nedirbama, jos turi būti rakinamos, o kai dirbama – saugomos. Visi raktai valdomi vadovaujantis 20 straipsniu;
b) visi į tokias zonas įeinantys asmenys ar įnešamos medžiagos kontroliuojami;
c) tokios zonos reguliariai fiziškai ir (arba) techniškai tikrinamos Komisijos saugumo institucijos. Be to, tokie patikrinimai atliekami, kai į zoną buvo įeita be leidimo ar įtariama apie tokį įėjimą;
d) tokiose zonose negali būti ryšių linijų, kurioms nesuteiktas leidimas, telefonų, kuriems nesuteiktas leidimas, ar kitų ryšių prietaisų bei elektros ar elektroninės įrangos, kuriems nesuteiktas leidimas.

7. Nepaisant 6 punkto d papunkčio, prieš naudojantis ryšių prietaisais ir elektros ar elektronine įranga zonose, kuriose rengiami susitikimai ar atliekamas darbas, susijęs su SECRET UE/ES SECRET arba aukštesnio laipsnio slaptumo žyma pažymėta informacija, taip pat kai grėsmė ESĮI vertinama kaip didelė, tokius prietaisus ir įrangą visų pirma ištiria Komisijos saugumo institucija, siekdama užtikrinti, kad naudojantis šia įranga nebūtų galima perduoti jokios suprantamos informacijos per neapdairumą ar neteisėtai už saugios zonos ploto.

8. Saugios zonos, kuriose nėra visą parą budinčio personalo, atitinkamais atvejais tikrinamos pasibaigus įprastoms darbo valandoms ir atsitiktiniais intervalais ne įprastomis darbo valandomis, išskyrus atvejus, kai įdiegta ĮAS.

9. Siekiant surengti susitikimą, kuriame naudojama įslaptinta informacija, arba bet kokiu kitu panašiu tikslu administracinėje zonoje gali būti laikinai įrengtos saugios zonos ir techniniu požiūriu saugios zonos.

10. Atitinkamo Komisijos padalinio VSP parengia kiekvienos saugios zonos, už kurią jis atsakingas, saugios eksploatacijos taisykles (SET), kuriose, laikantis šio sprendimo ir jo įgyvendinimo taisyklių, nurodoma:
a) ESĮI, kuri gali būti tvarkoma ir saugoma toje zonoje, slaptumo žymos lygis;
b) įdiegtinos stebėjimo ir apsaugos priemonės;
c) kokiems asmenims leidžiama nelydimiems įeiti į zoną, vadovaujantis principu, kad jiems „būtina žinoti“, ir jų saugumo leidimais;
d) atitinkamais atvejais palydos tvarka ir ESĮI apsaugos tvarka, kai kitiems asmenims leidžiama įeiti į zoną;
e) bet kurios kitos atitinkamos priemonės ir procedūros.

11. Saugiose zonose įrengiamos saugyklos. Sienos, grindys, lubos, langai ir durys su užraktais patvirtinamos Komisijos saugumo institucijos ir užtikrina apsaugą, kurią užtikrina apsauginės talpyklos, patvirtintos to paties lygio slaptumo žymos ESĮI saugoti.

19 straipsnis

Fizinės apsaugos priemonės tvarkant ir saugant ESĮI

1. Slaptumo žyma RESTREINT UE/ES RESTRICTED pažymėta ESĮI gali būti tvarkoma:

a) saugiose zonose;
b) administracinėse zonose, jeigu ESĮI yra apsaugota taip, kad su ja negalėtų susipažinti leidimo neturintys asmenys;
c) ne saugiose zonose ar administracinėse zonose, jeigu turėtojas gabena ESĮI pagal 31 straipsnį ir yra įsipareigojęs taikyti kompensacines priemones, nustatytas įgyvendinimo priemonėse, kad būtų užtikrinta, jog ESĮI yra apsaugota taip, kad su ja negalėtų susipažinti leidimo neturintys asmenys.

2. Slaptumo žyma RESTREINT UE/ES RESTRICTED pažymėta ESĮI saugoma tinkamuose rakinamuose biuro balduose administracinėse zonose arba saugiose zonose. Ji gali būti laikinai saugoma ne administracinėse zonose arba ne saugiose zonose, jeigu turėtojas yra įsipareigojęs taikyti kompensacines priemones, nustatytas įgyvendinimo priemonėse.

3. Slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėta ESĮI gali būti tvarkoma:

a) saugiose zonose;
b) administracinėse zonose, jeigu ESĮI yra apsaugota taip, kad su ja negalėtų susipažinti leidimo neturintys asmenys;
c) ne saugiose zonose ar administracinėse zonose, jeigu turėtojas:

i) yra įsipareigojęs taikyti kompensacines priemones, nustatytas įgyvendinimo priemonėse, kad būtų užtikrinta, jog ESĮI yra apsaugota taip, kad su ja negalėtų susipažinti leidimo neturintys asmenys;

ii) visą laiką asmeniškai kontroliuoja ESĮI;

iii) jei dokumentai yra popierinio pavidalo, apie tai pranešė atitinkamai registratūrai.

4. Slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėta ESĮI saugoma saugiose zonose

esančiose apsauginėse talpyklose arba saugyklose.

5. Slaptumo žyma TRES SECRET UE/ES TOP SECRET pažymėta ESĮI tvarkoma saugiose zonose, kurias sukuria ir tvarko Komisijos saugumo institucija ir kurias Komisijos saugumo akreditavimo institucija akredituoja kaip saugias zonas.

6. Slaptumo žyma TRES SECRET UE/ES TOP SECRET pažymėta ESĮI saugoma Komisijos saugumo akreditavimo institucijos akredituotose tokio lygio saugiose zonose laikantis kurios nors iš toliau nurodytų sąlygų:

a) apsauginėje talpykloje laikantis 18 straipsnio nuostatų, taikant vieną ar kelias iš toliau nurodytų kontrolės priemonių:

   1) nuolatinė apsauga arba tikrinimas, kurį vykdo apsaugos arba budintis personalas, kurio patikimumas patikrintas;

   2) patvirtinta ĮAS kartu veikiant apsaugos reagavimo personalui;

b) saugykloje su įrengta ĮAS kartu veikiant apsaugos reagavimo personalui.

20 straipsnis

ESĮI apsaugai užtikrinti naudojamų raktų ir kodų kontrolė

1. Kabinetų, patalpų, saugyklų ir apsauginių talpyklų raktų bei kodų valdymo procedūros nustatomos įgyvendinimo taisyklėse remiantis 60 straipsniu. Tokių procedūrų tikslas – apsaugoti nuo susipažinimo su informacija neturint leidimo.

2. Kodus įsimena kuo mažesnis asmenų, kuriems būtina juos žinoti, skaičius. Apsauginių talpyklų ir saugyklų, kuriose saugoma ESĮI, kodai keičiami:

a) gavus naują talpyklą;
b) pasikeitus kodus žinančiam personalui;
c) neteisėtai atskleidus kodus arba įtarus jų neteisėtą atskleidimą;
d) po spynos techninio patikrinimo ar remonto;
e) bent kas 12 mėnesių.

4 SKYRIUS

ES ĮSLAPTINTOS INFORMACIJOS VALDYMAS

21 straipsnis

Pagrindiniai principai

1. Visi ESĮI dokumentai turėtų būti tvarkomi laikantis Komisijos politikos dėl dokumentų tvarkymo, todėl jie turėtų būti užregistruojami, kataloguojami, saugomi ir galiausiai sunaikinami, atrenkami arba perduodami istoriniams archyvams laikantis bendro Europos Komisijos bylų saugojimo sąrašo.

2. CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta informacija saugumo tikslais registruojama prieš ją platinant ir ją gavus. Slaptumo žyma TRES SECRET UE/ES TOP SECRET pažymėta informacija registruojama tam skirtose registratūrose.

3. Komisijos ESĮI registravimo sistema sukuriama remiantis 27 straipsnio nuostatomis.

4. Komisijos padalinius ir patalpas, kuriuose ESĮI tvarkoma arba saugoma, reguliariai tikrina Komisijos saugumo institucija.

5. Už fiziškai apsaugotų zonų ribų ESĮI iš vienos tarnybos į kitą ir iš vienų patalpų į kitas perduodama šiais būdais:

a) paprastai ESĮI perduodama elektroninėmis priemonėmis apsaugant informaciją pagal 5 skyrių patvirtintomis kriptografinėmis priemonėmis;

b) kai nenaudojamos a papunktyje nurodytos priemonės, ESĮI gabenama:

i) elektroninėse laikmenose (pvz., USB atmintinėse, kompaktiniuose diskuose, kietuosiuose diskuose), informaciją apsaugant pagal 5 skyrių patvirtintomis kriptografinėmis priemonėmis;

ii) visais kitais atvejais – kaip nurodyta įgyvendinimo taisyklėse.

22 straipsnis

Slaptumo ir kitos žymos

1. Informacija įslaptinama tuo atveju, jei dėl jos konfidencialumo reikia ją apsaugoti pagal 3 straipsnio 1 dalį.

2. ESĮI rengėjas atsako už slaptumo žymos lygio nustatymą pagal atitinkamas įgyvendinimo taisykles, įslaptinimo standartus ir gaires ir už pirminį informacijos platinimą.

3. ESĮI slaptumo žymos lygis nustatomas vadovaujantis 3 straipsnio 2 dalimi ir susijusiomis įgyvendinimo nuostatomis.

4. Slaptumo žyma nurodoma aiškiai ir teisingai, neatsižvelgiant į tai, ar ESĮI yra pateikiama popieriuje, žodžiu, elektronine ar bet kuria kita forma.

5. Atskiroms dokumento dalims (t. y. puslapiams, pastraipoms, skirsniams, priedams ir priedėliams) gali būti suteikiamos skirtingos slaptumo žymos ir jos atitinkamai pažymimos, taip pat tais atvejais, kai jos saugomos elektronine forma.

6. Dokumento ar dokumentų bylos bendras slaptumo žymos lygis nustatomas bent pagal aukščiausią slaptumo žymos lygį turinčią jų dalį. Kai renkama informacija iš įvairių šaltinių, galutinis dokumentas peržiūrimas siekiant nustatyti jo bendrą slaptumo žymos lygį, nes gali prireikti jam suteikti aukštesnį slaptumo žymos lygį nei jo dalims.

7. Kiek įmanoma, dokumentams, kurių dalys pažymėtos skirtingo lygio slaptumo žymomis, suteikiama tokia struktūra, kad skirtingo lygio slaptumo žymomis pažymėtas dalis būtų galima lengvai nustatyti ir prireikus atskirti.

8. Su priedais pateikiamų dokumentų slaptumo žymos laipsnis atitinka priedų aukščiausio laipsnio slaptumo žymas. Jei tokie dokumentai pateikiami atskirai nuo priedų, įslaptintos informacijos rengėjas aiškiai nurodo, koks slaptumo žymos lygis jiems suteikiamas, naudodamas atitinkamą žymą, pavyzdžiui: CONFIDENTIEL UE/ES CONFIDENTIAL, be priedo (-ų) RESTREINT UE/ES RESTRICTED.

23 straipsnis

Žymos

Be vienos iš slaptumo žymų, nurodytų 3 straipsnio 2 dalyje, ESĮI gali būti pažymėta papildomomis žymomis, pavyzdžiui:

a) identifikatoriumi, kuriuo nurodomas įslaptintos informacijos rengėjas;
b) bet kuriomis žymomis, kodiniais žodžiais ar santrumpomis, kuriais nurodoma veiklos sritis, su kuria dokumentas yra susijęs, jo specialus platinimas vadovaujantis principu „būtina žinoti“ arba naudojimo apribojimai;
c) paskirstymo žymomis;
d) jei taikoma, nurodant datą ar konkretų įvykį, po kurio informacijos slaptumas gali būti sumažintas arba ji gali būti išslaptinta.

24 straipsnis

Žymų santrumpos

1. Nurodant atskirų teksto pastraipų slaptumo žymos lygį gali būti naudojamos standartinės slaptumo žymų santrumpos. Santrumpos nepakeičia visais žodžiais nurodytų slaptumo žymų.

2. ES įslaptintuose dokumentuose gali būti naudojamos šios standartinės santrumpos, kuriomis nurodomas skirsnių arba teksto dalių, užimančių mažiau nei vieną puslapį, slaptumo žymos lygis:

TRES SECRET UE/ES TOP SECRET	– TS-UE/ES-TS;
SECRET UE/ES SECRET	– S-UE/ES-S;
CONFIDENTIEL UE/ES CONFIDENTIAL	– C-UE/ES-C;
RESTREINT UE/ES RESTRICTED	– R-UE/ES-R.

25 straipsnis

ESĮI rengimas

1. Rengiant ES įslaptintą dokumentą:

a) kiekvienas puslapis aiškiai pažymimas slaptumo žyma;
b) kiekvienas puslapis numeruojamas;
c) dokumente nurodomas jo registracijos numeris ir tema, kurie nėra įslaptinta informacija, išskyrus tuos atvejus, kai jie pažymėti kaip įslaptinta informacija;

d) dokumente nurodoma data;

e) jei platinamos kelios dokumentų, pažymėtų SECRET UE/ES SECRET ar aukštesnio lygio slaptumo žyma, kopijos, kiekvienos iš jų kiekviename puslapyje nurodomas kopijos numeris.

2. Kai rengiant ESĮI neįmanoma taikyti 1 dalyje išdėstytų reikalavimų, remiantis įgyvendinimo taisyklėmis taikomos kitos tinkamos priemonės.

26 straipsnis

ESĮI slaptumo mažinimas ir ESĮI išslaptinimas

1. Įslaptintos informacijos rengėjas, kai įmanoma, rengdamas ESĮI nurodo, ar tam tikrą dieną arba po tam tikro įvykio galima sumažinti ESĮI slaptumą arba ją išslaptinti.

2. Kiekviena Komisijos tarnyba reguliariai peržiūri savo parengtą ESĮI, siekdama įsitikinti, ar slaptumo žymos lygis vis dar taikomas. Įgyvendinimo taisyklėse nustatoma sistema, skirta Komisijos parengtos registruotos ESĮI slaptumo žymos lygiui peržiūrėti ne rečiau kaip kas penkerius metus. Tokia peržiūra nėra reikalinga, jeigu įslaptintos informacijos rengėjas iš pat pradžių nurodo, kad informacijos slaptumas bus sumažintas arba informacija išslaptinta automatiškai, o informacija buvo atitinkamai pažymėta.

3. Komisijos parengta informacija, pažymėta slaptumo žyma RESTREINT UE/ES RESTRICTED, remiantis Reglamentu (EEB, Euratomas) Nr. 354/83 su pakeitimais, padarytais Tarybos reglamentu (EB, Euratomas) Nr. 1700/2003 ([10]), automatiškai laikoma visiškai išslaptinta praėjus trisdešimčiai metų.

27 straipsnis

ESĮI registravimo sistema Komisijoje

1. Nedarant poveikio 52 straipsnio 5 daliai, kiekviename Komisijos padalinyje, kuriame tvarkoma arba saugoma ESĮI, pažymėta CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET slaptumo žyma, nustatoma atsakinga vietinė ESĮI registratūra, siekiant užtikrinti, kad ESĮI būtų tvarkoma pagal šį sprendimą.

2. Generalinio sekretoriato valdoma ESĮI registratūra yra centrinė Komisijos ESĮI registratūra. Ji veikia kaip:

– vietinė Komisijos Generalinio sekretoriato ESĮI registratūra;
– privačių Komisijos narių kabinetų ESĮI registratūra, išskyrus atvejus, kai jiems paskirta vietinė ESĮI registratūra;
– generalinių direktoratų arba tarnybų, kuriose nėra vietinės ESĮI registratūros, ESĮI registratūra;
– pagrindinis visos informacijos, pažymėtos RESTREINT UE/ES RESTRICTED ir aukštesne, įskaitant SECRET UE/ES SECRET, slaptumo žyma, kuria keičiasi Komisija ir jos tarnybos su trečiosiomis valstybėmis bei tarptautinėmis organizacijomis, bei, kai tai numatyta specialia tvarka, kitos Europos Sąjungos institucijos, agentūros ir įstaigos, gavimo ir išsiuntimo punktas.

3. Komisijos saugumo institucija Komisijoje įsteigia centrinę registratūrą, kuri veikia kaip centrinė slaptumo žyma TRES SECRET UE/ES TOP SECRET pažymėtą informaciją gaunanti ir siunčianti institucija. Prireikus gali būti paskirtos antrinės registratūros, kurios tvarko tokią informaciją jos registravimo tikslais.

4. Antrinės registratūros negali perduoti slaptumo žyma TRES SECRET UE/ES TOP SECRET pažymėtų dokumentų tiesiogiai kitoms tos pačios centrinės TRES SECRET UE/ES TOP SECRET registratūros antrinėms registratūroms arba į išorę be aiškaus rašytinio centrinės registratūros leidimo.

5. ESĮI registratūros įrengiamos kaip 3 skyriuje nurodytos saugios zonos ir akredituojamos Komisijos saugumo akreditavimo institucijos (SAI).

28 straipsnis

Registracijos kontrolės pareigūnas

1. Kiekvieną ESĮI registratūrą valdo registracijos kontrolės pareigūnas (RKP).

2. RKP turi tinkamą patikimumo pažymėjimą.

3. RKP veiklą, susijusią su ESĮI dokumentų tvarkymo nuostatų taikymu ir atitinkamų saugumo taisyklių laikymusi Komisijos padalinyje, prižiūri vietos saugumo pareigūnas (VSP).

4. ESĮI registratūros, į kurią paskirtas, valdymo užduotis vykdančiam RKP pagal šį sprendimą ir atitinkamas įgyvendinimo taisykles, standar-

tus ir gaires tenka šios bendros užduotys:

– valdyti veiksmus, susijusius su informacijos registravimu, saugojimu, kopijavimu, vertimu, perdavimu, siuntimu ir naikinimu arba perdavimu ESĮI istorinių archyvų tarnybai;
– periodiškai tikrinti, ar būtina, kad informacija išliktų įslaptinta;
– atlikti bet kokias kitas su ESĮI apsauga susijusias įgyvendinimo taisyklėse nustatytas užduotis.

29 straipsnis

ESĮI registravimas saugumo tikslais

1. Šiame sprendime registravimas saugumo tikslais (toliau – registravimas) – procedūrų, kuriomis užregistruojamas ESĮI gyvavimo ciklas, įskaitant jos platinimą, taikymas.

2. Organizacinis vienetas, gavęs CONFIDENTIEL UE/ES CONFIDENTIAL ir aukštesnio lygio slaptumo žyma pažymėtą informaciją ar medžiagą arba ją išsiuntęs, ją užregistruoja tam skirtose registratūrose.

3. Kai ESĮI tvarkoma arba saugoma naudojant ryšių ir informacinę sistemą (RIS), registravimo procedūros gali būti atliekamos vykdant procesus pačioje RIS.

4. Išsamesnės ESĮI registravimo saugumo tikslais nuostatos numatomos įgyvendinimo taisyklėse.

30 straipsnis

ES įslaptintų dokumentų kopijavimas ir vertimas

1. Slaptumo žyma TRES SECRET UE/ES TOP SECRET pažymėti dokumentai kopijuojami arba verčiami tik gavus išankstinį rašytinį įslaptintos informacijos rengėjo sutikimą.

2. Jeigu SECRET UE/ES SECRET arba žemesnio lygio slaptumo žyma pažymėtų dokumentų rengėjas nenustatė apribojimų dėl jų kopijavimo ar vertimo, dokumento turėtojo nurodymu tokius dokumentus galima kopijuoti arba versti.

3. Dokumento kopijoms ir vertimams taikomos tokios pat saugumo priemonės kaip ir dokumento originalui.

31 straipsnis

ESĮI gabenimas

1. ESĮI gabenama taip, kad pervežama būtų apsaugota nuo neteisėto atskleidimo.

2. Gabenant ESĮI taikomos apsaugos priemonės, kurios:
- atitinka gabenamos ESĮI slaptumo žymos lygį;
- pritaikytos prie ypatingų jos gabenimo sąlygų, visų pirma atsižvelgiant į tai, ar ESĮI gabenama:
  - Komisijos pastate arba uždaroje Komisijos pastatų grupėje;
  - tarp Komisijos pastatų, esančių toje pačioje valstybėje narėje;
  - Europos Sąjungoje,
  - iš Europos Sąjungos į trečiosios valstybės teritoriją;
  - pritaikytos prie ESĮI pobūdžio ir formos.

3. Šios apsaugos priemonės išsamiai nustatomos įgyvendinimo taisyklėse arba, kai įgyvendinami 42 straipsnyje nurodyti projektai ir programos, yra neatsiejama atitinkamos programos ar projekto saugumo instrukcijų (PSI) dalis.

4. Į įgyvendinimo taisykles arba PSI įtraukiamos nuostatos, atitinkančios ESĮI slaptumo žymos lygį, susijusios su:
- gabenimo rūšimis, kaip antai, ar informaciją gabena kurjeris, diplomatinis arba karinis kurjeris, ar ji gabenama pašto tarnybomis arba komercinėmis kurjerių pašto tarnybomis;
- ESĮI pakuotėmis;
- techninėmis apsaugos priemonėmis, kai ESĮI gabenama elektroninėje laikmenoje;
- bet kokiomis kitomis procedūrinėmis, fizinėmis arba elektroninėmis priemonėmis;
- registravimo procedūromis;
- saugumo leidimus turinčių darbuotojų naudojimu.

5. Kai ESĮI gabenama elektroninėje laikmenoje ir nepaisant 21 straipsnio 5 dalies, atitinkamose įgyvendinimo taisyklėse nustatytos apsaugos priemonės gali būti papildytos Komisijos saugumo institucijos patvirtintomis techninėmis apsaugos priemonėmis, kad būtų sumažinta informacijos praradimo arba atskleidimo rizika.

32 straipsnis

ESĮI sunaikinimas

1. Nebereikalingi ES įslaptinti dokumentai gali būti sunaikinti, laikantis teisės aktų dėl archyvų ir Komisijos dokumentų tvarkymo ir archyvavimo taisyklių bei nuostatų, visų pirma bendrojo visos Komisijos informacijos saugojimo sąrašo.

2. Informacijos turėtojo arba kompetentingos institucijos nurodymu už ESĮI registratūrą atsakingas RKP sunaikina CONFIDENTIEL UE/ES CONFIDENTIAL ir aukštesnio lygio slaptumo žyma pažymėtą ESĮI. RKP atitinkamai atnaujina registrų knygos ir kitą registravimo informaciją.

3. Dokumentus, pažymėtus SECRET UE/ES SECRET arba TRES SECRET UE/ES TOP SECRET slaptumo žyma, RKP naikina dalyvaujant liudytojui, kuris turi leidimą susipažinti su ne žemesnio už naikinamo dokumento slaptumo žymos lygio įslaptinta informacija.

4. Už registrą atsakingas darbuotojas ir liudytojas, kai pastarojo dalyvavimas privalomas, pasirašo sunaikinimo aktą, kuris įtraukiamas į atitinkamą registrą. Už ESĮI registrą atsakingas RKP slaptumo žyma TRES SECRET UE/ES TOP SECRET pažymėtų dokumentų sunaikinimo aktus registre saugo ne trumpiau kaip dešimt metų, o CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET slaptumo žyma pažymėtų dokumentų sunaikinimo aktus – ne trumpiau kaip penkerius metus.

5. Įslaptinti dokumentai, įskaitant pažymėtus RESTREINT UE/ES RESTRICTED slaptumo žyma, sunaikinami įgyvendinimo taisyklėse nustatytais būdais, atitinkančiais atitinkamus ES arba lygiaverčius standartus.

6. Įslaptintai informacijai saugoti naudotos kompiuterinių duomenų saugojimo laikmenos sunaikinamos laikantis įgyvendinimo taisyklėse nustatytų procedūrų.

33 straipsnis

ESĮI sunaikinimas ekstremaliosios padėties atveju

1. ESĮI tvarkantys Komisijos padaliniai, atsižvelgdami į vietos sąlygas, parengia ES įslaptintos medžiagos apsaugojimo kriziniais atvejais planus, kurie prireikus gali apimti ir sunaikinimo ar evakuacijos ekstre-

maliosios padėties atveju planus. Juose pateikiami nurodymai, kurių reikia laikytis norint apsaugoti ESĮI nuo patekimo į leidimo ja naudotis neturinčių asmenų rankas.

2. Priemonės, skirtos slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėtai medžiagai apsaugoti ir (arba) sunaikinti kriziniais atvejais, jokiomis aplinkybėmis neturi pakenkti medžiagos, pažymėtos slaptumo žyma TRES SECRET UE/ES TOP SECRET, apsaugai arba sutrukdyti ją, taip pat ir šifravimo įrangą sunaikinti – tai padaryti yra aukščiausio prioriteto užduotis.

3. Ekstremaliosios padėties atveju, jei gresia tiesioginis neteisėto atskleidimo pavojus, ESĮI turėtojas sunaikina ją taip, kad ji negalėtų būti atkurta visa arba iš dalies. Rengėjas ir pirminė registratūra informuojami apie registruotos ESĮI sunaikinimą dėl ekstremaliosios padėties.

4. Išsamesnės ESĮI naikinimo nuostatos numatomos įgyvendinimo taisyklėse.

5 SKYRIUS

ES ĮSLAPTINTOS INFORMACIJOS APSAUGA RYŠIŲ IR INFORMACINĖSE SISTEMOSE (RIS)

34 straipsnis

Pagrindiniai informacijos saugumo užtikrinimo principai

1. Informacijos saugumo užtikrinimas (ISU) ryšių ir informacinių sistemų srityje – užtikrinimas, kad tokiose sistemose tvarkoma informacija bus apsaugota ir kad, valdant teisėtiems naudotojams, jos veiks taip, kaip turi veikti, ir tada, kada turi veikti.

2. Veiksmingu informacijos saugumo užtikrinimu garantuojamas tinkamas lygis:

Autentiškumo:	užtikrinimas, kad informacija yra tikra ir gauta iš *bona fide* šaltinių;
Prieinamumo:	galimybė leidimą turinčiam subjektui pateikus prašymą gauti informaciją ir ja naudotis;
Konfidencialumo:	savybė, kuri reiškia, kad informacija nėra atskleidžiama leidimo neturintiems asmenims ir subjektams arba panaudojama neteisėtiems procesams;
Vientisumo:	savybė, kuri reiškia, kad apsaugomas turto ir informacijos tikslumas ir visuma;
Nepaneigiamumo:	galimybė įrodyti, kad veiksmas buvo atliktas ar įvykis įvyko, kad šio įvykio ar veiksmo paskui nebūtų galima užginčyti.

3. ISU grindžiamas rizikos valdymo procesu.

35 straipsnis

Apibrėžtys

Šiame skyriuje vartojamų terminų apibrėžtys:

a) **akreditavimas** – saugumo akreditavimo institucijos (SAI) suteiktas oficialus leidimas ir patvirtinimas, kad ryšių ir informacinės sistemos veiklos aplinkoje galima tvarkyti ESĮI; jis suteikiamas po oficialaus saugumo plano patvirtinimo ir tinkamo jo įgyvendinimo;

b) **akreditavimo procesas** – būtini veiksmai ir užduotys, kuriuos privaloma atlikti siekiant gauti saugumo akreditavimo institucijos akreditavimą. Šie veiksmai bei užduotys nurodomi akreditavimo proceso standartuose;

c) **ryšių ir informacinė sistema (RIS)** – sistema, sudaranti sąlygas tvarkyti informaciją elektroniniu būdu. Ryšių ir informacinė sistema apima visas sistemos dalis, kurių reikia jos veikimui užtikrinti, įskaitant infrastruktūrą, organizavimą, personalą ir informacijos išteklius;

d) **likutinė rizika** – rizika, kuri lieka po to, kai buvo įgyvendintos saugumo priemonės, atsižvelgiant į tai, kad ne nuo visų grėsmių apsisaugoma ir ne visi pažeidžiamumo aspektai gali būti pašalinti;

e) **rizika** – galimybė, kad tam tikros grėsmės atveju bus pasinaudota organizacijos ar sistemų vidiniu ir išoriniu pažeidžiamumu ir taip bus padaryta žala organizacijai ir jos materialiajam ar nematerialiajam turtui. Ji įvertinama atsižvelgiant į kylančios grėsmės tikimybę ir į jos poveikį;

f) **rizikos pripažinimas** – valdant riziką priimtas sprendimas pripažinti, kad vis dar yra likutinė rizika;

g) **rizikos įvertinimas** – grėsmių ir pažeidžiamų sričių nustatymas bei susijusios rizikos analizės, t. y. galimumo ir poveikio analizės, atlikimas;

h) **informavimas apie riziką** – RIS vartotojų bendruomenės informuotumo apie riziką didinimas, patvirtinimo institucijų informavimas apie tokią riziką ir pranešimų vykdančiosioms institucijoms teikimas;

i) **rizikos valdymas** – rizikos silpninimas, šalinimas, mažinimas (taikant tinkamas technines, fizines, organizacines arba procedūrines priemones), perkėlimas arba stebėjimas.

36 straipsnis

RIS, kuriose tvarkoma ESĮI

1. RIS sistemose ESĮI tvarkoma laikantis ISU principo.

2. RIS sistemoms, kuriose tvarkoma ESĮI, taikoma Komisijos informacinių sistemų saugumo politika, apibrėžta Komisijos sprendime C(2006) 3602 ([11]):

a) įgyvendinant informacinių sistemų saugumo politiką visą informacinių sistemų gyvavimo ciklą taikomas principas „planuoti–daryti–tikrinti–veikti“;

b) atliekant veiklos poveikio vertinimą turi būti nustatomi saugumo poreikiai;
c) oficialiai klasifikuojamas informacinės sistemos inventorius ir joje kaupiami duomenys;
d) privaloma taikyti visas privalomas saugumo priemones, nustatytas įgyvendinant informacinių sistemų saugumo politiką;
e) privaloma taikyti rizikos valdymo procesą, kurį sudaro šie etapai: grėsmių ir pažeidžiamumo nustatymas, rizikos vertinimas, rizikos tvarkymas, rizikos pripažinimas ir informavimas apie riziką;
f) rengiamas, įgyvendinamas, tikrinamas ir peržiūrimas saugumo planas, įskaitant saugumo politiką ir saugios eksploatacijos taisykles.

3. Visi darbuotojai, dalyvaujantys kuriant, plėtojant, bandant, eksploatuojant, valdant ar naudojant RIS, kuriose tvarkoma ESĮI, SAS praneša apie visus galimus saugumo trūkumus, incidentus, pažeidimus arba neteisėto atskleidimo atvejus, kurie gali daryti poveikį RIS ir (arba) joje tvarkomos ESĮI apsaugai.

4. Kai ESĮI apsauga užtikrinama kriptografinėmis priemonėmis, tokios priemonės patvirtinamos taip:
a) pirmenybė teikiama priemonėms, kurias patvirtino Taryba arba Tarybos Generalinis sekretorius, vykdantis Tarybos kriptografijos patvirtinimo institucijos funkcijas, remdamiesi Komisijos saugumo ekspertų grupės rekomendacija;
b) kai tai pateisinama konkrečiomis su veikla susijusiomis priežastimis, Komisijos kriptografijos patvirtinimo institucija (KPI) gali, remdamasi Komisijos saugumo ekspertų grupės rekomendacija, netaikyti a punkte nurodytų reikalavimų ir suteikti laikiną patvirtinimą tam tikram laikotarpiui.

5. ESĮI perduodant, tvarkant ir saugant elektroninėmis priemonėmis, naudojamos patvirtintos kriptografinės priemonės. Nepaisant šio reikalavimo, esant ekstremaliajai padėčiai arba specifinių techninių konfigūracijų atvejais gali būti taikomos KPI patvirtintos specialios procedūros.

6. Įgyvendinamos saugumo priemonės, siekiant apsaugoti RIS, kuriose tvarkoma CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesne slaptumo žyma pažymėta informacija, kad tokia informacija negalėtų būti neteisėtai atskleista dėl netyčinio elektromagnetinio spinduliavimo (TEMPEST apsaugos priemonės). Tokios apsaugos priemonės turi būti proporcingos neteisėto pasinaudojimo informacija rizikai ir informacijos slaptumo žymos lygiui.

7. Komisijos saugumo institucija vykdo šias funkcijas:
– ISU institucijos (ISUI),
– Saugumo akreditavimo institucijos (SAI),
– TEMPEST institucijos (TEI),
– Kriptografijos patvirtinimo institucijos (KPI),
– Kriptografijos platinimo institucijos (KPLI).

8. Komisijos saugumo institucija paskiria kiekvienos sistemos ISU operacinę instituciją.

9. 7 ir 8 dalyse nurodytų funkcijų vykdymo pareigos bus nustatytos įgyvendinimo taisyklėse.

37 straipsnis

RIS, kuriose tvarkoma ESĮI, akreditavimas

1. Visų RIS, kuriose tvarkoma ESĮI, akreditavimo procesas vykdomas remiantis ISU principais, kurių išsamumo lygis turi atitikti reikiamą apsaugos lygį.

2. Akreditavimo procesas apima oficialų Komisijos SAS pateikiamą atitinkamos RIS saugumo plano patvirtinimą siekiant įsitikinti, kad:
a) buvo tinkamai atliktas 36 straipsnio 2 dalyje nurodytas rizikos valdymo procesas;
b) sistemos savininkas žino apie likutinės rizikos pavojų ir su tuo sutinka;
c) laikantis šio sprendimo pasiektas pakankamas RIS ir joje tvarkomos ESĮI apsaugos lygis.

3. Komisijos SAI išduoda akreditavimo pareiškimą, kuriame nurodytas aukščiausias ESĮI, kuri gali būti tvarkoma RIS, slaptumo žymos lygis ir atitinkami veiklos reikalavimai bei sąlygos. Tai nedaro poveikio Saugumo akreditavimo valdybos, apibrėžtos Europos Parlamento ir Tarybos reglamento (ES) Nr. 512/2014 ([12]) 11 straipsnyje, užduotims.

4. Jungtinė saugumo akreditavimo valdyba (SAV) atsakinga už Komisijos RIS, kuriose dalyvauja keletas šalių, akreditavimą. Valdybą sudaro po vieną kiekvienos dalyvaujančios šalies SAI atstovą, o jos posėdžiams pirmininkauja Komisijos SAI atstovas.

5. Akreditavimo procesą sudaro įvairios užduotys, kurias vykdo dalyvaujančios šalys. Už akreditavimo bylų ir dokumentų rengimą atsako tik sistemos RIS savininkas.

6. Už akreditavimą atsakinga Komisijos SAI, kuri bet kuriuo RIS gyvavimo ciklo etapu turi teisę:

a) reikalauti, kad būtų taikomas akreditavimo procesas;
b) atlikti RIS auditą arba patikrą;
c) jei nebesilaikoma veikimo sąlygų, reikalauti, kad per aiškiai apibrėžtą laikotarpį būtų nustatytas ir veiksmingai įgyvendinamas saugumo gerinimo planas, o jei reikia, panaikinti RIS veiklos leidimą, kol vėl bus laikomasi veikimo sąlygų.

7. Akreditavimo procesas nustatomas RIS, kuriose tvarkoma ESĮI, akreditavimo proceso standarte, kuris patvirtinamas remiantis Komisijos sprendimo C(2006) 3602 10 straipsnio 3 dalimi.

38 straipsnis

Ekstremalioji padėtis

1. Nepaisant šio skyriaus nuostatų, toliau apibūdintos specialios procedūros gali būti taikomos esant ekstremaliajai padėčiai, pavyzdžiui, gresiant ar esant krizei, konfliktui ar karinei padėčiai arba susidarius išskirtinėms veiklos sąlygoms.

2. ESĮI gali būti perduodama naudojant kriptografines priemones, kurios buvo patvirtintos žemesnio įslaptinimo lygio informacijai, arba nešifruota kompetentingai institucijai pritarus, jei vėlavimas padarytų aiškiai didesnę žalą nei įslaptintos medžiagos atskleidimas ir jei:

a) siuntėjas ir gavėjas neturi reikiamos šifravimo įrangos;
b) įslaptinta medžiaga negali būti laiku perduota kitomis priemonėmis.

3. 1 dalyje išdėstytomis aplinkybėmis perduodama įslaptinta informacija nėra žymima jokiomis žymomis arba nuorodomis, kurios sudarytų sąlygas ją atskirti nuo informacijos, kuri yra neįslaptinta arba kurią galima apsaugoti naudojant turimas kriptografines priemones. Gavėjams kitomis priemonėmis nedelsiant pranešama apie informacijos slaptumo lygį.

4. Vėliau pateikiama ataskaita kompetentingai institucijai ir Komisijos saugumo ekspertų grupei.

6 SKYRIUS

PRAMONINIS SAUGUMAS

39 straipsnis

Pagrindiniai principai

1. Pramoninis saugumas – priemonių taikymas, siekiant užtikrinti ESĮI apsaugą

a) vykdant įslaptintas sutartis:

i) užtikrinama kandidatų ar konkurso dalyvių apsauga pasiūlymų teikimo ir sutarčių sudarymo procedūros metu;

ii) užtikrinama rangovų arba subrangovų apsauga per visą įslaptintų sutarčių gyvavimo ciklą;

b) vykdant įslaptintus dotacijos susitarimus:

i) užtikrinama pareiškėjų apsauga vykstant dotacijos skyrimo procedūroms;

ii) užtikrinama dotacijos gavėjų apsauga per visą įslaptintų dotacijos susitarimų gyvavimo ciklą.

2. Tokiose sutartyse arba dotacijos susitarimuose nenumatoma galimybė susipažinti su slaptumo žyma TRES SECRET UE/ES TOP SECRET pažymėta informacija.

3. Išskyrus atvejus, kai nustatyta kitaip, šio skyriaus nuostatos, susijusios su įslaptintomis sutartimis ar rangovais, taip pat taikomos įslaptintoms subrangos sutartims ar subrangovams.

40 straipsnis

Apibrėžtys

Šiame skyriuje vartojamų terminų apibrėžtys:

a) **įslaptinta sutartis** – Komisijos arba jos padalinio su rangovu sudaryta Tarybos reglamente (EB, Euratomas) Nr. 1605/2002 ([13]) nurodyta preliminarioji sutartis arba kilnojamojo arba nekilnojamojo turto tiekimo, darbų vykdymo arba paslaugų teikimo sutartis, kurią vykdant reikia rengti, tvarkyti arba saugoti ESĮI arba suteikiama galimybė ją rengti,

tvarkyti arba saugoti;

b) **įslaptinta subrangos sutartis** – Komisijos arba jos padalinio rangovo ir kito rangovo (t. y. subrangovo) sudaryta kilnojamojo arba nekilnojamojo turto tiekimo, darbų vykdymo arba paslaugų teikimo sutartis, kurią vykdant reikia rengti, tvarkyti arba saugoti ESĮI arba suteikiama galimybė ją rengti, tvarkyti arba saugoti;

c) **įslaptintas dotacijos susitarimas** – susitarimas, kuriuo Komisija skiria dotaciją, kaip nurodyta Reglamento (EB, Euratomas) Nr. 1605/2002 I dalies VI antraštinėje dalyje, kurią vykdant reikia rengti, tvarkyti arba saugoti ESĮI arba suteikiama galimybė ją rengti, tvarkyti arba saugoti;

d) **paskirtoji saugumo institucija (PSI)** – valstybės narės nacionalinei saugumo institucijai (NSI) atsakinga institucija, kuri atsako už pramonės ar kitų subjektų informavimą apie nacionalinę politiką visais pramoninio saugumo klausimais ir duoda nurodymus bei padeda ją įgyvendinti. PSI funkciją gali vykdyti NSI arba kita kompetentinga institucija.

41 straipsnis

Įslaptintoms sutartims arba dotacijos susitarimams taikoma procedūra

1. Kiekvienas Komisijos padalinys, kaip perkančioji organizacija, užtikrina, kad, sudarant įslaptintas sutartis arba dotacijos susitarimus, sutartyse būtų paminėti arba į juos įtraukti šiame skyriuje nustatyti būtiniausi pramoninio saugumo standartai ir kad jų būtų laikomasi.

2. Taikant 1 dalį, kompetentingos Komisijos tarnybos konsultuojasi su Žmogiškųjų išteklių ir saugumo generaliniu direktoratu, visų pirma su Saugumo direktoratu, ir užtikrina, kad į pavyzdines sutartis ir subrangos sutartis bei pavyzdinius dotacijos susitarimus būtų įtraukiamos nuostatos dėl pagrindinių principų ir būtiniausių ESĮI apsaugos standartų, kurių turi laikytis rangovai ir subrangovai bei dotacijos gavėjai pagal susitarimus.

3. Komisija glaudžiai bendradarbiauja su NSI, PSI ar kitomis kompetentingomis atitinkamų valstybių narių institucijomis.

4. Kai perkančioji organizacija ketina pradėti procedūrą, kurios tikslas – sudaryti įslaptintą sutartį arba dotacijos susitarimą, visais procedūros etapais ji konsultuojasi su Komisijos saugumo institucija dėl klausimų, susijusių su įslaptintu procedūros pobūdžiu ir aspektais.

5. Įslaptintų sutarčių ir subrangos sutarčių ir įslaptintų dotacijos susitarimų formos ir pavyzdžiai, skelbimų apie pirkimą turinys, gairės dėl aplinkybių, kuriomis reikalaujama Įmonės patikimumą patvirtinančio pažymėjimo (ĮPPP), programos arba projekto saugumo instrukcijos (PSI), saugumo aspektų paaiškinimai (SAP), vizitų nuostatos, ESĮI perdavimo ir gabenimo vykdant įslaptintas sutartis arba įslaptintus dotacijos susitarimus nuostatos, pasikonsultavus su Komisijos saugumo ekspertų grupe, nustatomos pramoninio saugumo įgyvendinimo taisyklėse.

6. Komisija gali sudaryti įslaptintas sutartis arba dotacijos susitarimus, kuriuose ekonominės veiklos vykdytojams, registruotiems valstybėje narėje arba trečiojoje valstybėje, kuri yra sudariusi susitarimą arba administracinį susitarimą pagal šio sprendimo 7 skyrių, patikimos užduotys, kurioms atlikti reikia arba gali reikėti susipažinti su ESĮI arba ją tvarkyti ar saugoti.

42 straipsnis

Įslaptintos sutarties arba įslaptinto dotacijos susitarimo saugumo aspektai

1. Į įslaptintas sutartis arba dotacijos susitarimus įtraukiami tokie saugumo aspektai:

Programos arba projekto saugumo instrukcijos

a) Programos arba projekto saugumo instrukcijos (PSI) – saugumo procedūrų, kurios yra taikomos konkrečiai programai arba projektui, siekiant standartizuoti saugumo procedūras, sąrašas. Jos gali būti tikslinamos įgyvendinant programą arba projektą.
b) Žmogiškųjų išteklių ir saugumo generalinis direktoratas parengia bendrąsias PSI, o už programas arba projektus, kuriuose tvarkoma arba saugoma ESĮI, atsakingi Komisijos padaliniai, jei reikia, remdamiesi bendrosiomis PSI gali parengti konkrečias PSI.
c) Konkrečios PSI visų pirma rengiamos įgyvendinant didelės svarbos, apimties arba sudėtingumo programas ir projektus, arba kai juose dalyvauja daug ir (arba) įvairių rangovų, dotacijos gavėjų ir kitų partnerių bei suinteresuotųjų šalių, pavyzdžiui, ypač dėl skirtingo jų teisinio statuso. Glaudžiai bendradarbiaudamas (-i) su Žmogiškųjų išteklių ir saugumo generaliniu direktoratu, konkrečias PSI rengia Komisijos padalinys (-iai), kuris (-ie) valdo programą ar projektą.

d) Žmogiškųjų išteklių ir saugumo generalinis direktoratas su Komisijos saugumo ekspertų grupe konsultuojasi ir dėl bendrųjų, ir dėl konkrečių PSI.

Saugumo aspektų paaiškinimas

a) Saugumo aspektų paaiškinimas (SAP) – specialių sutartinių sąlygų rinkinys, kurį parengia perkančioji organizacija ir kuris yra įslaptintos sutarties, pagal kurią gali būti susipažįstama su ESĮI arba tokia informacija gali būti rengiama, sudėtinė dalis; jame nurodomi saugumo reikalavimai ir tos sutarties dalys, kurių saugumą būtina užtikrinti.
b) SAP aprašomi konkrečioms sutartims skirti saugumo reikalavimai. Prireikus į SAP įtraukiamas slaptumo žymų vadovas (SŽV). SAP yra neatsiejama įslaptintos sutarties, subrangos sutarties ar dotacijos susitarimo dalis.
c) SAP nustatomos nuostatos, pagal kurias reikalaujama, kad rangovas arba dotacijos gavėjas laikytųsi būtiniausių šiame sprendime nustatytų standartų. Perkančioji organizacija užtikrina, kad SAP būtų nurodyta, jog šių būtiniausių standartų nesilaikymas gali būti pakankamas pagrindas sutarčiai arba dotacijos susitarimui nutraukti.

2. Į PSI ir SAP įtraukiamas privalomas saugumo aspektas – SŽV:

a) Slaptumo žymų vadovas (SŽV) – dokumentas, kuriame aprašomi programos, projekto, sutarties arba dotacijos susitarimo įslaptinti elementai, nurodant taikomus slaptumo žymų lygius. SŽV gali būti papildomas programos, projekto, sutarties arba dotacijos susitarimo vykdymo laikotarpiu, o informacijos dalims gali būti suteiktos naujos slaptumo žymos arba jų slaptumas gali būti sumažintas; tais atvejais, kai yra parengtas SŽV, jis yra SAP dalis.
b) Prieš paskelbdamas kvietimą teikti pasiūlymus įslaptintai sutarčiai sudaryti arba prieš sudarydamas įslaptintą sutartį, Komisijos padalinys, kaip perkančioji institucija, nustato visos informacijos, kuri turi būti suteikta kandidatams ir konkurso dalyviams arba rangovams, slaptumo žymą, taip pat visos informacijos, kurią turi parengti rangovas, slaptumo žymą. Pasikonsultavęs su Komisijos saugumo institucija, tuo tikslu jis parengia SŽV, kuris turi būti naudojamas vykdant sutartį pagal šį sprendimą ir jo įgyvendinimo taisykles.

c) Siekiant nustatyti skirtingų įslaptintos sutarties dalių slaptumo žymą, taikomi toliau nurodyti principai:

i) rengdamas SŽV, Komisijos padalinys, kaip perkančioji institucija, atsižvelgia į visus svarbius saugumo aspektus, įskaitant slaptumo žymą, kurią informacijai priskyrė informacijos rengėjas ir kurią jis patvirtino kaip naudotiną tai sutarčiai;

ii) bendras sutarties slaptumo žymos lygis negali būti žemesnis nei aukščiausia bet kurios jos dalies slaptumo žyma;

iii) atitinkamais atvejais, jei daromi pakeitimai, susiję su slaptumo žymų suteikimu informacijai, parengtai rangovų ar jiems suteiktai vykdant sutartį, ir jei daromi vėlesni SŽV pakeitimai, perkančioji institucija per Komisijos saugumo instituciją palaiko ryšius su valstybių narių NSI, PSI ar kitomis atitinkamomis kompetentingomis saugumo institucijomis.

43 straipsnis

Rangovų ir dotacijos gavėjų darbuotojų teisė susipažinti su ESĮI

Perkančioji institucija arba dotaciją skiriančioji institucija užtikrina, kad į įslaptintą sutartį arba įslaptintą dotacijos susitarimą būtų įtrauktos nuostatos, pagal kurias rangovo, subrangovo arba dotacijos gavėjo darbuotojai, kuriems vykdant įslaptintą sutartį, subrangos sutartį arba dotacijos susitarimą reikia susipažinti su ESĮI, turėtų galimybę susipažinti su tokia informacija, jei:

a) jiems buvo išduotas atitinkamo lygio saugumo leidimas arba kitas tinkamas leidimas nustačius, kad jiems „būtina žinoti“;
b) jie buvo informuoti apie ESĮI apsaugai užtikrinti taikomas saugumo taisykles ir patvirtino savo pareigą saugoti tokią informaciją;
c) atitinkama NSI, PSI ar bet kuri kita kompetentinga institucija jiems išdavė atitinkamo lygmens asmens patikimumo pažymėjimus, suteikiančius teisę susipažinti su informacija, pažymėta CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET slaptumo žyma.

44 straipsnis

Įmonės patikimumą patvirtinantis pažymėjimas

Įmonės patikimumą patvirtinantis pažymėjimas (ĮPPP) – NSI, PSI ar kitos kompetentingos saugumo institucijos išduotas administracinis patvirtinimas, kad saugumo požiūriu patalpose gali būti užtikrinta tinkama nurodyto slaptumo žymos lygio ESĮI apsauga.

2. NSI, PSI ar kita kompetentinga valstybės narės saugumo institucija, laikydamasi nacionalinių įstatymų ir kitų teisės aktų, išduoda ĮPPP, kuriuo nurodoma, kad ekonominės veiklos vykdytojas savo patalpose gali apsaugoti atitinkamo slaptumo žyma (CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET) pažymėtą ESĮI. Šis ĮPPP pateikiamas Komisijos saugumo institucijai, o ši jį perduoda Komisijos padaliniui, veikiančiam kaip perkančioji arba dotaciją skiriančioji institucija, prieš suteikiant kandidatui, konkurso dalyviui ar rangovui arba dotacijos gavėjui ESĮI arba galimybę susipažinti su ESĮI.

3. Atitinkamais atvejais perkančioji institucija per Komisijos saugumo instituciją praneša atitinkamai NSI, PSI ar kitai kompetentingai saugumo institucijai, kad sutarčiai vykdyti reikalingas ĮPPP. ĮPPP arba APP reikalaujama turėti tais atvejais, kai viešųjų pirkimų arba dotacijos skyrimo procedūrų metu reikia suteikti ESĮI, pažymėtą CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET slaptumo žyma.

4. Perkančioji institucija arba dotaciją skiriančioji institucija nesudaro įslaptintos sutarties arba dotacijos susitarimo su konkurso laimėtoju arba dalyviu prieš tai negavusi valstybės narės, kurioje yra registruotas atitinkamas rangovas ar subrangovas, NSI, PSI ar kitos kompetentingos saugumo institucijos patvirtinimo, kad reikiamais atvejais yra išduotas tinkamas ĮPPP.

5. Kai NSI, PSI ar kita kompetentinga ĮPPP išdavusi saugumo institucija Komisijos saugumo institucijai praneša apie pasikeitimus, turinčius įtakos ĮPPP, Komisijos saugumo institucija apie tai praneša Komisijos padaliniui, veikiančiam kaip perkančioji arba dotaciją skiriančioji institucija. Subrangos sutarties atveju apie tai atitinkamai informuojama NSI, PSI ar kita kompetentinga saugumo institucija.

6. Jeigu atitinkama NSI, PSI ar kita kompetentinga saugumo institucija panaikina ĮPPP, tai yra pakankamas pagrindas, kad perkančioji arba dotaciją skiriančioji institucija nutrauktų įslaptintą sutartį arba pašalintų kan-

didatą, konkurso dalyvį arba paraiškos teikėją iš konkurso. Tokia nuostata įtraukiama į rengiamas pavyzdines sutartis ir dotacijos susitarimus.

45 straipsnis

Įslaptintoms sutartims ir dotacijos susitarimams taikomos nuostatos

1. Tais atvejais, kai kandidatui, konkurso dalyviui arba paraiškos teikėjui ESĮI suteikiama, vykstant viešųjų pirkimų, kvietimo pateikti pasiūlymus arba kvietimo teikti paraiškas procedūrai, numatoma nuostata, kuria pasiūlymo arba paraiškos nepateikęs arba neatrinktas kandidatas, konkurso dalyvis arba paraiškos teikėjas įpareigojamas per nurodytą laiką grąžinti visus įslaptintus dokumentus.

2. Perkančioji arba dotaciją skiriančioji institucija per Komisijos saugumo instituciją praneša NSI, PSI ar kitai kompetentingai saugumo institucijai, kad sudaryta įslaptinta sutartis arba dotacijos susitarimas, ir perduoda susijusius duomenis, kaip antai: rangovo (-ų) arba dotacijos gavėjų pavadinimus, sutarties trukmę ir aukščiausią informacijos įslaptinimo lygį.

3. Kai tokia sutartis arba dotacijos susitarimas nutraukiami, perkančioji arba dotaciją skiriančioji institucija per Komisijos saugumo instituciją nedelsdama praneša apie tai NSI, PSI ar kitai kompetentingai valstybės narės, kurioje yra įregistruotas rangovas arba dotacijos gavėjas, saugumo institucijai.

4. Paprastai reikalaujama, kad, nutraukus įslaptintą sutartį ar įslaptintą dotacijos susitarimą arba dotacijos gavėjui nebedalyvaujant įgyvendinant įslaptintą sutartį ar įslaptintą dotacijos susitarimą, rangovas arba dotacijos gavėjas perkančiajai arba dotaciją skiriančiajai institucijai grąžintų visą turimą ESĮI.

5. SAP nustatomos konkrečios nuostatos dėl ESĮI sunaikinimo vykdant įslaptintą sutartį arba įslaptintą dotacijos susitarimą arba juos nutraukus.

6. Tais atvejais, kai rangovui arba dotacijos gavėjui suteikiamas leidimas nutraukus įslaptintą sutartį arba įslaptintą dotacijos susitarimą negrąžinti ESĮI, rangovas arba dotacijos gavėjas toliau laikosi šiame sprendime nustatytų būtiniausių standartų ir užtikrina ESĮI konfidencialumą.

46 straipsnis

Įslaptintoms sutartims taikomos konkrečios nuostatos

1. ESĮI apsaugai svarbios sąlygos, kuriomis rangovas gali sudaryti subrangos sutartis, nurodomos kvietime teikti paraiškas ir įslaptintoje sutartyje.

2. Prieš sudarydamas subrangos sutartis dėl įslaptintos sutarties dalių, rangovas turi gauti perkančiosios institucijos leidimą. Su trečiojoje šalyje registruotais subrangovais negali būti sudaromos sutartys, kurias vykdant reikia susipažinti su ESĮI, išskyrus atvejus, kai nustatoma 7 skyriuje numatyta informacijos saugumo reglamentavimo sistema.

3. Rangovas atsako už tai, kad visa subrangos veikla būtų vykdoma laikantis šiame sprendime nustatytų būtiniausių standartų, ir negali suteikti subrangovui ESĮI be išankstinio rašytinio perkančiosios institucijos sutikimo.

4. Komisija laikoma ESĮI, kurią parengė ar tvarko rangovas, rengėja, o rengėjo teisėmis naudojasi perkančioji institucija.

47 straipsnis

Su įslaptintomis sutartimis susiję vizitai

1. Jei vykdant įslaptintą sutartį arba dotacijos susitarimą Komisijos darbuotojui arba rangovo ar dotacijos gavėjo personalui vienas kito patalpose reikia susipažinti su CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET slaptumo žyma pažymėta informacija, dėl vizitų susitariama palaikant ryšius su NSI, PSI arba kita susijusia kompetentinga saugumo institucija. Apie tokius vizitus pranešama Komisijos saugumo institucijai. Tačiau įgyvendinant tam tikras programas arba projektus NSI, PSI arba kita kompetentinga saugumo institucija gali taip pat susitarti dėl tvarkos, pagal kurią dėl tokių vizitų gali būti susitariama tiesiogiai.

2. Tam, kad būtų leista susipažinti su ESĮI, kuri susijusi su įslaptinta sutartimi, visi lankytojai turi turėti atitinkamą patikimumo pažymėjimą ir jiems turi būti „būtina žinoti“.

3. Lankytojams leidžiama susipažinti tik su ta ESĮI, kuri yra susijusi su vizito tikslu.

4. Išsamesnės nuostatos nustatomos įgyvendinimo taisyklėse.

5. Privaloma laikytis šiame sprendime ir įgyvendinimo taisyklėse, nurodytose šio straipsnio 4 dalyje, numatytų vizitų, susijusių su įslaptintomis sutartimis, nuostatų.

48 straipsnis

ESĮI perdavimas ir gabenimas vykdant įslaptintas sutartis arba įslaptintus dotacijos susitarimus

1. Perduodant ESĮI elektroninėmis priemonėmis taikomos atitinkamos šio sprendimo 5 skyriaus nuostatos.

2. Gabenant ESĮI taikomos atitinkamos šio sprendimo 4 skyriaus nuostatos, laikantis nacionalinių įstatymų ir kitų teisės aktų.

3. Nustatant įslaptintos medžiagos kaip krovinio gabenimui taikomą saugumo tvarką taikomi toliau nurodyti principai:

a) saugumas užtikrinamas visuose gabenimo etapuose nuo išgabenimo vietos iki galutinės paskirties vietos;
b) siuntai suteikiamas apsaugos lygis nustatomas pagal joje esančios medžiagos aukščiausią slaptumo žymos lygį;
c) prieš gabenant per valstybių sienas medžiagą, pažymėtą CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET slaptumo žyma, siuntėjas parengia, o atitinkamos NSI, PSI ar kitos kompetentingos saugumo institucijos patvirtina gabenimo planą;
d) stengiamasi, kad kelionės vyktų be sustojimo ir būtų užbaigtos kuo greičiau, atsižvelgiant į aplinkybes;
e) kai galima, turėtų būti pasirenkami maršrutai tik per valstybes nares. Maršrutais per valstybes, kurios nėra valstybės narės, turėtų būti gabenama tik gavus siuntėjo ir gavėjo valstybių NSI, PSI ar kitos kompetentingos saugumo institucijos leidimą.

49 straipsnis

ESĮI perdavimas trečiosiose valstybėse įsikūrusiems rangovams arba dotacijos gavėjams

Trečiosiose valstybėse įsikūrusiems rangovams ir dotacijos gavėjams ESĮI perduodama laikantis saugumo priemonių, dėl kurių susita-

rė Komisijos saugumo institucija, Komisijos padalinys, kaip perkančioji arba dotaciją skiriančioji institucija, ir atitinkamos trečiosios valstybės, kurioje registruotas rangovas arba dotacijos gavėjas, NSI, PSI ar kita kompetentinga saugumo institucija.

50 straipsnis

Informacijos, pažymėtos RESTREINT UE/ES RESTRICTED žyma, tvarkymas vykdant įslaptintas sutartis arba įslaptintus dotacijos susitarimus

1. Įslaptintos informacijos, pažymėtos RESTREINT UE/ES RESTRICTED slaptumo žyma, tvarkomos ir saugomos pagal įslaptintas sutartis arba įslaptintus dotacijos susitarimus, apsauga grindžiama proporcingumo ir ekonominio efektyvumo principais.

2. Vykdant įslaptintas sutartis arba įslaptintus dotacijos susitarimus, kai tvarkoma RESTREINT UE/ES RESTRICTED slaptumo žyma pažymėta informacija, nereikalaujama turėti ĮPPP arba APP.

3. Kai pagal sutartį arba dotacijos susitarimą numatytas informacijos, pažymėtos RESTREINT UE/ES RESTRICTED slaptumo žyma, tvarkymas rangovo arba dotacijos gavėjo eksploatuojamoje RIS, perkančioji arba dotaciją skiriančioji institucija, pasikonsultavusi su Komisijos saugumo institucija, užtikrina, kad sutartyje arba dotacijos susitarime būtų nustatyti su RIS akreditavimu arba patvirtinimu susiję būtini techniniai ir administraciniai reikalavimai, kurie atitiktų įvertintą riziką, atsižvelgiant į visus svarbius veiksnius. Komisijos saugumo institucija ir atitinkama NSI ar PSI susitaria dėl tokio RIS akreditavimo arba patvirtinimo masto.

7 SKYRIUS

KEITIMASIS ĮSLAPTINTA INFORMACIJA SU KITOMIS EUROPOS SĄJUNGOS INSTITUCIJOMIS, AGENTŪROMIS, ĮSTAIGOMIS IR ORGANAIS, SU VALSTYBĖMIS NARĖMIS IR SU TREČIOSIOMIS VALSTYBĖMIS BEI TARPTAUTINĖMIS ORGANIZACIJOMIS

51 straipsnis

Pagrindiniai principai

1. Komisijai arba vienam iš jos padalinių nusprendus, kad reikia keistis ESĮI su kita Europos Sąjungos institucija, agentūra, įstaiga ar organu arba su trečiąja valstybe ar tarptautine organizacija, imamasi reikalingų priemonių, kad būtų nustatyta tam skirta tinkama teisinė arba administracinė sistema, į kurią gali būti įtraukiami susitarimai dėl informacijos saugumo arba administraciniai susitarimai, sudaryti laikantis atitinkamų teisės aktų.

2. Nedarant poveikio 57 straipsniui, ESĮI su kita Europos Sąjungos institucija, agentūra, įstaiga ar organu arba su trečiąja valstybe ar tarptautine organizacija gali būti keičiamasi, tik jeigu nustatyta tokia tinkama teisinė arba administracinė sistema ir jeigu pateikta pakankamai garantijų, kad Europos Sąjungos institucija, agentūra, įstaiga ar organas arba atitinkama trečioji valstybė ar tarptautinė organizacija taiko lygiaverčius pagrindinius įslaptintos informacijos apsaugos principus ir būtiniausius standartus.

52 straipsnis

Keitimasis ESĮI su kitomis Europos Sąjungos institucijomis, agentūromis, įstaigomis ir organais

1. Prieš sudarydama administracinį susitarimą dėl keitimosi ESĮI su kita Europos Sąjungos institucija, agentūra, įstaiga ar organu, Komisija įsitikina, kad ta Europos Sąjungos institucija, agentūra, įstaiga ar organas:

a) yra nustatę ESĮI apsaugos reguliavimo sistemą, kurioje išdėstyti pagrindiniai principai ir būtiniausi standartai, lygiaverčiai nustatytiesiems šiame sprendime ir jo įgyvendinimo taisyklėse;

b) taiko saugumo standartus ir asmens patikimumo, fizinio saugumo, ESĮI valdymo ir ryšių ir informacinių sistemų (RIS) saugumo gaires, kuriais užtikrinamas Komisijos taikomam apsaugos lygiui lygiavertis ESĮI apsaugos lygis;
c) savo parengtą ESĮI žymi įslaptintos informacijos žymomis.

2. Žmogiškųjų išteklių ir saugumo generalinis direktoratas, glaudžiai bendradarbiaudamas su kitais kompetentingais Komisijos padaliniais, vadovauja Komisijai sudarant administracinius susitarimus dėl keitimosi ESĮI su kitomis Europos Sąjungos institucijomis, agentūromis, įstaigomis ar organais.

3. Administraciniai susitarimai paprastai sudaromi pasikeičiant laiškais, kuriuos Komisijos vardu pasirašo Žmogiškųjų išteklių ir saugumo generalinis direktorius.

4. Prieš sudarant administracinį susitarimą dėl keitimosi ESĮI, Komisijos saugumo institucija surengia įvertinimo vizitą, kurio tikslas – įvertinti ESĮI apsaugai skirtą reguliavimo sistemą ir įsitikinti, kad ESĮI apsaugos priemonės įgyvendinamos veiksmingai. Administracinis susitarimas įsigalioja ir ESĮI keičiamasi tik tuo atveju, jei šio įvertinimo vizito rezultatai yra patenkinami ir buvo laikomasi po vizito pateiktų rekomendacijų. Reguliariai rengiami tolesni įvertinimo vizitai, siekiant patikrinti, ar laikomasi administracinių susitarimų ir ar apsaugos priemonės vis dar atitinka nustatytus pagrindinius principus ir būtiniausius standartus.

5. Generalinio sekretoriato valdoma Komisijos ESĮI registratūra paprastai yra pagrindinis įslaptintos informacijos, kuria keičiamasi su kitomis Europos Sąjungos institucijomis, agentūromis, įstaigomis ir organais, gavimo ir išsiuntimo punktas. Tačiau tais atvejais, kai dėl saugumo, organizacinių arba veiklos priežasčių ESĮI apsaugai labiau tiktų vietinės ESĮI registratūros, remiantis šiuo sprendimu ir jo įgyvendinimo taisyklėmis, Komisijos padaliniuose įsteigiamos tokios registratūros, kurios veikia kaip įslaptintos informacijos, susijusios su atitinkamų Komisijos padalinių kompetencijos klausimais, gavimo ir išsiuntimo punktai.

6. Komisijos Saugumo ekspertų grupė informuojama apie administracinių susitarimų pagal 2 dalį sudarymo eigą.

53 straipsnis

Keitimasis ESĮI su valstybėmis narėmis

1. ESĮI gali būti keičiamasi su valstybėmis narėmis ir ta informacija gali būti joms teikiama su sąlyga, kad valstybės narės saugos įslaptintą informaciją, laikydamosi reikalavimų, taikomų lygiaverčio nacionalinės slaptumo žymos lygio ESĮI, kaip nustatyta I priede pateiktoje slaptumo žymų atitikmenų lentelėje.

2. Valstybėms narėms nacionaline slaptumo žyma pažymėtą įslaptintą informaciją perdavus į Europos Sąjungos struktūras ar tinklus, Komisija tą informaciją saugo laikydamasi reikalavimų, taikomų lygiaverčio slaptumo žymos lygio ESĮI, kaip nustatyta I priede pateiktoje slaptumo žymų atitikmenų lentelėje.

54 straipsnis

Keitimasis ESĮI su trečiosiomis valstybėmis ir tarptautinėmis organizacijomis

1. Kai Komisija nustato, kad yra ilgalaikis poreikis keistis įslaptinta informacija su trečiosiomis valstybėmis arba tarptautinėmis organizacijomis, imamasi reikalingų priemonių, kad būtų nustatyta tam skirta tinkama teisinė arba administracinė sistema, į kurią gali būti įtraukiami susitarimai dėl informacijos saugumo arba administraciniai susitarimai, sudaryti laikantis atitinkamų teisės aktų.

2. Tokiuose 1 dalyje nurodytuose susitarimuose dėl informacijos saugumo ir administraciniuose susitarimuose numatomos nuostatos, kuriomis užtikrinama, kad trečiosioms valstybėms arba tarptautinėms organizacijoms gavus ESĮI ta informacija būtų saugoma atsižvelgiant į jos slaptumo žymos lygį, remiantis būtiniausiais standartais, kurie atitinka šiame sprendime nustatytus standartus.

3. Komisija gali pagal 56 straipsnį sudaryti administracinius susitarimus tuomet, kai ESĮI slaptumo žyma paprastai nėra aukštesnė nei RESTREINT UE/ES RESTRICTED.

4. 3 dalyje nurodytuose administraciniuose susitarimuose dėl keitimosi įslaptinta informacija numatomos nuostatos, kuriomis užtikrinama, kad trečiosioms valstybėms arba tarptautinėms organizacijoms gavus ESĮI ta informacija būtų saugoma atsižvelgiant į jos slaptumo žymos lygį, remiantis būtiniausiais standartais, kurie atitinka šiame sprendi-

me nustatytus standartus. Dėl susitarimų dėl informacijos saugumo arba administracinių susitarimų sudarymo konsultuojamasi su Komisijos saugumo ekspertų grupe.

5. Sprendimą suteikti Komisijos parengtą ESĮI trečiajai valstybei arba tarptautinei organizacijai priima tą ESĮI parengęs Komisijos padalinys, atskirai kiekvienu konkrečiu atveju atsižvelgdamas į tokios informacijos pobūdį ir turinį bei tai, ar gavėjui „būtina žinoti“, ir įvertinęs naudą Europos Sąjungai. Jeigu Komisija nėra įslaptintos informacijos, kurią prašoma suteikti, arba pradinės medžiagos, kuri gali būti įtraukta į tą informaciją, rengėja, įslaptintą informaciją turintis Komisijos padalinys pirmiausia prašo jos rengėjo pateikti rašytinį sutikimą suteikti šią informaciją. Jei įslaptintos informacijos rengėjo neįmanoma nustatyti, įslaptintą informaciją turintis Komisijos padalinys, pasikonsultavęs su Komisijos saugumo ekspertų grupe, prisiima rengėjo atsakomybę.

55 straipsnis

Susitarimai dėl informacijos saugumo

1. Susitarimai dėl informacijos saugumo su trečiosiomis valstybėmis arba tarptautinėmis organizacijomis sudaromi remiantis SESV 218 straipsniu.

2. Susitarimuose dėl informacijos saugumo:

a) nustatomi pagrindiniai principai ir būtiniausi standartai, reglamentuojantys Europos Sąjungos ir trečiosios valstybės ar tarptautinės organizacijos keitimąsi įslaptinta informacija;
b) numatomi techniniai įgyvendinimo susitarimai, dėl kurių turi susitarti atitinkamų Europos Sąjungos institucijų ir įstaigų kompetentingos saugumo tarnybos ir kompetentinga atitinkamos trečiosios valstybės ar tarptautinės organizacijos saugumo institucija. Tokiuose susitarimuose atsižvelgiama į atitinkamoje trečiojoje valstybėje ar tarptautinėje organizacijoje galiojančiais saugumo nuostatais ir esamomis struktūromis bei procedūromis užtikrinamą apsaugos lygį;
c) numatoma, kad prieš keičiantis įslaptinta informacija pagal susitarimą būtų užtikrinta, kad gaunančioji šalis atitinkamu būdu gali apsaugoti ir saugoti jai teikiamą įslaptintą informaciją.

3. Kai remiantis 51 straipsnio 1 dalimi nustatoma, kad yra poreikis keistis įslaptinta informacija, Komisija prireikus konsultuojasi su Europos išorės veiksmų tarnyba, Tarybos generaliniu sekretoriatu ir kitomis Europos Sąjungos institucijomis bei įstaigomis, kad nustatytų, ar

reikia pateikti rekomendaciją pagal SESV 218 straipsnio 3 dalį.

4. Keistis ESĮI elektroninėmis priemonėmis neleidžiama, jei tai nėra aiškiai numatyta susitarime dėl informacijos saugumo arba techniniuose įgyvendinimo susitarimuose.

5. Generalinio sekretoriato valdoma Komisijos ESĮI registratūra paprastai yra pagrindinis įslaptintos informacijos, kuria keičiamasi su trečiosiomis valstybėmis ir tarptautinėmis organizacijomis, gavimo ir išsiuntimo punktas. Tačiau tais atvejais, kai dėl saugumo, organizacinių arba veiklos priežasčių ESĮI apsaugai labiau tiktų vietinės ESĮI registratūros, remiantis šiuo sprendimu ir jo įgyvendinimo taisyklėmis Komisijos padaliniuose įsteigiamos tokios registratūros, kurios veikia kaip įslaptintos informacijos, susijusios su atitinkamų Komisijos padalinių kompetencijos klausimais, gavimo ir išsiuntimo punktai.

6. Siekiant įvertinti atitinkamos trečiosios valstybės ar tarptautinės organizacijos saugumo nuostatus, struktūras ir procedūras, Komisija, bendradarbiaudama su kitomis Europos Sąjungos institucijomis, agentūromis arba įstaigomis, dalyvauja įvertinimo vizituose abipusiu susitarimu su atitinkama trečiąja valstybe ar tarptautine organizacija. Tokiuose įvertinimo vizituose įvertinama:

a) įslaptintai informacijai apsaugoti taikoma reglamentavimo sistema;
b) bet kurie konkretūs saugumo politikos ypatumai ir saugumo organizavimo tvarka trečiojoje valstybėje arba tarptautinėje organizacijoje, kurie galėtų daryti poveikį įslaptintos informacijos, kuria gali būti keičiamasi, slaptumo žymos lygiui;
c) faktiškai taikomos saugumo priemonės ir procedūros;
d) patikimumo patikrinimo procedūros, susijusios su numatomos suteikti ESĮI slaptumo žymos lygiu.

56 straipsnis

Administraciniai susitarimai

1. Kai, taikant Europos Sąjungos politinę arba teisinę sistemą, yra ilgalaikis poreikis su trečiąja valstybe arba tarptautine organizacija keistis įslaptinta informacija, kurios slaptumo žyma paprastai nebūna aukštesnė nei RESTREINT UE/ES RESTRICTED, ir kai Komisijos saugumo institucija po konsultacijų su Komisijos saugumo ekspertų grupe visų pirma nustato, kad atitinkama šalis neturi pakankamai išplėtotos saugumo sistemos, kad galėtų sudaryti susitarimą dėl informacijos saugumo, Komisija

gali nuspręsti su atitinkamos trečiosios valstybės ar tarptautinės organizacijos atitinkamomis institucijomis sudaryti administracinį susitarimą.

2. Tokie administraciniai susitarimai paprastai sudaromi pasikeičiant laiškais.

3. Prieš sudarant susitarimą surengiamas įvertinimo vizitas. Komisijos saugumo ekspertų grupė informuojama apie įvertinimo vizito rezultatus. Jei esama išskirtinių priežasčių skubiai pasikeisti įslaptinta informacija, ESĮI gali būti suteikta su sąlyga, kad dedamos visos pastangos įvertinimo vizitą surengti kuo greičiau.

4. Keistis ESĮI elektroninėmis priemonėmis neleidžiama, jei tai nėra aiškiai numatyta administraciniame susitarime.

57 straipsnis

ESĮI *ad hoc* suteikimas išimtine tvarka

1. Jei nėra sudarytas susitarimas dėl informacijos saugumo arba administracinis susitarimas ir jei Komisija arba kuris nors jos padalinys nustato, kad taikant Europos Sąjungos politinę arba teisinę sistemą išimtiniu atveju trečiajai valstybei arba tarptautinei organizacijai reikia suteikti ESĮI, Komisijos saugumo institucija kreipiasi į atitinkamos trečiosios valstybės arba tarptautinės organizacijos saugumo institucijas ir kiek įmanoma patikrina, ar jų saugumo nuostatai, struktūros bei procedūros užtikrina, jog joms suteikta ESĮI būtų saugoma taikant ne mažiau griežtus nei šiame sprendime nustatytieji standartus.

2. Pasikonsultavusi su Komisijos saugumo ekspertų grupe, sprendimą suteikti ESĮI atitinkamai trečiajai valstybei arba tarptautinei organizacijai priima Komisija, remdamasi už saugumo klausimus atsakingo Komisijos nario pasiūlymu.

3. Komisijai priėmus sprendimą suteikti ESĮI ir gavus išankstinį rašytinį rengėjo, įskaitant pradinės medžiagos, kuri gali būti įtraukta į tą informaciją, rengėjus, sutikimą, kompetentingas Komisijos padalinys perduoda atitinkamą informaciją, pažymėtą leidimo suteikti informaciją žyma, kurioje nurodyta trečioji valstybė arba tarptautinė organizacija, kuriai informacija buvo suteikta. Prieš suteikiant tokią informaciją arba faktinio jos suteikimo metu atitinkama trečioji šalis raštu įsipareigoja apsaugoti ESĮI, kurią ji gauna, pagal šiame sprendime nustatytus pagrindinius principus ir būtiniausius standartus.

8 SKYRIUS

BAIGIAMOSIOS NUOSTATOS

58 straipsnis

Ankstesnio sprendimo pakeitimas

Šis sprendimas panaikina ir pakeičia Komisijos sprendimą 2001/844/EB, EAPB, Euratomas ([14]).

59 straipsnis

Įslaptinta informacija, parengta iki šio sprendimo įsigaliojimo

1. Visa ESĮI, įslaptinta pagal Sprendimą 2001/844/EB, EAPB, Euratomas, toliau saugoma pagal šio sprendimo atitinkamas nuostatas.

2. Visa įslaptinta informacija, Komisijos turėta Sprendimo 2001/844/EB, EAPB, Euratomas įsigaliojimo dieną, išskyrus Euratomo įslaptintą informaciją:

a) jei ji buvo parengta Komisijos, jos slaptumo žyma ir toliau laikoma pakeista į žymą RESTREINT UE, jei iki 2002 m. sausio 31 d. jos autorius nenusprendė suteikti informacijai kitos slaptumo žymos ir apie tai nepranešė visiems atitinkamo dokumento gavėjams;
b) jei ji buvo parengta ne Komisijos autorių, išlaiko savo pradinę slaptumo žymą ir todėl nelaikoma lygiaverte slaptumo žyma ESĮI, jei jos autorius nesutinka, kad informacija būtų išslaptinta arba kad jos slaptumas būtų sumažintas.

60 straipsnis

Įgyvendinimo taisyklės ir saugumo pranešimai

1. Prireikus, visapusiškai laikantis vidaus darbo tvarkos taisyklių, šio sprendimo įgyvendinimo taisyklės priimamos atskiru Komisijos sprendimu dėl įgaliojimų suteikimo už saugumo reikalus atsakingam Komisijos nariui.

2. Gavęs įgaliojimus pagal pirmiau minėtą Komisijos sprendimą, už saugumo reikalus atsakingas Komisijos narys gali rengti saugumo pranešimus, kuriuose nustatomos saugumo gairės ir geriausios praktikos pa-

vyzdžiai šio sprendimo ir jo įgyvendinimo taisyklių taikymo srityje.

3. Visapusiškai laikydamasi vidaus darbo tvarkos taisyklių, Komisija 1 ir 2 šio straipsnio dalyse minėtas užduotis atskiru sprendimu dėl įgaliojimų perdavimo gali pavesti Žmogiškųjų išteklių ir saugumo generalinio direktorato generaliniam direktoriui.

61 straipsnis

Įsigaliojimas

Šis sprendimas įsigalioja kitą dieną po jo paskelbimo *Europos Sąjungos oficialiajame leidinyje*.

Priimta Briuselyje 2015 m. kovo 13 d.

Komisijos vardu

Pirmininkas

Jean-Claude JUNCKER

([1]) Žr. 2004 m. gruodžio 31 d. „Arrangement entre le Gouvernement belge et le Parlement européen, le Conseil, la Commission, le Comité économique et social européen, le Comité des régions, la Banque européenne d'investissement en matière de sécurité", 2007 m. sausio 20 d. „Accord de sécurité signé entre la Commission et le Gouvernement luxembourgeois" ir 1959 m. liepos 22 d. „Accordo tra il Governo italiano e la Commissione europea dell'energia atomica (Euratomas) per l'istituzione di un Centro comune di ricerche nucleari di competenza generale".

([2]) 2002 m. sausio 23 d. Komisijos sprendimas 2002/47/EB, EAPB, Euratomas, iš dalies keičiantis jos darbo tvarkos taisykles (OL L 21, 2002 1 24, p. 23).

([3]) 2004 m. liepos 7 d. Komisijos sprendimas 2004/563/EB, Euratomas, iš dalies keičiantis jos darbo tvarkos taisykles (OL L 251, 2004 7 27, p. 9).

([4]) 1958 m. liepos 31 d. Reglamentas (Euratomas) Nr. 3, įgyvendinantis Europos atominės energijos bendrijos steigimo sutarties 24 straipsnį (OL 17, 1958 10 6, p. 406/58).

([5]) 2001 m. gegužės 30 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 1049/2001 „Dėl galimybės visuomenei susipažinti su Europos Parlamento, Tarybos ir Komisijos dokumentais" (OL L 145, 2001 5 31, p. 43).

([6]) 2000 m. gruodžio 18 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 45/2001 „Dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo" (OL L 8, 2001 1 12, p. 1).

([7]) 1983 m. vasario 1 d. Tarybos reglamentas (EEB, Euratomas) Nr. 354/83 „Dėl Europos eko-

nominės bendrijos ir Europos atominės energijos bendrijos istorinių archyvų atvėrimo visuomenei“ (OL L 43, 1983 2 15, p. 1).

([8]) 2015 m. kovo 13 d. Komisijos sprendimas (ES, Euratomas) 2015/443 „Dėl Komisijos saugumo“ (žr. šio Oficialiojo leidinio p. 41).

([9]) 1968 m. vasario 29 d. Tarybos reglamentas (EEB, Euratomas, EAPB) Nr. 259/68, nustatantis Europos Bendrijų pareigūnų tarnybos nuostatus ir kitų Europos Bendrijų tarnautojų įdarbinimo sąlygas bei Komisijos pareigūnams laikinai taikomas specialias priemones (Kitų tarnautojų įdarbinimo sąlygos) (OL L 56, 1968 3 4, p. 1).

([10]) 2003 m. rugsėjo 22 d. Tarybos reglamentas (EB, Euratomas) Nr. 1700/2003, iš dalies keičiantis Reglamentą (EEB, Euratomas) Nr. 354/83 „Dėl Europos ekonominės bendrijos ir Europos atominės energijos bendrijos istorinių archyvų atvėrimo visuomenei“ (OL L 243, 2003 9 27, p. 1).

([11]) 2006 m. rugpjūčio 16 d. Sprendimas C(2006) 3602 „Dėl Europos Komisijos naudojamų informacinių sistemų saugumo“.

([12]) 2014 m. balandžio 16 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 512/2014, kuriuo iš dalies keičiamas Reglamentas (ES) Nr. 912/2010, kuriuo įsteigiama Europos GNSS agentūra (OL L 150, 2014 5 20, p. 72).

([13]) 2002 m. birželio 25 d. Tarybos reglamentas (EB, Euratomas) Nr. 1605/2002 „Dėl Europos Bendrijų bendrajam biudžetui taikomo Finansinio reglamento“ (OL L 248, 2002 9 16, p. 1).

([14]) 2001 m. lapkričio 29 d. Komisijos sprendimas 2001/844/EB, EAPB, Euratomas, iš dalies keičiantis jos darbo tvarkos taisykles (OL L 317, 2001 12 3, p. 1).

I PRIEDAS

SLAPTUMO ŽYMŲ ATITIKMENYS

ES	TRES SECRET UE/ES TOP SECRET	SECRET UE/ES SECRET	CONFIDENTIEL UE/ES CONFIDENTIAL	RESTREINT UE/ES RESTRICTED
Euratomas	EURA TOP SECRET	EURA SECRET	EURA CONFIDENTIAL	EURA RESTRICTED
Belgija	Très Secret (Loi 11.12.1998) Zeer Geheim (Wet 11.12.1998)	Secret (Loi 11.12.1998) Geheim (Wet 11.12.1998)	Confidentiel (Loi 11.12.1998) Vertrouwelijk (Wet 11.12.1998)	([1]) pastaba
Bulgarija	Строго секретно	Секретно	Поверително	За служебно ползване
Čekija	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Danija	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Vokietija	Streng geheim	Geheim	VS ([2]) – Vertraulich	VS – Nur für den Dienstgebrauch
Estija	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Airija	Top Secret	Secret	Confidential	Restricted
Graikija	Άκρως Απόρρητο Trumpinys: ΑΑΠ	Απόρρητο Trumpinys: (ΑΠ)	Εμπιστευτικό Trumpinys: (ΕΜ)	Περιορισμένης Χρήσης Trumpinys: (ΠΧ)
Ispanija	Secreto	Reservado	Confidencial	Difusión Limitada
Prancūzija	Très Secret Défense	Secret Défense	Confidentiel Défense	([3]) pastaba
Kroatija	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Italija	Segretissimo	Segreto	Riservatissimo	Riservato
Kipras	Άκρως Απόρρητο Trumpinys: (ΑΑΠ)	Απόρρητο Trumpinys: (ΑΠ)	Εμπιστευτικό Trumpinys: (ΕΜ)	Περιορισμένης Χρήσης Trumpinys: (ΠΧ)

Latvija	Sevišķi slepeni	Slepeni	Konfidenciāli	Visiškai slaptai
Lietuva	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Liuksemburgas	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Vengrija	„Szigorúan titkos!“	„Titkos!“	„Bizalmas!“	„Korlátozott terjesztésű!“
Malta	L-Ogħla Segretezza	Sigriet	Kunfidenzjali	Ristrett
Nyderlandai	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Austrija	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Lenkija	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugalija	Muito Secreto	Secreto	Confidencial	Reservado
Rumunija	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu
Slovėnija	Strogo tajno	Tajno	Zaupno	Interno
Slovakija	Prísne tajné	Tajné	Dôverné	Vyhradené
Suomija	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Švedija ([4])	HEMLIG/TOP SECRET HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG/SECRET HEMLIG	HEMLIG/CONFIDENTIAL HEMLIG	HEMLIG/RESTRICTED HEMLIG
Jungtinė Karalystė	UK TOP SECRET	UK SECRET	Atitikmens nėra ([5])	UK OFFICIAL – SENSITIVE

(1) „Diffusion Restreinte/Beperkte Verspreiding“ Belgijoje nėra slaptumo žyma. Žyma RESTREINT UE/ES RESTRICTED pažymėtą informaciją Belgija tvarko ir saugo taip pat griežtai, kaip taikant nustatytus Europos Sąjungos Tarybos saugumo taisyklėse aprašytus standartus ir procedūras.

(2) Vokietijoje: VS = *Verschlusssache*.

(3) Prancūzijos nacionalinėje sistemoje slaptumo žyma RESTREINT nenaudojama. Žyma RESTREINT UE/ES RESTRICTED pažymėtą informaciją Prancūzija tvarko ir saugo taip pat griežtai, kaip taikant nustatytus Europos Sąjungos Tarybos saugumo taisyklėse aprašytus standartus ir procedūras.

(4) Švedija: viršutinėje eilutėje nurodytas slaptumo žymas naudoja gynybos institucijos, o nurodytas apatinėje eilutėje – kitos institucijos.

(5) Žyma CONFIDENTIEL UE/ES CONFIDENTIAL pažymėtą ESĮI Jungtinė Karalystė tvarko ir saugo laikydamasi žyma UK SECRET pažymėtai informacijai taikomų saugumo reikalavimų.

II PRIEDAS

SANTRUMPŲ SĄRAŠAS

Santrumpa	Reikšmė
KI	Kriptografijos institucija
KPI	Kriptografijos patvirtinimo institucija
AVSS	Apsauginė vaizdo stebėjimo sistema
KPLI	Kriptografijos platinimo institucija
RIS	Ryšių ir informacinės sistemos, kuriose tvarkoma ESĮI
PSI	Paskirtoji saugumo institucija
ESĮI	ES įslaptinta informacija
ĮPPP	Įmonės patikimumą patvirtinantis pažymėjimas
ISU	Informacijos saugumo užtikrinimas
ISUI	Informacijos saugumo užtikrinimo institucija
ĮAS	Įsibrovimo aptikimo sistema
IT	Informacinės technologijos
VSP	Vietos saugumo pareigūnas
NSI	Nacionalinė saugumo institucija
APP	Asmens patikimumo pažymėjimas
APPPP	Asmens patikimumo pažymėjimą patvirtinanti pažyma
PRSI	Programos / projekto saugumo instrukcijos
RKP	Registracijos kontrolės pareigūnas
SAI	Saugumo akreditavimo institucija
SAP	Saugumo aspektų paaiškinimas
SŽV	Slaptumo žymų vadovas
SEK	Saugios eksploatacijos taisyklės
TEI	Institucija TEMPEST
SESV	Sutartis dėl ES veikimo

III PRIEDAS

NACIONALINIŲ SAUGUMO INSTITUCIJŲ SĄRAŠAS

BELGIJA

Autorité nationale de Sécurité
SPF Affaires étrangères, Commerce extérieur et Coopération au Développement
15, rue des Petits Carmes
1000 Bruxelles
Sekretoriato tel. +32 25014542
Faks. +32 25014596
El. p. nvo-ans@diplobel.fed.be

BULGARIJA

State Commission on Information Security
90 Cherkovna Str.
1505 Sofia
Tel. +359 29333600
Faks. +359 29873750
El. p. dksi@government.bg
Interneto svetainė www.dksi.bg

ČEKIJA

Národní bezpečnostní úřad
(National Security Authority)
Na Popelce 2/16
CZ-150 06 Praha 56
Tel. +420 257283335
Faks. +420 257283110
El. p. czech.nsa@nbu.cz
Interneto svetainė www.nbu.cz

DANIJA

Politiets Efterretningstjeneste
(Danish Security Intelligence Service)
Klausdalsbrovej 1
DK-2860 Søborg
Tel. +45 33148888
Faks. +45 33430190

Forsvarets Efterretningstjeneste
(Danish Defence Intelligence Service)
Kastellet 30
DK-2100 Copenhagen Ø
Tel. +45 33325566
Faks. +45 33931320

VOKIETIJA

Bundesministerium des Innern
Referat ÖS III 3
Alt-Moabit 101 D
11014 Berlin
Tel. +49 30186810
Faks. +49 30186811441
El. p. oesIII3@bmi.bund.de

ESTIJA

National Security Authority Department
Estonian Ministry of Defence
Sakala 1
EE-15094 Tallinn
Tel.: +372 7170019, +372 7170117
Faks. +372 7170213
El. p. nsa@mod.gov.ee

GRAIKIJA

Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)

Διακλαδική Διεύθυνση Στρατιωτικών Πληροφοριών (ΔΔΣΠ)

Διεύθυνση Ασφαλείας και Αντιπληροφοριών

ΣΤΓ 1020 -Χολαργός (Αθήνα)

Ελλάδα

Tel.: + 30/210/657 20 45 (darbo valandomis)

+ 30/210/657 20 09 (darbo valandomis)

Faks.: +30 2106536279; + 30 2106577612

Hellenic National Defence General Staff (HNDGS)

Military Intelligence Sectoral Directorate

Security Counterintelligence Directorate

GR-STG 1020 Holargos – Athens

Tel.: +30 2106572045, + 30 2106572009

Faks.: +30 2106536279, +30 2106577612

ISPANIJA

Autoridad Nacional de Seguridad

Oficina Nacional de Seguridad

Avenida Padre Huidobro s/n

E-28023 Madrid

Tel. +34 913725000

Faks. +34 913725808

El. p. nsa-sp@areatec.com

PRANCŪZIJA

Secrétariat général de la défense et de la sécurité nationale

Sous-direction Protection du secret (SGDSN/PSD)

51 Boulevard de la Tour-Maubourg

F-75700 Paris 07 SP

Tel. +33 171758177

Faks. +33 171758200

KROATIJA

Office of the National Security Council
Croatian NSA
Jurjevska 34
10000 Zagrebas
Kroatija
Tel. +385 14681222
Faks. + 385 14686049
Interneto svetainė www.uvns.hr

AIRIJA

National Security Authority
Department of Foreign Affairs
76–78 Harcourt Street
Dublin 2
Tel. +353 14780822
Faks. +353 14082959

ITALIJA

Presidenza del Consiglio dei Ministri
D.I.S. – U.C.Se.
Via di Santa Susanna, 15
IT-00187 Roma
Tel. +39 0661174266
Faks. +39 064885273

KIPRAS

ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ
ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Υπουργείο Άμυνας
Λεωφόρος Εμμανουήλ Ροΐδη 4
1432 Λευκωσία, Κύπρος

Tel.: +357 22807569, +357 22807643,

+357 22807764

Faks. +357 22302351

Ministry of Defence

Minister's Military Staff

National Security Authority (NSA)

4 Emanuel Roidi street

1432 Nicosia

Tel.: +357 22807569, +357 22807643,

+357 22807764

Faks. +357 22302351

El. p. cynsa@mod.gov.cy

LATVIJA

National Security Authority

Constitution Protection Bureau of the Republic of Latvia

P.O.Box 286

LV-1001 Ryga

Tel. +371 67025418

Faks. +371 67025454

El. p. ndi@sab.gov.lv

LIETUVA

Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija

(Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija – Nacionalinė saugumo institucija)

Gedimino pr. 40/1

LT-01110 Vilnius

Tel.: +370 70666701, +370 70666702

Faks. +370 70666700

El. p. nsa@vsd.lt

LIUKSEMBURGAS

Autorité nationale de Sécurité
Boîte postale 2379
1023 Luxembourg
Tel.: + 352/2478 22 10 (centrinis),
+ 352 24782253 (tiesioginis)
Faks. +352 24782243

VENGRIJA

Nemzeti Biztonsági Felügyelet
(Vengrijos nacionalinė saugumo institucija)
H-1024 Budapest, Szilágyi Erzsébet fasor 11/B
Tel. +36 (1) 7952303
Faks. +36 (1) 7950344
Pašto adresas:
H-1357 Budapest, PO Box 2
El. p. nbf@nbf.hu
Interneto svetainė www.nbf.hu

MALTA

Ministry for Home Affairs and National Security
P.O. Box 146
MT-Valletta
Tel. +356 21249844
Faks. +356 25695321

NYDERLANDAI

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20010
NL-2500 EA Den Haag
Tel. +31 703204400
Faks. +31 703200733

Ministerie van Defensie

Beveiligingsautoriteit
Postbus 20701
NL-2500 ES Den Haag
Tel. +31 703187060
Faks. +31 703187522

AUSTRIJA

Informationssicherheitskommission
Bundeskanzleramt
Ballhausplatz 2
AT-1014 Wien
Tel. +43 1531152594
Faks. +43 1531152615
El. p. ISK@bka.gv.at

LENKIJA

Agencja Bezpieczeństwa Wewnętrznego – ABW
(Vidaus saugumo agentūra)
2A Rakowiecka St.
00–993 Warszawa
Tel. +48 22 58 57 944
Faks. +48 22 58 57 443
El. p. nsa@abw.gov.pl
Interneto svetainė www.abw.gov.pl

PORTUGALIJA

Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Rua da Junqueira, 69
1300–342 Lisboa
Tel. +351 213031710
Faks. +351 213031711

RUMUNIJA

Oficiul Registrului Național al Informațiilor Secrete de Stat
(Rumunijos NSI – ORNISS Nacionalinis įslaptintos informacijos registro biuras)
4 Mures Street
012275 Bucharest
Tel. +40 212245830
Faks. +40 212240714
El. p. nsa.romania@nsa.ro
Interneto svetainė www.orniss.ro

SLOVĖNIJA

Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
1000 Ljubljana
Tel. +386 14781390
Faks. +386 14781399
El. p. gp.uvtp@gov.si

SLOVAKIJA

Národný bezpečnostný úrad
(Nacionalinė saugumo institucija)
Budatínska 30
P.O. Box 16
850 07 Bratislava
Tel. +421 268692314
Faks. +421 263824005
Interneto svetainė www.nbusr.sk

SUOMIJA

National Security Authority
Ministry for Foreign Affairs
P.O. Box 453
FI-00023 Government
Tel. 16055890
Faks. +358 916055140
El. p. NSA@formin.fi

ŠVEDIJA

Utrikesdepartementet
(Užsienio reikalų ministerija)
SSSB
S-103 39 Stockholm
Tel. +46 84051000
Faks. +46 87231176
El. p. ud-nsa@foreign.ministry.se

JUNGTINĖ KARALYSTĖ

UK National Security Authority
Room 335, 3rd Floor
70 Whitehall
London
SW1A 2AS
1 tel. +44 2072765649
2 tel. +44 2072765497
Faks. +44 2072765651
El. p. UK-NSA@cabinet-office.x.gsi.gov.uk

2.12. COMMISSION DECISION (EU, EURATOM) 2015/444 OF 13 MARCH 2015 ON THE SECURITY RULES FOR PROTECTING EU CLASSIFIED INFORMATION

COMMISSION DECISION (EU, Euratom) 2015/444

of 13 March 2015

on the security rules for protecting EU classified information

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 249 thereof,

Having regard to the Treaty establishing the European Atomic Energy Community, and in particular Article 106 thereof,

Having regard to the Protocol No 7 on the Privileges and Immunities of the European Union annexed to the Treaties, and in particular Article 18 thereof,

Whereas:

(1) The Commission's security provisions regarding the protection of European Union Classified Information (EUCI) need to be reviewed and updated, taking into account institutional, organisational, operational and technological developments.

(2) The European Commission has entered into instruments on security matters for its principal sites with the governments of Belgium, Luxembourg and Italy ([1]).

(3) The Commission, the Council and the European External Action Service are committed to applying equivalent security standards for protecting EUCI.

(4) It is important that, where appropriate, the European Parliament and other Union institutions, agencies, bodies or offices, are associated with the principles, standards and rules for protecting classified information which are necessary in order to protect the interests of the Union and its Member States.

(5) Risk to EUCI shall be managed as a process. This process shall be aimed at determining known security risks, defining security measures to reduce such risks to an acceptable level in accordance with the basic principles and minimum standards set out in this Decision and at applying these measures in line with the concept of defence in depth. The effectiveness of such measures shall be continuously evaluated.

(6) Within the Commission, physical security aimed at protecting classified information is the application of physical and technical protective measures intended to prevent unauthorised access to EUCI.

(7) The management of EUCI is the application of administrative measures for controlling EUCI throughout its life-cycle to supplement the measures provided for in Chapters 2, 3 and 5 of this Decision and thereby help deter, detect and recover from deliberate or accidental compromise or loss of such information. Such measures relate in particular to the creation, storage, registration, copying, translation, downgrading, declassification, carriage and destruction of EUCI and they supplement the general rules on document management of the Commission (Decisions 2002/47/EC ([2]), ECSC, Euratom and 2004/563/EC, Euratom ([3])).

(8) The provision of this Decision shall be without prejudice to:

(a) Regulation (Euratom) No 3 ([4]);

(b) Regulation (EC) No 1049/2001 of the European Parliament and of the Council ([5]);

(c) Regulation (EC) No 45/2001 of the European Parliament and of the Council ([6]);

(d) Council Regulation (EEC, Euratom) No 354/83 ([7]),

HAS ADOPTED THIS DECISION:

CHAPTER 1

BASIC PRINCIPLES AND MINIMUM STANDARDS

Article 1

Definitions

For the purpose of this Decision, the following definitions shall apply:

(1) **'Commission department'** means any Commission Directorate-General or service, or any Cabinet of a Member of the Commission;
(2) **'cryptographic (Crypto) material'** means cryptographic algorithms, cryptographic hardware and software modules, and products including implementation details and associated documentation and keying material;
(3) **'declassification'** means the removal of any security classification;
(4) **'defence in depth'** means the application of a range of security measures organised as multiple layers of defence;
(5) **'document'** means any recorded information regardless of its physical form or characteristics;
(6) **'downgrading'** means a reduction in the level of security classification;
(7) **'handling'** of EUCI means all possible actions to which EUCI may be subject throughout its life-cycle. It comprises its creation, registration, processing, carriage, downgrading, declassification and destruction. In relation to Communication and Information Systems (CIS) it also comprises its collection, display, transmission and storage;
(8) **'holder'** means a duly authorised individual with an established need-to-know who is in possession of an item of EUCI and is accordingly responsible for protecting it;
(9) **'implementing rules'** means any set of rules or security notices adopted in accordance with Chapter 5 of Commission Decision (EU, Euratom) 2015/443 ([8]);
(10) **'material'** means any medium, data carrier or item of machinery or equipment, either manufactured or in the process of manufacture;

(11) **'originator'** means the Union institution, agency or body, Member State, third state or international organisation under whose authority classified information has been created and/or introduced into the Union's structures;

(12) **'premises'** means any immovable or assimilated property and possessions of the Commission;

(13) **'security risk management process'** means the entire process of identifying, controlling and minimising uncertain events that may affect the security of an organisation or of any of the systems it uses. It covers the entirety of risk-related activities, including assessment, treatment, acceptance and communication;

(14) **'Staff Regulations'** means the Staff Regulations of officials of the European Union and the Conditions of Employment of other servants of the European Union, as laid down by Regulation (EEC, Euratom, ECSC) No 259/68 of the Council ([9]);

(15) **'threat'** means a potential cause of an unwanted incident which may result in harm to an organisation or any of the systems it uses; such threats may be accidental or deliberate (malicious) and are characterised by threatening elements, potential targets and attack methods;

(16) **'vulnerability'** means a weakness of any nature that can be exploited by one or more threats. A vulnerability may be an omission or it may relate to a weakness in controls in terms of their strength, completeness or consistency and may be of a technical, procedural, physical, organisational or operational nature.

Article 2

Subject matter and scope

1. This Decision lays down the basic principles and minimum standards of security for protecting EUCI.

2. This Decision shall apply to all Commission departments and in all premises of the Commission.

3. Notwithstanding any specific indications concerning particular groups of staff, this Decision shall apply to the Members of the Commission, to Commission staff under the scope of the Staff Regulations and of the Conditions of Employment of other servants of the European Communities to national experts seconded to the Commission (SNEs), to service providers and their staff, to trainees and to any individual

with access to Commission buildings or other assets, or to information handled by the Commission.

4. The provisions of this Decision shall be without prejudice to Decision 2002/47/EC, ECSC, Euratom and Decision 2004/563/EC, Euratom.

Article 3

Definition of EUCI, security classifications and markings

1. 'European Union classified information' (EUCI) means any information or material designated by an EU security classification, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States.

2. EUCI shall be classified at one of the following levels:

(a) **TRES SECRET UE/EU TOP SECRET**: information and material the unauthorised disclosure of which could cause exceptionally grave prejudice to the essential interests of the European Union or of one or more of the Member States;

(b) **SECRET UE/EU SECRET**: information and material the unauthorised disclosure of which could seriously harm the essential interests of the European Union or of one or more of the Member States;

(c) **CONFIDENTIEL UE/EU CONFIDENTIAL**: information and material the unauthorised disclosure of which could harm the essential interests of the European Union or of one or more of the Member States;

(d) **RESTREINT UE/EU RESTRICTED**: information and material the unauthorised disclosure of which could be disadvantageous to the interests of the European Union or of one or more of the Member States.

3. EUCI shall bear a security classification marking in accordance with paragraph 2. It may bear additional markings, which are not classification markings, but are intended to designate the field of activity to which it relates, identify the originator, limit distribution, restrict use or indicate releasability.

Article 4

Classification management

1. Each Member of the Commission or Commission department shall ensure that EUCI it creates, is appropriately classified, clearly identified as EUCI and retains its classification level for only as long as necessary.

2. Without prejudice to Article 26 below, EUCI shall not be downgraded or declassified nor shall any of the security classification markings referred to in Article 3(2) be modified or removed without the prior written consent of the originator.

3. Where appropriate, implementing rules on handling EUCI, including a practical classification guide, shall be adopted in accordance with Article 60 below.

Article 5

Protection of classified information

1. EUCI shall be protected in accordance with this Decision and its implementing rules.

2. The holder of any item of EUCI shall be responsible for protecting it, in accordance with this Decision and its implementing rules, according to the rules laid out in Chapter 4 below.

3. Where Member States introduce classified information bearing a national security classification marking into the structures or networks of the Commission, the Commission shall protect that information in accordance with the requirements applicable to EUCI at the equivalent level, as set out in the table of equivalence of security classifications contained in Annex I.

4. An aggregate of EUCI may warrant a level of protection corresponding to a higher classification than that of its individual components.

Article 6

Security risk management

1. Security measures for protecting EUCI throughout its life-cycle shall be commensurate in particular with its security classification, the form and the volume of the information or material, the location and construction of facilities housing EUCI and the locally assessed threat of malicious and/or criminal activities, including espionage, sabotage and terrorism.

2. Contingency plans shall take account of the need to protect EUCI during emergency situations in order to prevent unauthorised access, disclosure or loss of integrity or availability.

3. Preventive and recovery measures to minimise the impact of major failures or incidents on the handling and storage of EUCI shall be included in all services' business continuity plans.

Article 7

Implementation of this Decision

1. Where necessary, implementing rules to supplement or support this Decision shall be adopted in accordance with Article 60 below.

2. The Commission departments shall take all necessary measures falling under their responsibility in order to ensure that, when handling or storing EUCI or any other classified information, this Decision and the relevant implementing rules are applied.

3. The security measures taken in implementation of this Decision shall be compliant with the principles for security in the Commission laid down in Article 3 of Decision (EU, Euratom) 2015/443.

4. The Director-General for Human Resources and Security shall set up the Commission Security Authority within the Directorate-General for Human Resources and Security. The Commission Security Authority shall have the responsibilities assigned to it by this Decision and its implementing rules.

5. Within each Commission department, the Local Security Officer (LSO), as referred to in Article 20 of Decision (EU, Euratom) 2015/443, shall have the following overall responsibilities for protecting EUCI in

accordance with this Decision, in close cooperation with the Directorate-General for Human Resources and Security:

(a) managing requests for security authorisations for staff;
(b) contributing to security training and awareness briefings;
(c) supervising the department's Registry Control Officer (RCO);
(d) reporting on breaches of security and compromise of EUCI;
(e) holding spare keys and a written record of each combination setting;
(f) assuming other tasks related to the protection of EUCI or defined by implementing rules.

Article 8

Breaches of security and compromise of EUCI

1. A breach of security occurs as the result of an act or omission by an individual which is contrary to the security rules laid down in this Decision and its implementing rules.

2. Compromise of EUCI occurs when, as a result of a breach of security, it has wholly or in part been disclosed to unauthorised persons.

3. Any breach or suspected breach of security shall be reported immediately to the Commission Security Authority.

4. Where it is known or where there are reasonable grounds to assume that EUCI has been compromised or lost, a security inquiry shall be conducted in accordance with Article 13 of Decision (EU, Euratom) 2015/443.

5. All appropriate measures shall be taken to:

(a) inform the originator;
(b) ensure that the case is investigated by personnel not immediately concerned with the breach in order to establish the facts;
(c) assess the potential damage caused to the interests of the Union or of the Member States;
(d) take appropriate measures to prevent a recurrence; and
(e) notify the appropriate authorities of the action taken.

6. Any individual who is responsible for a breach of the security rules laid down in this Decision may be liable to disciplinary action in accordance with the Staff regulations. Any individual who is responsible for compromising or losing EUCI shall be liable to disciplinary and/or legal action in accordance with the applicable laws, rules and regulations.

CHAPTER 2

PERSONNEL SECURITY

Article 9

Definitions

For the purpose of this Chapter, the following definitions apply:

(1) 'authorisation for access to EUCI' means a decision by the Commission Security Authority taken on the basis of an assurance given by a competent authority of a Member State that a Commission official, other servant or seconded national expert may, provided his 'need-to-know' has been determined and he has been appropriately briefed on his responsibilities, be granted access to EUCI up to a specified level (CONFIDENTIEL UE/EU CONFIDENTIAL or above) until a specified date; the individual thus described is said to be 'security authorised'.

(2) 'personnel security authorisation' is the application of measures to ensure that access to EUCI is granted only to individuals who have:

(a) a need-to-know;

(b) been security authorised to the relevant level, where appropriate; and

(c) been briefed on their responsibilities.

(3) 'Personnel Security Clearance' (PSC) means a statement by a competent authority of a Member State which is made following completion of a security investigation conducted by the competent authorities of a Member State and which certifies that an individual may, provided his 'need-to-know' has been determined and he has been appropriately briefed on his responsibilities, be granted access to EUCI up to a specified level (CONFIDENTIEL UE/EU CONFIDENTIAL or above) until a specified date;

(4) 'Personnel Security Clearance Certificate' (PSCC) means a certificate issued by a competent authority establishing that an individual holds a valid security clearance or a security authorisation issued by the Commission Security Authority and which shows the level of EUCI to which that individual may be granted access (CONFIDENTIEL UE/EU CONFIDENTIAL or above), the period of validity of the relevant security clearance or authorisation and the date of expiry of the certificate itself.

(5) 'security investigation' means the investigative procedures conducted by the competent authority of a Member State in accordance with its national laws and regulations in order to obtain an assurance that nothing adverse is known which would prevent an individual from being granted a security clearance up to a specified level (CONFIDENTIEL UE/EU CONFIDENTIAL or above).

Article 10

Basic Principles

1. An individual shall only be granted access to EUCI after

(1) his need-to-know has been determined;

(2) he has been briefed on the security rules for protecting EUCI and the relevant security standards and guidelines, and has acknowledged his responsibilities with regard to protecting such information;

(3) for information classified CONFIDENTIEL UE/EU CONFIDENTIAL and above, he has been security authorised to the relevant level or is otherwise duly authorised by virtue of his functions in accordance with national laws and regulations.

2. All individuals whose duties may require them to have access to EUCI classified CONFIDENTIEL UE/EU CONFIDENTIAL or above shall be security authorised to the relevant level before being granted access to such EUCI. The individual concerned shall consent in writing to being submitted to the personnel security clearance procedure. Failure to do so shall mean that the individual cannot be assigned to a post, function or task which involves access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above.

3. Personnel security clearance procedures shall be designed to determine whether an individual, taking into account his loyalty, trustworthiness and reliability, may be authorised to access EUCI.

4. The loyalty, trustworthiness and reliability of an individual for the purposes of being security cleared for access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above shall be determined by means of a security investigation conducted by the competent authorities of a Member State in accordance with its national laws and regulations.

5. The Commission Security Authority shall be solely responsible for liaising with the national security authorities ('NSAs') or other competent national authorities in the context of all security clearance issues. All contacts between Commission services and their staff and the NSAs and other competent authorities shall be conducted through the Commission Security Authority.

Article 11

Security authorisation procedure

1. Each Director-General or head of service within the Commission shall identify the positions within his department for which the holders need to access information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above to perform their duties and so need to be security authorised.

2. As soon as it is known that an individual will be appointed to a position requiring access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above, the LSO of the Commission department concerned shall inform the Commission Security Authority, which shall transmit to the individual the security clearance questionnaire issued by the NSA of the Member State under whose nationality the individual has been appointed as a staff member of the European institutions. The individual shall consent in writing to being submitted to the security clearance procedure and return the completed questionnaire within the shortest deadline to the Commission Security Authority.

3. The Commission Security Authority shall forward the completed security clearance questionnaire to the NSA of the Member State under whose nationality the individual has been appointed as a staff member of the European institutions, requesting that a security investigation be undertaken for the level of EUCI to which the individual will require access.

4. Where information relevant to a security investigation is known to the Commission Security Authority concerning an individual who has applied for a security clearance, the Commission Security Authority, acting in accordance with the relevant rules and regulations, shall notify the competent NSA thereof.

5. Following completion of the security investigation, and as soon as possible after having been notified by the relevant NSA of its overall assessment of the findings of the security investigation, the Commission Security Authority:

(a) may grant an authorisation for access to EUCI to the individual concerned and authorise access to EUCI up to the relevant level until a date specified by him but for a maximum of 5 years, where the security investigation results in an assurance that nothing adverse is known which would call into question the loyalty, trustworthiness and reliability of the individual;

(b) shall, where the security investigation does not result in such an assurance, in accordance with the relevant rules and regulations, notify the individual concerned, who may ask to be heard by the Commission Security Authority, who in turn may ask the competent NSA for any further clarification it can provide according to its national laws and regulations. If the outcome of the security investigation is confirmed, the authorisation for access to EUCI shall not be issued.

6. The security investigation together with the results obtained shall be subject to the relevant laws and regulations in force in the Member State concerned, including those concerning appeals. Decisions by the Commission Security Authority shall be subject to appeals in accordance with the Staff Regulations.

7. The Commission shall accept the authorisation for access to EUCI granted by any other Union institution, body or agency provided it remains valid. Authorisations shall cover any assignment by the individual concerned within the Commission. The Union institution, body or agency in which the individual is taking up employment will notify the relevant NSA of the change of employer.

8. If an individual's period of service does not commence within 12 months of the notification of the outcome of the security investigation to the Commission Security Authority, or if there is a break of 12 months in an individual's service, during which time he has not been employed

by the Commission or by any other Union Institution, body or agency, or in a position with a national administration of a Member State, the Commission Security Authority shall refer the matter to the relevant NSA for confirmation that the security clearance remains valid and appropriate.

9. Where information becomes known to the Commission Security Authority concerning a security risk posed by an individual who holds a valid security authorisation, the Security Authority, acting in accordance with the relevant rules and regulations, shall notify the competent NSA thereof.

10. Where an NSA notifies the Commission Security Authority of the withdrawal of an assurance given in accordance with paragraph 5(a) for an individual who holds a valid authorisation for access to EUCI, the Commission Security Authority may ask for any clarification the NSA can provide according to its national laws and regulations. If the adverse information is confirmed by the relevant NSA, the security authorisation shall be withdrawn and the individual shall be excluded from access to EUCI and from positions where such access is possible or where he might endanger security.

11. Any decision to withdraw or suspend an authorisation for access to EUCI from any individual falling under the scope of this Decision, and, where appropriate, the reasons for doing so, shall be notified to the individual concerned, who may ask to be heard by the Commission Security Authority. Information provided by an NSA shall be subject to the relevant laws and regulations in force in the Member State concerned. Decisions made in this context by the Commission Security Authority shall be subject to appeals in accordance with the Staff Regulations.

12. Commission departments shall make sure that national experts seconded to them for a position requiring security authorisation to access EUCI shall present, prior to taking up their assignment, a valid PSC or Personnel Security Clearance Certificate ('PSCC'), according to national law and regulations, to the Commission Security Authority, who, on the basis thereof, will grant a security authorisation for access to EUCI up to the level equivalent to the one referred to in the national security clearance, with a maximum validity for the duration of their assignment.

13. The Members of the Commission, who have access to EUCI by virtue of their functions on the basis of the Treaty, shall be briefed on

their security obligations in respect of protecting EUCI.

14. Records of security clearances and authorisations granted for access to EUCI shall be maintained by the Commission Security Authority in accordance with this Decision. These records shall contain as a minimum the level of EUCI to which the individual may be granted access, the date of issue of the security clearance and its period of validity.

15. The Commission Security Authority may issue a PSCC showing the level of EUCI to which the individual may be granted access (CONFIDENTIEL UE/EU CONFIDENTIAL or above), the date of validity of the relevant authorisation for access to EUCI and the date of expiry of the certificate itself.

16. After the initial granting of security authorisations and provided that the individual has had uninterrupted service with the European Commission or another Union Institution, body or agency and has a continuing need for access to EUCI, the security authorisation for access to EUCI shall be reviewed for renewal, as a general rule, every five years from the date of notification of the outcome of the last security investigation on which it was based.

17. The Commission Security Authority may extend the validity of the existing security authorisation for a period of up to 12 months, if no adverse information has been received from the relevant NSA or other competent national authority within a period of two months from the date of transmission of the request for renewal and the corresponding security clearance questionnaire. If, at the end of this 12-month period, the relevant NSA or other competent national authority has not notified the Commission Security Authority of its opinion, the individual shall be assigned to duties which do not require a security authorisation.

Article 12

Security authorisation briefings

1. After having participated in the security authorisation briefing organised by the Commission Security Authority, all individuals who have been security authorised shall acknowledge in writing that they have understood their obligations in respect of protecting EUCI and the consequences if EUCI is compromised. A record of such a

written acknowledgement shall be kept by the Commission Security Authority.

2. All individuals who are authorised to have access to, or required to handle EUCI, shall initially be made aware, and periodically briefed on the threats to security and must report immediately to the Commission Security Authority any approach or activity that they consider suspicious or unusual.

3. All individuals who cease to be employed in duties requiring access to EUCI shall be made aware of, and where appropriate acknowledge in writing, their obligations in respect of the continued protection of EUCI.

Article 13

Temporary security authorisations

1. In exceptional circumstances, where duly justified in the interests of the service and pending completion of a full security investigation, the Commission Security Authority, may, after consulting the NSA of the Member State of which the individual is a national and subject to the outcome of preliminary checks to verify that no relevant adverse information is known, grant a temporary authorisation for individuals to access EUCI for a specific function, without prejudice to the provisions regarding renewal of security clearances. Such temporary authorisations for access to EUCI shall be valid for a single period not exceeding six months and shall not permit access to information classified TRES SECRET UE/EU TOP SECRET.

2. After having been briefed in accordance with Article 12(1), all individuals who have been granted a temporary authorisation shall acknowledge in writing that they have understood their obligations in respect of protecting EUCI and the consequences if EUCI is compromised. A record of such a written acknowledgement shall be kept by the Commission Security Authority.

Article 14

Attendance at classified meetings organised by the Commission

1. Commission departments responsible for organising meetings at which information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above is discussed shall, through their LSO or through the meeting organiser, inform the Commission Security Authority well in advance of the dates, times, venue and participants of such meetings.

2. Subject to the provisions of Article 11(13), individuals assigned to participate in meetings organised by the Commission at which information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above is discussed, may only do so upon confirmation of their security clearance or security authorisation status. Access to such classified meetings shall be denied to individuals for whom the Commission Security Authority has not seen a PSCC or other proof of security clearance, or, to participants of the Commission who are not in possession of a security authorisation.

3. Before organising a classified meeting, the responsible meeting organiser or the LSO of the Commission department organising the meeting, shall request external participants to provide the Commission Security Authority a PSCC or other proof of security clearance. The Commission Security Authority shall inform the LSO or the meeting organiser of PSCC or other proof of PSC received. Where applicable, a consolidated list of names may be used, giving the relevant proof of security clearance.

4. Where the Commission Security Authority is informed by the competent authorities that a PSC has been withdrawn from an individual whose duties require attendance at meetings organised by the Commission, the Commission Security Authority shall notify the LSO of the Commission department responsible for organising the meeting.

Article 15

Potential Access to EUCI

Couriers, guards and escorts shall be security authorised to the appropriate level or otherwise appropriately investigated in accordance with national laws and regulations, be briefed on security procedures for protecting EUCI and be instructed on their duties for protecting such information entrusted to them.

CHAPTER 3

PHYSICAL SECURITY AIMED AT PROTECTING CLASSIFIED INFORMATION

Article 16

Basic principles

1. Physical security measures shall be designed to deny surreptitious or forced entry by an intruder, to deter, impede and detect unauthorised actions and to allow for segregation of personnel in their access to EUCI on a need-to-know basis. Such measures shall be determined based on a risk management process, in accordance with this Decision and its implementing rules.

2. In particular, physical security measures shall be designed to prevent unauthorised access to EUCI by:

(a) ensuring that EUCI is handled and stored in an appropriate manner;
(b) allowing for segregation of personnel in terms of access to EUCI on the basis of their need-to-know and, where appropriate, their security authorisation;
(c) deterring, impeding and detecting unauthorised actions; and
(d) denying or delaying surreptitious or forced entry by intruders.

3. Physical security measures shall be put in place for all premises, buildings, offices, rooms and other areas in which EUCI is handled or stored, including areas housing communication and information systems as referred to in Chapter 5.

4. Areas in which EUCI classified CONFIDENTIEL UE/EU CONFIDENTIAL or above is stored shall be established as Secured Areas in accordance with this Chapter and accredited by the Commission Security Accreditation Authority.

5. Only equipment or devices approved by the Commission Security Authority shall be used for protecting EUCI at the level CONFIDENTIEL UE/EU CONFIDENTIAL or above.

Article 17

Physical security requirements and measures

1. Physical security measures shall be selected on the basis of a threat assessment made by the Commission Security Authority, where appropriate in consultation with other Commission departments, other Union institutions, agencies or bodies and/or competent authorities in the Member States. The Commission shall apply a risk management process for protecting EUCI on its premises to ensure that a commensurate level of physical protection is afforded against the assessed risk. The risk management process shall take account of all relevant factors, in particular:

(a) the classification level of EUCI;

(b) the form and volume of EUCI, bearing in mind that large quantities or a compilation of EUCI may require more stringent protective measures to be applied;

(c) the surrounding environment and structure of the buildings or areas housing EUCI; and

(d) the assessed threat from intelligence services which target the Union, its institutions, bodies or agencies, or the Member States and from sabotage, terrorist, subversive or other criminal activities.

2. The Commission Security Authority, applying the concept of defence in depth, shall determine the appropriate combination of physical security measures to be implemented. To that effect, the Commission Security Authority shall develop minimum standards, norms and criteria, set out in implementing rules.

3. The Commission Security Authority is authorised to conduct entry and exit searches to act as a deterrent to the unauthorised introduction of material or the unauthorised removal of EUCI from premises or buildings.

4. When EUCI is at risk of being overlooked, even accidentally, the Commission departments concerned shall take the appropriate measures, as defined by the Commission Security Authority, to counter this risk.

5. For new facilities, physical security requirements and their functional specifications shall be defined in consent with the Commission Security Authority as part of the planning and design of the facilities. For existing facilities, physical security requirements shall be implemented in accordance with the minimum standards, norms and criteria set out in implementing rules.

Article 18

Equipment for the physical protection of EUCI

1. Two types of physically protected areas shall be established for the physical protection of EUCI:
(a) Administrative Areas; and
(b) Secured Areas (including technically Secured Areas).

2. The Commission Security Accreditation Authority shall establish that an area meets the requirements to be designated as an Administrative Area, a Secured Area or a technically Secured Area.

3. For Administrative Areas:
(a) a visibly defined perimeter shall be established which allows individuals and, where possible, vehicles to be checked;
(b) unescorted access shall be granted only to individuals who are duly authorised by the Commission Security Authority or any other competent authority; and
(c) all other individuals shall be escorted at all times or be subject to equivalent controls.

4. For Secured Areas:
(a) a visibly defined and protected perimeter shall be established through which all entry and exit is controlled by means of a pass or personal recognition system;
(b) unescorted access shall be granted only to individuals who are security-cleared and specifically authorised to enter the area on the basis of their need-to-know;
(c) all other individuals shall be escorted at all times or be subject to equivalent controls.

5. Where entry into a Secured Area constitutes, for all practical purposes, direct access to the classified information contained in it, the following additional requirements shall apply:
(a) the level of highest security classification of the information normally held in the area shall be clearly indicated;
(b) all visitors shall require specific authorisation to enter the area, shall be escorted at all times and shall be appropriately security cleared unless steps are taken to ensure that no access to EUCI is possible.

6. Secured Areas protected against eavesdropping shall be designated technically Secured Areas. The following additional requirements shall apply:

(a) such areas shall be equipped with an Intrusion Detection System ('IDS'), be locked when not occupied and be guarded when occupied. Any keys shall be managed in accordance with Article 20;
(b) all persons and material entering such areas shall be controlled;
(c) such areas shall be regularly physically and/or technically inspected by the Commission Security Authority. Such inspections shall also be conducted following any unauthorised entry or suspicion of such entry; and
(d) such areas shall be free of unauthorised communication lines, unauthorised telephones or other unauthorised communication devices and electrical or electronic equipment.

7. Notwithstanding point (d) of paragraph 6, before being used in areas where meetings are held or work is being performed involving information classified SECRET UE/EU SECRET and above, and where the threat to EUCI is assessed as high, any communications devices and electrical or electronic equipment shall first be examined by the Commission Security Authority to ensure that no intelligible information can be inadvertently or illicitly transmitted by such equipment beyond the perimeter of the Secured Area.

8. Secured Areas which are not occupied by duty personnel on a 24-hour basis shall, where appropriate, be inspected at the end of normal working hours and at random intervals outside normal working hours, unless an IDS is in place.

9. Secured Areas and technically Secured Areas may be set up temporarily within an Administrative Area for a classified meeting or any other similar purpose.

10. The LSO of the Commission department concerned shall draw up Security Operating Procedures (SecOPs) for each Secured Area under his responsibility stipulating, in accordance with the provisions of this Decision and its implementing rules:
(a) the level of EUCI which may be handled and stored in the area;
(b) the surveillance and protective measures to be maintained;
(c) the individuals authorised to have unescorted access to the area by virtue of their need-to-know and security authorisation;
(d) where appropriate, the procedures for escorts or for protecting EUCI when authorising any other individuals to access the area;
(e) any other relevant measures and procedures.

11. Strong rooms shall be constructed within Secured Areas. The

walls, floors, ceilings, windows and lockable doors shall be approved by the Commission Security Authority and afford protection equivalent to a security container approved for the storage of EUCI of the same classification level.

Article 19

Physical protective measures for handling and storing EUCI

1. EUCI which is classified RESTREINT UE/EU RESTRICTED may be handled:
(a) in a Secured Area,
(b) in an Administrative Area provided the EUCI is protected from access by unauthorised individuals, or
(c) outside a Secured Area or an Administrative Area provided the holder carries the EUCI in accordance with Article 31 and has undertaken to comply with compensatory measures, set out in implementing measures, to ensure that EUCI is protected from access by unauthorised persons.

2. EUCI which is classified RESTREINT UE/EU RESTRICTED shall be stored in suitable locked office furniture in an Administrative Area or a Secured Area. It may temporarily be stored outside an Administrative Area or a Secured Area provided the holder has undertaken to comply with compensatory measures laid down in implementing rules.

3. EUCI which is classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET may be handled:
(a) in a Secured Area;
(b) in an Administrative Area provided the EUCI is protected from access by unauthorised individuals; or
(c) outside a Secured Area or an Administrative Area provided the holder:

(i) has undertaken to comply with compensatory measures, set out in implementing rules, to ensure the EUCI is protected from access by unauthorised persons;

(ii) keeps the EUCI at all times under his personal control; and

(iii) in the case of documents in paper form, has notified the relevant registry of the fact.

4. EUCI which is classified CONFIDENTIEL UE/EU

CONFIDENTIAL and SECRET UE/EU SECRET shall be stored in a Secured Area in a security container or a strong room.

5. EUCI which is classified TRES SECRET UE/EU TOP SECRET shall be handled in a Secured Area, set up and maintained by the Commission Security Authority, and accredited to that level by the Commission Security Accreditation Authority.

6. EUCI which is classified TRES SECRET UE/EU TOP SECRET shall be stored in a Secured Area, accredited to that level by the Commission Security Accreditation Authority, under one of the following conditions:

(a) in a security container in accordance with the provisions of Article 18 with one or more of the following supplementary controls:

(1) continuous protection or verification by cleared security staff or duty personnel;

(2) an approved IDS in combination with security response personnel;

or

(b) in an IDS-equipped strong room in combination with security response personnel.

Article 20

Management of keys and combinations used for protecting EUCI

1. Procedures for managing keys and combination settings for offices, rooms, strong rooms and security containers shall be laid down in implementing rules according to Article 60 below. Such procedures shall be intended to guard against unauthorised access.

2. Combination settings shall be committed to memory by the smallest possible number of individuals needing to know them. Combination settings for security containers and strong rooms storing EUCI shall be changed:

(a) on receipt of a new container;
(b) whenever there is a change in personnel knowing the combination;
(c) whenever a compromise has occurred or is suspected;
(d) when a lock has undergone maintenance or repair; and
(e) at least every 12 months.

CHAPTER 4

MANAGEMENT OF EU CLASSIFIED INFORMATION

Article 21

Basic principles

1. All EUCI documents should be managed in compliance with the Commission's policy on document management and consequently should be registered, filed, preserved and finally eliminated, sampled or transferred to the Historical Archives in accordance with the common Commission-level retention list for European Commission files.

2. Information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above shall be registered for security purposes prior to distribution and on receipt. Information classified TRES SECRET UE/EU TOP SECRET shall be registered in designated registries.

3. Within the Commission, a EUCI registry system shall be set up in accordance with the provisions of Article 27.

4. Commission departments and premises where EUCI is handled or stored shall be subject to regular inspection by the Commission Security Authority.

5. EUCI shall be conveyed between services and premises outside physically protected areas as follows:

(a) as a general rule, EUCI shall be transmitted by electronic means protected by cryptographic products approved in accordance with Chapter 5;

(b) when the means referred to in point (a) are not used, EUCI shall be carried either:

(i) on electronic media (e.g. USB sticks, CDs, hard drives) protected by cryptographic products approved in accordance with Chapter 5; or

(ii) in all other cases, as prescribed in implementing rules.

Article 22

Classifications and markings

1. Information shall be classified where it requires protection with regard to its confidentiality, in accordance with Article 3(1).

2. The originator of EUCI shall be responsible for determining the security classification level, in accordance with the relevant implementing rules, standards and guidelines regarding classification, and for the initial dissemination of the information.

3. The classification level of EUCI shall be determined in accordance with Article 3(2) and with the relevant implementing rules.

4. The security classification shall be clearly and correctly indicated, regardless of whether the EUCI is on paper, oral, electronic or in any other form.

5. Individual parts of a given document (i.e. pages, paragraphs, sections, annexes, appendices, attachments and enclosures) may require different classifications and be marked accordingly, including when stored in electronic form.

6. The overall classification level of a document or file shall be at least as high as that of its most highly classified component. When information from various sources is collated, the final product shall be reviewed to determine its overall security classification level, since it may warrant a higher classification than its component parts.

7. To the extent possible, documents containing parts with different classification levels shall be structured so that parts with a different classification level may be easily identified and detached if necessary.

8. The classification of a letter or note covering enclosures shall be as high as the highest classification of its enclosures. The originator shall indicate clearly at which level it is classified when detached from its enclosures by means of an appropriate marking, e.g.:

CONFIDENTIEL UE/EU CONFIDENTIAL
Without attachment(s) RESTREINT UE/EU RESTRICTED

Article 23

Markings

In addition to one of the security classification markings set out in Article 3(2), EUCI may bear additional markings, such as:

(a) an identifier to designate the originator;
(b) any caveats, code-words or acronyms specifying the field of activity to which the document relates, a particular distribution on a need-to-know basis or restrictions on use;
(c) releasability markings;
(d) where applicable, the date or specific event after which it may be downgraded or declassified.

Article 24

Abbreviated classification markings

1. Standardised abbreviated classification markings may be used to indicate the classification level of individual paragraphs of a text. Abbreviations shall not replace the full classification markings.

2. The following standard abbreviations may be used within EU classified documents to indicate the classification level of sections or blocks of text of less than a single page:

TRES SECRET UE/EU TOP SECRET	TS-UE/EU-TS
SECRET UE/EU SECRET	S-UE/EU-S
CONFIDENTIEL UE/EU CONFIDENTIAL	C-UE/EU-C
RESTREINT UE/EU RESTRICTED	R-UE/EU-R

Article 25

Creation of EUCI

1. When creating an EU classified document:
(a) each page shall be marked clearly with the classification level;
(b) each page shall be numbered;
(c) the document shall bear a registration number and a subject, which is not itself classified information, unless it is marked as such;
(d) the document shall be dated;
(e) documents classified SECRET UE/EU SECRET or above shall bear a copy number on every page, if they are to be distributed in several copies.

2. Where it is not possible to apply paragraph 1 to EUCI, other appropriate measures shall be taken in accordance with implementing rules.

Article 26

Downgrading and declassification of EUCI

1. At the time of its creation, the originator shall indicate, where possible, whether EUCI can be downgraded or declassified on a given date or following a specific event.

2. Each Commission department shall regularly review EUCI for which it is the originator to ascertain whether the classification level still applies. A system to review the classification level of registered EUCI which has originated in the Commission no less frequently than every five years shall be established by implementing rules. Such a review shall not be necessary where the originator has indicated from the outset that the information will automatically be downgraded or declassified and the information has been marked accordingly.

3. Information classified RESTREINT UE/EU RESTRICTED having originated in the Commission will be considered to be automatically declassified after thirty years, in accordance with Regulation (EEC, Euratom) No 354/83 as amended by Council Regulation (EC, Euratom) No 1700/2003 ([10]).

Article 27

EUCI registry system in the Commission

1. Without prejudice to Article 52 paragraph 5 below, in each Commission department in which EUCI is handled or stored at the level of CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET, a responsible local EUCI registry shall be identified to ensure that EUCI is handled in accordance with this Decision.

2. The EUCI registry managed by the Secretariat-General shall be the Commission's Central EUCI Registry. It shall act as:

- the Local EUCI Registry for the Commission's Secretariat-General,
- the EUCI registry for the private offices of Members of the Commission, unless these have a designated local EUCI registry,
- the EUCI registry for Directorates-General or services which do not have a local EUCI registry,

– the main point of entry and exit for all information classified RESTREINT UE/EU RESTRICTED and up to including SECRET UE/EU SECRET exchanged between the Commission and its services and third States and international organisations, and, when provided for in specific arrangements, for other Union institutions, agencies and bodies.

3. Within the Commission, a registry shall be designated by the Commission Security Authority to act as the central receiving and dispatching authority for information classified TRES SECRET UE/EU TOP SECRET. Where necessary, subordinate registries may be designated to handle that information for registration purposes.

4. The subordinate registries may not transmit TRES SECRET UE/EU TOP SECRET documents directly to other subordinate registries of the same central TRES SECRET UE/EU TOP SECRET registry or externally without the express written approval of the latter.

5. EUCI registries shall be established as Secured Areas as defined in Chapter 3, and accredited by the Commission's Security Accreditation Authority (SAA).

Article 28

Registry control officer

1. Each EUCI registry shall be managed by a Registry Control Officer ('RCO').

2. The RCO shall be appropriately security-cleared.

3. The RCO shall be subject to the supervision of the LSO within the Commission department, as far as the application of the provisions regarding the handling of EUCI documents and compliance with the relevant security rules, standards and guidelines is concerned.

4. Within his responsibility for managing the EUCI Registry to which he has been assigned, the RCO shall assume the following overall tasks in accordance with this Decision and the relevant implementing rules, standards and guidelines:

– manage operations relating to the registration, preservation, reproduction, translation, transmission, dispatch and destruction or transfer to the historical archives service of EUCI,

– verify periodically the need to maintain the classification of information,
– assume any other tasks related to the protection of EUCI defined in implementing rules.

Article 29

Registration of EUCI for security purposes

1. For the purposes of this Decision, registration for security purposes (hereinafter referred to as 'registration') means the application of procedures which record the life-cycle of EUCI, including its dissemination.

2. All information or material classified CONFIDENTIEL UE/EU CONFIDENTIAL and above shall be registered in designated registries when it is received in or dispatched from an organisational entity.

3. When EUCI is handled or stored using a Communication and Information System (CIS), registration procedures may be performed by processes within the CIS itself.

4. More detailed provisions concerning the registration of EUCI for security purposes shall be laid down in implementing rules.

Article 30

Copying and translating EU classified documents

1. TRES SECRET UE/EU TOP SECRET documents shall not be copied or translated without the prior written consent of the originator.

2. Where the originator of documents classified SECRET UE/EU SECRET and below has not imposed caveats on their copying or translation, such documents may be copied or translated on instruction from the holder.

3. The security measures applicable to the original document shall apply to copies and translations thereof.

Article 31

Carriage of EUCI

1. EUCI shall be carried in such a way as to protect it from unauthorised disclosure during its carriage.

2. Carriage of EUCI shall be subject to the protective measures, which shall:

– be commensurate with the level of classification of the EUCI carried, and
– be adapted to the specific conditions of its carriage, in particular depending on whether EUCI is carried:

  – within a Commission building or a self-contained group of Commission buildings,

  – between Commission buildings located in the same Member State,

  – within the Union,

  – from within the Union to the territory of a third State, and

  – be adapted to the nature and form of the EUCI.

3. These protective measures shall be laid down in detail in implementing rules, or, in case of projects and programmes referred to in Article 42, as an integral part of the relevant Programme or Project Security Instructions (PSI).

4. The implementing rules or PSI shall include provisions commensurate with the level of EUCI, regarding:

– the type of carriage, such as hand carriage, carriage by diplomatic or military courier, carriage by postal services or commercial courier services,
– packaging of EUCI,
– technical countermeasures for EUCI carried on electronic media,
– any other procedural, physical or electronic measure,
– registration procedures,
– use of security authorised personnel.

5. When EUCI is carried on electronic media, and notwithstanding Article 21, paragraph 5, the protective measures set out in the relevant implementing rules may be supplemented by appropriate technical countermeasures approved by the Commission Security Authority so as to minimise the risk of loss or compromise.

Article 32

Destruction of EUCI

1. EU classified documents which are no longer required may be destroyed, taking account of regulations on archives and of the Commission's rules and regulations on document management and archiving, and in particular with the Common Commission-Level Retention List.

2. EUCI of the level of CONFIDENTIEL UE/EU CONFIDENTIAL and above shall be destroyed by the RCO of the responsible EUCI registry on instruction from the holder or from a competent authority. The RCO shall update the logbooks and other registration information accordingly.

3. For documents classified SECRET UE/EU SECRET or TRES SECRET UE/EU TOP SECRET, such destruction shall be performed by the RCO in the presence of a witness who shall be cleared to at least the classification level of the document being destroyed.

4. The registrar and the witness, where the presence of the latter is required, shall sign a destruction certificate, which shall be filed in the registry. The RCO of the responsible EUCI registry shall keep destruction certificates of TRES SECRET UE/EU TOP SECRET documents for a period of at least 10 years and for documents classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET for a period of at least five years.

5. Classified documents, including those classified RESTREINT UE/EU RESTRICTED, shall be destroyed by methods which shall be defined in implementing rules and which shall meet relevant EU or equivalent standards.

6. Computer storage media used for EUCI shall be destroyed in accordance with procedures laid down in implementing rules.

Article 33

Destruction of EUCI in emergencies

1. Commission departments holding EUCI shall prepare plans based on local conditions for the safeguarding of EU classified material in a crisis including if necessary emergency destruction and evacuation

plans. They shall promulgate instructions deemed necessary to prevent EUCI from falling into unauthorised hands.

2. The arrangements for the safeguarding and/or destruction of CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET material in a crisis shall under no circumstances adversely affect the safeguarding or destruction of TRES SECRET UE/EU TOP SECRET material, including the enciphering equipment, whose treatment shall take priority over all other tasks.

3. In the event of an emergency, if there is an imminent risk of unauthorised disclosure, EUCI shall be destroyed by the holder in such a way that it cannot be reconstructed in whole or in part. The originator and originating registry shall be informed of the emergency destruction of registered EUCI.

4. More detailed provisions for destruction of EUCI shall be laid down in implementing rules.

CHAPTER 5

PROTECTION OF EU CLASSIFIED INFORMATION IN COMMUNICATION AND INFORMATION SYSTEMS (CIS)

Article 34

Basic principles of Information Assurance

1. Information Assurance (IA) in the field of communication and information systems is the confidence that such systems will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users.

2. Effective Information Assurance shall ensure appropriate levels of:

Authenticity	:	the guarantee that information is genuine and from *bona fide* sources;
Availability	:	the property of being accessible and usable upon request by an authorised entity;

Confidentiality	:	the property that information is not disclosed to unauthorised individuals, entities or processes;
Integrity	:	the property of safeguarding the accuracy and completeness of assets and information;
Non-repudiation	:	the ability to prove an action or event has taken place, so that this event or action cannot subsequently be denied.

3. IA shall be based on a risk management process.

Article 35

Definitions

For the purpose of this Chapter, the following definitions apply:

(a) 'Accreditation' means the formal authorisation and approval granted to a communication and information system by the Security Accreditation Authority (SAA) to process EUCI in its operational environment, following the formal validation of the Security Plan and its correct implementation;

(b) 'Accreditation Process' means the necessary steps and tasks required prior to the accreditation by the Security Accreditation Authority. These steps and tasks shall be specified in an Accreditation Process Standard;

(c) 'Communication and Information System' (CIS) means any system enabling the handling of information in electronic form. A communication and information system shall comprise the entire assets required for it to operate, including the infrastructure, organisation, personnel and information resources;

(d) 'Residual risk' means the risk which remains after security measures have been implemented, given that not all threats are countered and not all vulnerabilities can be eliminated;

(e) 'Risk' means the potential that a given threat will exploit internal and external vulnerabilities of an organisation or of any of the systems it uses and thereby cause harm to the organisation and to its tangible or intangible assets. It is measured as a combination of the likelihood of threats occurring and their impact;

(f) 'Risk acceptance' is the decision to agree to the further existence of a residual risk after risk treatment;

(g) 'Risk assessment' consists of identifying threats and vulnerabilities and conducting the related risk analysis, i.e. the analysis of probability and impact;
(h) 'Risk communication' consists of developing awareness of risks among CIS user communities, informing approval authorities of such risks and reporting them to operating authorities;
(i) 'Risk treatment' consists of mitigating, removing, reducing (through an appropriate combination of technical, physical, organisational or procedural measures), transferring or monitoring the risk.

Article 36

CIS handling EUCI

1. CIS shall handle EUCI in accordance with the concept of IA.

2. For CIS handling EUCI, compliance with the Commission's information systems security policy, as referred to in Commission Decision C(2006)3602 ([11]), implies that:
(a) the Plan-Do-Check-Act approach shall be applied for the implementation of the information systems security policy during the full life-cycle of the information system;
(b) the security needs must be identified through a business impact assessment;
(c) the information system and the data therein must undergo a formal asset classification;
(d) all mandatory security measures as determined by the policy on security of information systems must be implemented;
(e) a risk management process must be applied, consisting of the following steps: threat and vulnerability identification, risk assessment, risk treatment, risk acceptance and risk communication;
(f) a security plan, including the Security Policy and the Security Operating Procedures, is defined, implemented, checked and reviewed.

3. All staff involved in the design, development, testing, operation, management or usage of CIS handling EUCI shall notify to the SAA all potential security weaknesses, incidents, breaches of security or compromise which may have an impact on the protection of the CIS and/or the EUCI therein.

4. Where the protection of EUCI is provided by cryptographic products, such products shall be approved as follows:

(a) preference shall be given to products which have been approved by the Council or by the Secretary-General of the Council in its function as crypto approval authority of the Council, upon recommendation of the Commission Security Expert Group;

(b) where warranted on specific operational grounds, the Commission Crypto Approval Authority (CAA) may, upon recommendation of the Commission Security Expert Group, waive the requirements referred to under a) and grant an interim approval for a specific period.

5. During transmission, processing and storage of EUCI by electronic means, approved cryptographic products shall be used. Notwithstanding this requirement, specific procedures may be applied under emergency circumstances or in specific technical configurations after approval by the CAA.

6. Security measures shall be implemented to protect CIS handling information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above against compromise of such information through unintentional electromagnetic emanations ('TEMPEST security measures'). Such security measures shall be commensurate with the risk of exploitation and the level of classification of the information.

7. The Commission Security Authority shall assume the following functions:

- IA Authority (IAA),
- Security Accreditation Authority (SAA),
- TEMPEST Authority (TA),
- Crypto Approval Authority (CAA),
- Crypto Distribution Authority (CDA).

8. The Commission Security Authority shall appoint for each system the IA Operational Authority.

9. The responsibilities of the functions described in paragraphs 7 and 8 will be defined in the implementing rules.

Article 37

Accreditation of CIS handling EUCI

1. All CIS handling EUCI shall undergo an accreditation process, based upon the principles of IA, whose level of detail must be commensurate with the level of protection required.

2. The accreditation process shall include the formal validation by the Commission SAA of the Security Plan for the CIS concerned in order to obtain assurance that:

(a) the risk management process, as referenced in Article 36(2), has been properly carried out;
(b) the System Owner has knowingly accepted the residual risk; and
(c) a sufficient level of protection of the CIS, and of the EUCI handled in it, has been achieved in accordance with this decision.

3. The Commission's SAA shall issue an accreditation statement which determines the maximum classification level of the EUCI that may be handled in the CIS as well as the corresponding terms and conditions for operation. This is without prejudice to the tasks entrusted to the Security Accreditation Board defined in Article 11 of Regulation (EU) No 512/2014 of the European Parliament and of the Council ([12]).

4. A joint Security Accreditation Board (SAB) shall be responsible for accrediting Commission's CIS involving several parties. It shall be composed of a SAA representative of each party involved and be chaired by an SAA representative of the Commission.

5. The accreditation process shall consist of a series of tasks to be assumed by the parties involved. The responsibility for the preparation of the accreditation files and documentation shall rest entirely upon the CIS System Owner.

6. The accreditation shall be the responsibility of the Commission SAA, who, at any moment in the life cycle of the CIS, shall have the right to:

(a) require that an accreditation process be applied;
(b) audit or inspect the CIS;
(c) where conditions for operation are no any longer satisfied, require the definition and effective implementation of a security improvement plan within a well-defined timescale, potentially withdrawing permission to operate the CIS until conditions for operation are again satisfied.

7. The accreditation process shall be established in a standard on the accreditation process for CIS handling EUCI, which shall be adopted in accordance with Article 10(3) of Decision C(2006) 3602.

Article 38

Emergency circumstances

1. Notwithstanding the provisions of this Chapter, the specific procedures described below may be applied in an emergency, such as during impending or actual crisis, conflict, war situations or in exceptional operational circumstances.

2. EUCI may be transmitted using cryptographic products which have been approved for a lower classification level or without encryption with the consent of the competent authority if any delay would cause harm clearly outweighing the harm entailed by any disclosure of the classified material and if:

(a) the sender and recipient do not have the required encryption facility; and

(b) the classified material cannot be conveyed in time by other means.

3. Classified information transmitted under the circumstances set out in paragraph 1 shall not bear any markings or indications distinguishing it from information which is unclassified or which can be protected by an available cryptographic product. Recipients shall be notified of the classification level, without delay, by other means.

4. A subsequent report shall be made to the competent authority and to the Commission Security Expert Group.

CHAPTER 6

INDUSTRIAL SECURITY

Article 39

Basic principles

1. Industrial security is the application of measures to ensure the protection of EUCI

(a) within the framework of classified contracts, by:

(i) candidates or tenderers throughout the tendering and contracting procedure;

(ii) contractors or subcontractors throughout the life-cycle of classified contracts;

(b) within the framework of classified grant agreements, by

(i) applicants during grant award procedures;

(ii) beneficiaries throughout the life-cycle of classified grant agreements.

2. Such contracts or grant agreements shall not involve information classified TRES SECRET UE/EU TOP SECRET.

3. Unless stated otherwise, provisions in this Chapter referring to classified contracts or contractors shall be applicable also to classified subcontracts or subcontractors.

Article 40

Definitions

For the purpose of this Chapter, the following definitions shall apply:

(a) 'Classified contract' means a framework contract or contract, as referred to in Council Regulation (EC, Euratom) No 1605/2002 ([13]), entered into by the Commission or one of its departments, with a contractor for the supply of movable or immovable assets, the execution of works or the provision of services, the performance of which requires or involves the creation, handling or storing of EUCI;

(b) 'Classified subcontract' means a contract entered into by a contractor of the Commission or one of its departments, with another contractor (i.e. the subcontractor) for the supply of movable or immovable assets, the execution of works or the provision of services, the performance of which requires or involves the creation, handling or storing of EUCI;

(c) 'Classified grant agreement' means an agreement whereby the Commission awards a grant, as referred to in Part I, Title VI, of Regulation (EC, Euratom) No 1605/2002, the performance of which requires or involves the creation, handling or storing of EUCI;

(d) 'Designated Security Authority' (DSA) means an authority responsible to the National Security Authority (NSA) of a Member State which is responsible for communicating to industrial or other entities national policy on all matters of industrial security and for providing direction and assistance in its implementation. The function of DSA may be carried out by the NSA or by any other competent authority.

Article 41

Procedure for classified contracts or grant agreements

1. Each Commission department, as contracting authority, shall ensure that the minimum standards on industrial security set out in this Chapter, are referred to or incorporated in the contract, and complied with when awarding classified contracts or grant agreements.

2. For the purposes of paragraph 1, the competent services within the Commission shall seek the advice of the Directorate-General for Human Resources and Security, and in particular its Security Directorate, and shall ensure that model contracts and subcontracts and model grant agreements include provisions reflecting the basic principles and minimum standards for protecting EUCI to be complied with by contractors and subcontractors, and respectively beneficiaries of grant agreements.

3. The Commission shall closely cooperate with the NSA, the DSA or any other competent authority of the Member States concerned.

4. When a contracting authority, intends to launch a procedure aimed at concluding a classified contract or grant agreement, it shall seek the advice of the Commission Security Authority on issues regarding the classified nature and elements of the procedure, during all its stages.

5. Templates for and models of classified contracts and subcontracts, classified grant agreements, contract notices, guidance on the circumstances where Facility Security Clearances (FSCs) are required, Programme or Project Security Instructions (PSI), Security Aspects Letters (SALs), visits, transmission and carriage of EUCI under classified contracts or classified grant agreements shall be laid down in implementing rules on industrial security, after consulting the Commission Security Expert Group.

6. The Commission may conclude classified contracts or grant agreements which entrust tasks involving or entailing access to or the handling or storage of EUCI by economic operators registered in a Member State or in a third State with which an agreement or an administrative arrangement has been concluded in accordance with Chapter 7 of this Decision.

Article 42

Security elements in a classified contract or grant agreement

1. Classified contracts or grant agreements shall include the following security elements:

Programme or Project Security Instructions

(a) 'Programme or Project Security Instruction' (PSI) means a list of security procedures which are applied to a specific programme or project in order to standardise security procedures. It may be revised throughout the programme or project.
(b) The Directorate-General Human Resources and Security shall develop a generic PSI, the Commission departments responsible for programmes or projects involving handling or storage of EUCI may develop, where appropriate, specific PSIs, which shall be based upon the generic PSI.
(c) A specific PSI shall be developed in particular for programmes and projects characterised by their considerable scope, scale or complexity, or by the multitude and/or the diversity of contractors, beneficiaries and other partners and stakeholders involved, for instance as regards their legal status. The specific PSI shall be developed by the Commission department(s) managing the programme or project, in close cooperation with the Directorate-General Human Resources and Security.
(d) The Directorate-General Human Resources and Security shall submit both the generic and specific PSIs for advice to the Commission Security Expert Group.

Security Aspects Letter

(a) 'Security Aspects Letter' (SAL) means a set of special contractual conditions, issued by the contracting authority, which forms an integral part of any classified contract involving access to or the creation of EUCI, that identifies the security requirements and those elements of the contract requiring security protection.

(b) The contract-specific security requirements shall be described in a SAL. The SAL shall, where appropriate, contain the Security Classification Guide ('SCG') and shall be an integral part of a classified contract or sub-contract, or grant agreement.

(c) The SAL shall contain the provisions requiring the contractor or beneficiary to comply with the minimum standards laid down in this Decision. The contracting authority shall ensure the SAL indicates that non-compliance with these minimum standards may constitute sufficient grounds for the contract or the grant agreement to be terminated.

2. Both PSIs and SALs shall include a SCG as a mandatory security element:

(a) 'Security Classification Guide' (SCG) means a document which describes the elements of a programme, project, contract or grant agreement which are classified, specifying the applicable security classification levels. The SCG may be expanded throughout the life of the programme, project, contract or grant agreement and the elements of information may be re-classified or downgraded; where an SCG exists it shall be part of the SAL.

(b) Prior to launching a call for tender or letting a classified contract, the Commission department, as contracting authority, shall determine the security classification of any information to be provided to candidates and tenderers or contractors, as well as the security classification of any information to be created by the contractor. For that purpose, it shall prepare an SCG to be used for the performance of the contract, in accordance with this Decision and its implementing rules, after consulting the Commission Security Authority.

(c) In order to determine the security classification of the various elements of a classified contract, the following principles shall apply:

(i) in preparing an SCG, the Commission department, as the contracting authority, shall take into account all relevant security aspects, including the security classification assigned to information provided and approved to be used for the contract by the originator of the information;

(ii) the overall level of classification of the contract may not be lower than the highest classification of any of its elements; and

(iii) where relevant, the contracting authority shall liaise, through the Commission Security Authority, with the Member States' NSAs, DSAs or any other competent security authority concerned in the event of any changes regarding the classification of information created by or provided to contractors in the performance of a contract and when making any subsequent changes to the SCG.

Article 43

Access to EUCI for contractors' and beneficiaries' staff

The contracting or granting authority, shall ensure that the classified contract or classified grant agreement includes provisions indicating that staff of a contractor, subcontractor or beneficiary who, for the performance of the classified contract, subcontract or grant agreement, require access to EUCI, shall be granted such access only if:

(a) he has been security authorised to the relevant level or is otherwise duly authorised by their need-to-know has been determined;

(b) they have been briefed on the applicable security rules for protecting EUCI, and have acknowledged their responsibilities with regard to protecting such information;

(c) they have been security cleared at the relevant level for information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET by the respective NSA, DSA or any other competent authority.

Article 44

Facility security clearance

1. 'Facility Security Clearance' (FSC) means an administrative determination by a NSA, DSA or any other competent security authority that, from the security viewpoint, a facility can afford an adequate level of protection to EUCI to a specified security classification level.

2. A FSC granted by the NSA or DSA or any other competent security authority of a Member State to indicate, in accordance with national laws and regulations, that an economic operator can protect EUCI at the appropriate classification level (CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET) within its facilities, shall be presented to the Commission Security Authority, which will forward it to the Commission department acting as the contracting or granting authority, before a candidate, tenderer or contractor, or grant applicant or beneficiary may be provided with or granted access to EUCI.

3. Where relevant, the contracting authority shall notify, through the Commission Security Authority, the appropriate NSA, DSA or any other competent security authority that an FSC is required for performing the contract. A FSC or PSC shall be required where EUCI classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET has to be provided in the course of the procurement or grant award procedure.

4. The contracting or granting authority shall not award a classified contract or a grant agreement to a preferred bidder or participant before having received confirmation from the NSA, DSA or any other competent security authority of the Member State in which the contractor or subcontractor concerned is registered that, where required, an appropriate FSC has been issued.

5. When the Commission Security Authority has been notified by the NSA, DSA or any other competent security authority which has issued a FSC about changes affecting the FSC, it shall inform the Commission department, acting as contracting or granting authority. In the case of a sub-contract, the NSA, DSA or any other competent security authority shall be informed accordingly.

6. Withdrawal of a FSC by the relevant NSA, DSA or any other competent security authority shall constitute sufficient grounds for

the contracting or granting authority, to terminate a classified contract or exclude a candidate, tenderer or applicant from the competition. A provision to that effect shall be included in the model contracts and grant agreements to be developed.

Article 45

Provisions for classified contracts and grant agreements

1. Where EUCI is provided to a candidate, tenderer or applicant during the procurement procedure, the call for tender or call for proposal shall contain a provision obliging the candidate, tenderer or applicant failing to submit a tender or proposal or who is not selected, to return all classified documents within a specified period of time.

2. The contracting or granting authority, shall notify, through the Commission Security Authority, the competent NSA, DSA or any other competent security authority of the fact that a classified contract or grant agreement has been awarded, and of the relevant data, such as the name of the contractor(s) or beneficiaries, the duration of the contract and the maximum level of classification.

3. When such contracts or grant agreements are terminated, the contracting or granting authority, shall promptly notify, through the Commission Security Authority, the NSA, DSA or any other competent security authority of the Member State in which the contractor or grant beneficiary is registered.

4. As a general rule, the contractor or grant beneficiary shall be required to return to the contracting or granting authority, upon termination of the classified contract or the grant agreement, or of the participation of a grant beneficiary, any EUCI held by it.

5. Specific provisions for the disposal of EUCI during the performance of the classified contract or the classified grant agreement or upon its termination shall be laid down in the SAL.

6. Where the contractor or grant beneficiary is authorised to retain EUCI after termination of a classified contract or grant agreement, the minimum standards contained in this Decision shall continue to be complied with and the confidentiality of EUCI shall be protected by the contractor or the grant beneficiary.

Article 46

Specific provisions for classified contracts

1. The conditions relevant for the protection of EUCI under which the contractor may subcontract shall be defined in the call for tender and in the classified contract.

2. A contractor shall obtain permission from the contracting authority, before sub-contracting any parts of a classified contract. No subcontract involving access to EUCI may be awarded to subcontractors registered in a third country, unless there is a regulatory framework for the security of information as provided for in Chapter 7.

3. The contractor shall be responsible for ensuring that all sub-contracting activities are undertaken in accordance with the minimum standards laid down in this Decision and shall not provide EUCI to a subcontractor without the prior written consent of the contracting authority.

4. With regard to EUCI created or handled by the contractor, the Commission shall be considered to be the originator, and the rights incumbent on the originator shall be exercised by the contracting authority.

Article 47

Visits in connection with classified contracts

1. Where a Commission staff member or contractors' or grant beneficiaries' personnel require access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET in each other's premises for the performance of a classified contract or grant agreement, visits shall be arranged in liaison with the NSAs, DSAs or any other competent security authority concerned. The Commission Security Authority shall be informed of such visits. However, in the context of specific programmes or projects, the NSAs, DSAs or any other competent security authority may also agree on a procedure whereby such visits can be arranged directly.

2. All visitors shall hold an appropriate security clearance and have a 'need-to-know' for access to the EUCI related to the classified contract.

3. Visitors shall be given access only to EUCI related to the purpose of the visit.

4. More detailed provisions shall be set out in implementing rules.

5. Compliance with the provisions regarding visits in connection with classified contracts, set out in this Decision and in the implementing rules referred to in paragraph 4, shall be mandatory.

Article 48

Transmission and carriage of EUCI in connection with classified contracts or classified grant agreements

1. With regard to the transmission of EUCI by electronic means, the relevant provisions of Chapter 5 of this Decision shall apply.

2. With regard to the carriage of EUCI, the relevant provisions of Chapter 4 of this Decision and its implementing rules shall apply, in accordance with national laws and regulations.

3. For the transport of classified material as freight, the following principles shall be applied when determining security arrangements:

(a) security shall be assured at all stages during transportation from the point of origin to the final destination;

(b) the degree of protection afforded to a consignment shall be determined by the highest classification level of material contained within it;

(c) prior to any cross-border movement of material classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET, a transportation plan shall be drawn up by the consignor and approved by the NSA, DSA or any other competent security authority concerned;

(d) journeys shall be point to point to the extent possible, and shall be completed as quickly as circumstances permit;

(e) whenever possible, routes should be only through Member States. Routes through States other than Member States should only be undertaken when authorised by the NSA, DSA or any other competent security authority of the States of both the consignor and the consignee.

Article 49

Transfer of EUCI to contractors or grant beneficiaries located in third states

EUCI shall be transferred to contractors or grant beneficiaries located in third States in accordance with security measures agreed between the Commission Security Authority, the Commission department, as the contracting or granting authority, and the NSA, DSA or other competent security authority of the concerned third country where the contractor or grant beneficiary is registered.

Article 50

Handling of information classified RESTREINT UE/EU RESTRICTED in the context of classified contracts or classified grant agreements

1. Protection of information classified RESTREINT UE/EU RESTRICTED handled or stored under classified contracts or grant agreements shall be based on the principles of proportionality and cost-effectiveness.

2. No FSC or PSC shall be required in the context of classified contracts or classified grant agreements involving the handling of information classified at the level of RESTREINT UE/EU RESTRICTED.

3. Where a contract or grant agreement involves handling of information classified RESTREINT UE/EU RESTRICTED in a CIS operated by a contractor or grant beneficiary, the contracting or granting authority shall ensure, after consulting the Commission Security Authority, that the contract or grant agreement specifies the necessary technical and administrative requirements regarding accreditation or approval of the CIS commensurate with the assessed risk, taking account of all relevant factors. The scope of accreditation or approval of such CIS shall be agreed between the Commission Security Authority and the relevant NSA or DSA.

CHAPTER 7

EXCHANGE OF CLASSIFIED INFORMATION WITH OTHER UNION INSTITUTIONS, AGENCIES, BODIES AND OFFICES, WITH MEMBER STATES, AND WITH THIRD STATES AND INTERNATIONAL ORGANISATIONS

Article 51

Basic principles

1. Where the Commission or one of its departments determines that there is a need to exchange EUCI with another Union Institution, agency, body or office, or with a third State or international organisation, the necessary steps shall be undertaken to establish an appropriate legal or administrative framework to that effect, which may include security of information agreements or administrative arrangements concluded in accordance with the relevant regulations.

2. Without prejudice to Article 57, EUCI shall only be exchanged with another Union Institution, agency, body or office, or with a third State or international organisation, provided such an appropriate legal or administrative framework is in place, and that there are sufficient guarantees that the Union Institution, agency, body or office, or the third State or international organisation concerned applies equivalent basic principles and minimum standards for the protection of classified information.

Article 52

Exchange of EUCI with other Union institutions, agencies, bodies and offices

1. Before entering into an administrative arrangement for the exchange of EUCI with another Union Institution, agency, body or office, the Commission shall seek assurance that the Union Institution, agency, body or office concerned:

(a) has a regulatory framework for the protection of EUCI in place, which lays down basic principles and minimum standards equivalent to those laid down in this Decision and its implementing rules;
(b) applies security standards and guidelines regarding personnel security, physical security, management of EUCI and security of Communication and Information Systems (CIS), which guarantee an equivalent level of protection of EUCI as that afforded in the Commission;
(c) marks classified information which it creates, as EUCI.

2. The Directorate-General Human Resources and Security shall, in close cooperation with other competent Commission departments, be the lead service within the Commission for the conclusion of administrative arrangements for the exchange of EUCI with other Union institutions, agencies, bodies or offices.

3. Administrative arrangements shall as a general rule take the form of an Exchange of Letters, signed by the Director-General for Human Resources and Security on behalf of the Commission.

4. Before entering into an administrative arrangement on the exchange of EUCI, the Commission Security Authority shall conduct an assessment visit aimed at assessing the regulatory framework for protecting EUCI and ascertaining the effectiveness of measures implemented for protecting EUCI. The administrative arrangement shall enter into force, and EUCI shall be exchanged, only if the outcome of this assessment visit is satisfactory and the recommendations made further to the visit have been complied with. Regular follow-up assessment visits shall be conducted to verify that the administrative arrangement is complied with and the security measures in place continue to meet the basic principles and minimum standards agreed.

5. Within the Commission, the EUCI registry managed by the Secretariat General shall, as a general rule, be the main point of entry and exit for classified information exchanges with other Union institutions, agencies, bodies and offices. However, where on security, organisational or operational grounds it is more appropriate for protecting EUCI, local EUCI registries established within Commission departments in accordance with this Decision and its implementing rules, shall operate as the point of entry and exit for classified information regarding matters within the competence of the Commission departments concerned.

6. The Commission Security Expert Group shall be informed of the process of concluding administrative arrangements pursuant to paragraph 2.

Article 53

Exchange of EUCI with Member States

1. EUCI may be exchanged with and released to Member States provided that they protect that information in accordance with the requirements applicable to classified information bearing a national security classification at the equivalent level as set out in the table of equivalence of security classifications contained in Annex I.

2. Where Member States introduce classified information bearing a national security classification marking into the structures or networks of the European Union, the Commission shall protect that information in accordance with the requirements applicable to EUCI at the equivalent level as set out in the table of equivalence of security classifications contained in Annex I.

Article 54

Exchange of EUCI with third States and international organisations

1. Where the Commission determines that it has a long-term need to exchange classified information with third States or international organisations, the necessary steps shall be undertaken to establish an appropriate legal or administrative framework to that effect, which may include security of information agreements or administrative arrangements concluded in accordance with the relevant regulations.

2. Such security of information agreements and administrative agreements referred to in paragraph 1 shall contain provisions to ensure that when third States or international organisations receive EUCI, such information is given protection appropriate to its classification level and according to minimum standards which are equivalent to those laid down in this Decision.

3. The Commission may enter into administrative arrangements in accordance with Article 56 where the classification level of EUCI is as a general rule no higher than RESTREINT UE/EU RESTRICTED.

4. Administrative arrangements for the exchange of classified information referred to in paragraph 3 shall contain provisions to ensure that when third States or international organisations receive EUCI, such information is given protection appropriate to its classification level and according to minimum standards which are equivalent to those laid down in this Decision. The Commission Security Expert Group shall be consulted on the conclusion of security of information agreements or administrative arrangements.

5. The decision to release EUCI originating in the Commission to a third State or international organisation shall be taken by the Commission department, as originator of this EUCI within the Commission, on a case-by-case basis, according to the nature and content of such information, the recipient's need-to-know and the measure of advantage to the Union. If the originator of the classified information for which release is desired, or of the source material it may contain, is not the Commission, the Commission department which holds this classified information, shall first seek the originator's written consent to release. If the originator cannot be established, the Commission department, which holds this classified information, shall assume the former's responsibility after consulting the Commission Security Expert Group.

Article 55

Security of information agreements

1. Security of information agreements with third states or international organisations are concluded in accordance with Article 218 TFEU.

2. Security of information agreements shall:

(a) establish the basic principles and minimum standards governing the exchange of classified information between the Union and a third State or international organisation;

(b) provide for technical implementing arrangements to be agreed between the competent security authorities of the relevant Union institutions and bodies and the competent security authority of the third State or international organisation in question. Such arrangements shall take account of the level of protection provided by the security regulations, structures and procedures in place in the third State or international organisation concerned;

(c) provide that prior to the exchange of classified information under the agreement, it shall be ascertained that the receiving party is able to protect and safeguard classified information provided to it in an appropriate manner.

3. The Commission shall, when a need to exchange classified information is determined according to Article 51(1), consult the European External Action Service, the General Secretariat of the Council and other Union institutions and bodies, where appropriate, in order to determine whether a recommendation according to Article 218(3) TFEU should be submitted.

4. No EUCI shall be exchanged by electronic means unless explicitly provided for in the security of information agreement or technical implementing arrangements.

5. Within the Commission, the EUCI registry managed by the Secretariat-General shall, as a general rule, be the main point of entry and exit for classified information exchanges with third States and international organisations. However, where on security, organisational or operational grounds it is more appropriate for protecting EUCI, local EUCI registries established within Commission departments in accordance with this Decision and its implementing rules, shall operate as the point of entry and exit for classified information regarding matters within the competence of the Commission departments concerned.

6. In order to assess the effectiveness of the security regulations, structures and procedures in the third State or international organisation concerned, the Commission shall, in collaboration with other Union institutions, agencies or bodies, participate in assessment visits, in mutual agreement with the third State or international organisation concerned. Such assessment visits shall evaluate:

(a) the regulatory framework applicable for protecting classified information;
(b) any specific features of the security policy and the way in which security is organised in the third State or international organisation which may have an impact on the level of classified information that may be exchanged;
(c) the security measures and procedures actually in place; and
(d) security clearance procedures for the level of EUCI to be released.

Article 56

Administrative arrangements

1. Where a long-term need exists in the context of a Union political or legal framework to exchange information classified as a general rule no higher than RESTREINT UE/EU RESTRICTED with a third State or international organisation, and where the Commission Security Authority, after consulting the Commission Security Expert Group, has established, in particular, that the party in question does not have a sufficiently developed security system for it to be possible to enter into a security of information agreement, the Commission may decide to enter into an administrative arrangement with the relevant authorities of the third State or international organisation in question.

2. Such administrative arrangements shall as a general rule take the form of an Exchange of Letters.

3. An assessment visit shall be conducted prior to the conclusion of the arrangement. The Commission Security Expert Group shall be informed of the outcome of the assessment visit. Where there are exceptional reasons for exchanging classified information urgently, EUCI may be released provided every attempt is made to conduct an assessment visit as soon as possible.

4. No EUCI shall be exchanged by electronic means unless explicitly provided for in the administrative arrangement.

Article 57

Exceptional ad hoc release of EUCI

1. Where no security of information agreement or administrative arrangement is in place, and where the Commission or one of its departments determines that there is an exceptional need in the context of an Union political or legal framework to release EUCI to a third State or international organisation, the Commission Security Authority shall, to the extent possible, verify with the security authorities of the third State or international organisation concerned that its security regulations, structures and procedures are such that EUCI released to it will be protected to standards no less stringent than those laid down in this Decision.

2. The decision to release the EUCI to the third State or international organisation concerned, shall, after consultation of the Commission Security Expert Group, be taken by the Commission on the basis of a proposal by the member of the Commission responsible for security matters.

3. Following the Commission's decision to release EUCI and subject to prior written consent of originator, including the originators of source material it may contain, the competent Commission department shall forward the information concerned, which shall bear a releasability marking indicating the third State or international organisation to which it has been released. Prior to or upon actual release, the third party in question shall undertake in writing to protect the EUCI it receives in accordance with the basic principles and minimum standards set out in this Decision.

CHAPTER 8

FINAL PROVISIONS

Article 58

Replacement of previous decision

This Decision shall repeal and replace Commission Decision 2001/844/EC, ECSC, Euratom ([14]).

Article 59

Classified information created before the entry into force of this Decision

1. All EUCI classified in accordance with Decision 2001/844/EC, ECSC, Euratom shall continue to be protected in accordance with the relevant provisions of this Decision.

2. All classified information held by the Commission on the date that Decision 2001/844/EC, ECSC, Euratom entered into force, with the exception of Euratom classified information, shall:

(a) if created by the Commission, continue to be considered to have been reclassified RESTREINT UE by default, unless its author had decided to give it another classification by 31 January 2002 and had informed all addressees of the document concerned;

(b) if created by authors outside the Commission, retain its original classification and thus be treated as EUCI of the equivalent level, unless the author agrees to declassification or downgrading of the information.

Article 60

Implementing rules and security notices

1. As necessary, the adoption of the implementing rules for this decision will be the subject of a separate empowerment decision of the Commission in favour of the Member of the Commission responsible for security matters, in full compliance with the internal rules of procedure.

2. After being empowered following the above-mentioned Commission Decision, the Member of the Commission responsible for security matters may develop security notices setting out security guidelines and best practices within the scope of this Decision and its implementing rules.

3. The Commission may delegate the tasks mentioned in the first and second paragraph of this Article to the Director-General for Human Resources and Security by a separate delegation decision, in full compliance with the internal rules of procedure.

Article 61

Entry into force

This Decision shall enter into force on the day following that of its publication in the *Official Journal of the European Union*.

Done at Brussels, 13 March 2015.

For the Commission

The President

Jean-Claude JUNCKER

([1]) Cf. the 'Arrangement entre le Gouvernement belge et le Parlement européen, le Conseil, la Commission, le Comité économique et social européen, le Comité des régions, la Banque européenne d'investissement en matière de sécurité' of 31 December 2004, the 'Accord de sécurité signé entre la Commission et le Gouvernement luxembourgeois' of 20 January 2007, and the 'Accordo tra il Governo italiano e la Commissione europea dell'energia atomica (Euratom) per l'istituzione di un Centro comune di ricerche nucleari di competenza generale' of 22 July 1959.

([2]) Commission Decision 2002/47/EC, ECSC, Euratom of 23 January 2002 amending its rules of procedure (OJ L 21, 24.1.2002, p. 23).

([3]) Commission Decision 2004/563/EC, Euratom of 7 July 2004 amending its Rules of Procedure (OJ L 251, 27.7.2004, p. 9).

([4]) Regulation (Euratom) No 3 of 31 July 1958 implementing Article 24 of the Treaty establishing the European Atomic Energy Community (OJ 17, 6.10.1958, p. 406/58).

([5]) Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43).

([6]) Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).

([7]) Council Regulation (EEC, Euratom) No 354/83 of 1 February 1983 concerning the opening to the public of the historical archives of the European Economic Community and the European Atomic Energy Community (OJ L 43, 15.2.1983, p. 1).

([8]) Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission (See page 41 of this Official Journal).

([9]) Regulation (EEC, Euratom, ECSC) No 259/68 of the Council of 29 February 1968 laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Communities and instituting special measures temporarily applicable to officials of the Commission (Conditions of Employment of Other Servants) (OJ L 56, 4.3.1968, p. 1).

([10]) Council Regulation (EC, Euratom) No 1700/2003 of 22 September 2003 amending Regulation (EEC, Euratom) No 354/83 concerning the opening to the public of the historical archives of the European Economic Community and the European Atomic Energy Community (OJ L 243, 27.9.2003, p. 1).

([11]) C(2006) 3602 of 16 August 2006 concerning the security of information systems used by the European Commission.

([12]) Regulation (EU) No 512/2014 of the European Parliament and of the Council of 16 April 2014 amending Regulation (EU) No 912/2010 setting up the European GNSS Agency (OJ L 150, 20.5.2014, p. 72).

([13]) Council Regulation (EC, Euratom) No 1605/2002 of 25 June 2002 on the Financial Regulation applicable to the general budget of the European Communities (OJ L 248, 16.9.2002, p. 1).

([14]) Commission Decision 2001/844/EC,ECSC,Euratom of 29 November 2001 amending its internal Rules of Procedure (OJ L 317, 3.12.2001, p. 1).

ANNEX I

EQUIVALENCE OF SECURITY CLASSIFICATIONS

EU	TRES SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
EURATOM	EURA TOP SECRET	EURA SECRET	EURA CONFIDENTIAL	EURA RESTRICTED
Belgium	Très Secret (Loi 11.12.1998) Zeer Geheim (Wet 11.12.1998)	Secret (Loi 11.12.1998) Geheim (Wet 11.12.1998)	Confidentiel (Loi 11.12.1998) Vertrouwelijk (Wet 11.12.1998)	nota ([1]) below
Bulgaria	Строго секретно	Секретно	Поверително	За служебно ползване
Czech Republic	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Denmark	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Germany	Streng geheim	Geheim	VS ([2]) – Vertraulich	VS – Nur für den Dienstgebrauch
Estonia	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Ireland	Top Secret	Secret	Confidential	Restricted
Greece	Άκρως Απόρρητο Abr: ΑΑΠ	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Spain	Secreto	Reservado	Confidencial	Difusión Limitada
France	Très Secret Défense	Secret Défense	Confidentiel Défense	nota ([3]) below
Croatia	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Italy	Segretissimo	Segreto	Riservatissimo	Riservato
Cyprus	Άκρως Απόρρητο Abr: (ΑΑΠ)	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Latvia	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Lithuania	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Luxembourg	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Hungary	'Szigorúan titkos!'	'Titkos!'	'Bizalmas!'	'Korlátozott terjesztésű!'
Malta	L-Ogħla Segretezza	Sigriet	Kunfidenzjali	Ristrett

Netherlands	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Austria	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Poland	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugal	Muito Secreto	Secreto	Confidencial	Reservado
Romania	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu
Slovenia	Strogo tajno	Tajno	Zaupno	Interno
Slovakia	Prísne tajné	Tajné	Dôverné	Vyhradené
Finland	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Sweden ([4])	HEMLIG/TOP SECRET HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG/SECRET HEMLIG	HEMLIG/CONFIDENTIAL HEMLIG	HEMLIG/RESTRICTED HEMLIG
United Kingdom	UK TOP SECRET	UK SECRET	No equivalent ([5])	UK OFFICIAL – SENSITIVE

([1]) Diffusion Restreinte/Beperkte Verspreiding is not a security classification in Belgium. Belgium handles and protects 'RESTREINT UE/EU RESTRICTED' information in a manner no less stringent than the standards and procedures described in the security rules of the Council of the European Union.

([2]) Germany: VS = Verschlusssache.

([3]) France does not use the classification 'RESTREINT' in its national system. France handles and protects 'RESTREINT UE/EU RESTRICTED' information in a manner no less stringent than the standards and procedures described in the security rules of the Council of the European Union.

([4]) Sweden: the security classification markings in the top row are used by the defence authorities and the markings in the bottom row by other authorities.

([5]) The UK handles and protects EUCI marked CONFIDENTIEL UE/EU CONFIDENTIAL in accordance with the protective security requirements for UK SECRET.

ANNEX II

LIST OF ABBREVIATIONS

Acronym	Meaning
CA	Crypto Authority
CAA	Crypto Approval Authority
CCTV	Closed Circuit Television
CDA	Crypto Distribution Authority
CIS	Communication and Information Systems handling EUCI
DSA	Designated Security Authority
EUCI	EU Classified Information
FSC	Facility Security Clearance
IA	Information Assurance
IAA	Information Assurance Authority
IDS	Intrusion Detection System
IT	Information Technology
LSO	Local Security Officer
NSA	National Security Authority
PSC	Personnel Security Clearance
PSCC	Personnel Security Clearance Certificate
PSI	Programme/Project Security Instructions
RCO	Registry Control Officer
SAA	Security Accreditation Authority
SAL	Security Aspects Letter
SCG	Security Classification Guide
SecOPs	Security Operating Procedures
TA	TEMPEST Authority
TFEU	Treaty on the Functioning of the EU

ANNEX III

LIST OF NATIONAL SECURITY AUTHORITIES

BELGIUM

Autorité nationale de Sécurité
SPF Affaires étrangères, Commerce extérieur et Coopération au Développement
15, rue des Petits Carmes
1000 Bruxelles
Tel. Secretariat: +32 25014542
Fax +32 25014596
E-mail: nvo-ans@diplobel.fed.be

BULGARIA

State Commission on Information Security
90 Cherkovna Str.
1505 Sofia
Tel. +359 29333600
Fax +359 29873750
E-mail: dksi@government.bg
Website: www.dksi.bg

CZECH REPUBLIC

Národní bezpečnostní úřad
(National Security Authority)
Na Popelce 2/16
150 06 Praha 56
Tel. +420 257283335
Fax +420 257283110
E-mail: czech.nsa@nbu.cz
Website: www.nbu.cz

DENMARK

Politiets Efterretningstjeneste
(Danish Security Intelligence Service)
Klausdalsbrovej 1
2860 Søborg
Tel. +45 33148888
Fax +45 33430190

Forsvarets Efterretningstjeneste
(Danish Defence Intelligence Service)
Kastellet 30
2100 Copenhagen Ø
Tel. +45 33325566
Fax +45 33931320

GERMANY

Bundesministerium des Innern
Referat ÖS III 3
Alt-Moabit 101 D
D-11014 Berlin
Tel. +49 30186810
Fax +49 30186811441
E-mail: oesIII3@bmi.bund.de

ESTONIA

National Security Authority Department
Estonian Ministry of Defence
Sakala 1
15094 Tallinn
Tel. +372 7170113 0019, +372 7170117
Fax +372 7170213
E-mail: nsa@mod.gov.ee

GREECE

Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Διακλαδική Διεύθυνση Στρατιωτικών Πληροφοριών (ΔΔΣΠ)
Διεύθυνση Ασφαλείας και Αντιπληροφοριών
ΣΤΓ 1020 -Χολαργός (Αθήνα)
Ελλάδα
Τηλ.: +30 2106572045 (ώρες γραφείου)
+ 30 2106572009 (ώρες γραφείου)
Φαξ: +30 2106536279; + 30 2106577612

Hellenic National Defence General Staff (HNDGS)
Military Intelligence Sectoral Directorate
Security Counterintelligence Directorate
GR-STG 1020 Holargos – Athens
Tel. +30 2106572045
+ 30 2106572009
Fax +30 2106536279, +30 2106577612

SPAIN

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
28023 Madrid
Tel. +34 913725000
Fax +34 913725808
E-mail: nsa-sp@areatec.com

FRANCE

Secrétariat général de la défense et de la sécurité nationale
Sous-direction Protection du secret (SGDSN/PSD)
51 Boulevard de la Tour-Maubourg
75700 Paris 07 SP
Tel. +33 171758177
Fax + 33 171758200

CROATIA

Office of the National Security Council
Croatian NSA
Jurjevska 34
10000 Zagreb
Croatia
Tel. +385 14681222
Fax + 385 14686049
Website: www.uvns.hr

IRELAND

National Security Authority
Department of Foreign Affairs
76 – 78 Harcourt Street
Dublin 2
Tel. +353 14780822
Fax +353 14082959

ITALY

Presidenza del Consiglio dei Ministri
D.I.S. – U.C.Se.
Via di Santa Susanna, 15
00187 Roma
Tel. +39 0661174266
Fax +39 064885273

CYPRUS

ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ
ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Υπουργείο Άμυνας
Λεωφόρος Εμμανουήλ Ροΐδη 4
1432 Λευκωσία, Κύπρος

Τηλέφωνα: +357 22807569, +357 22807643,
+357 22807764
Τηλεομοιότυπο: +357 22302351

Ministry of Defence
Minister's Military Staff
National Security Authority (NSA)
4 Emanuel Roidi street
1432 Nicosia
Tel. +357 22807569, +357 22807643,
+357 22807764
Fax +357 22302351
E-mail: cynsa@mod.gov.cy

LATVIA

National Security Authority
Constitution Protection Bureau of the Republic of Latvia
P.O. Box 286
LV-1001 Riga
Tel. +371 67025418
Fax +371 67025454
E-mail: ndi@sab.gov.lv

LITHUANIA

Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija
(The Commission for Secrets Protection Coordination of the Republic of Lithuania National Security Authority)
Gedimino 40/1
LT-01110 Vilnius
Tel. +370 706 66701, +370 706 66702
Fax +370 706 66700
E-mail: nsa@vsd.lt

LUXEMBOURG

Autorité nationale de Sécurité
Boîte postale 2379
1023 Luxembourg
Tel. +352 24782210 central
+ 352 24782253 direct
Fax +352 24782243

HUNGARY

Nemzeti Biztonsági Felügyelet
(National Security Authority of Hungary)
H-1024 Budapest, Szilágyi Erzsébet fasor 11/B
Tel. +36 (1) 7952303
Fax +36 (1) 7950344

Postal address:
H-1357 Budapest, PO Box 2
E-mail: nbf@nbf.hu
Website: www.nbf.hu

MALTA

Ministry for Home Affairs and National Security
P.O. Box 146
MT-Valletta
Tel. +356 21249844
Fax +356 25695321

NETHERLANDS

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20010
2500 EA Den Haag
Tel. +31 703204400
Fax +31 703200733

Ministerie van Defensie
Beveiligingsautoriteit
Postbus 20701
2500 ES Den Haag
Tel. +31 703187060
Fax +31 703187522

AUSTRIA

Informationssicherheitskommission
Bundeskanzleramt
Ballhausplatz 2
1014 Wien
Tel. +43 1531152594
Fax +43 1531152615
E-mail: ISK@bka.gv.at

POLAND

Agencja Bezpieczeństwa Wewnętrznego – ABW
(Internal Security Agency)
2A Rakowiecka St.
00-993 Warszawa
Tel. +48 22 58 57 944
Fax +48 22 58 57 443
E-mail: nsa@abw.gov.pl
Website: www.abw.gov.pl

PORTUGAL

Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Rua da Junqueira, 69
1300-342 Lisboa
Tel. +351 213031710
Fax +351 213031711

ROMANIA

Oficiul Registrului Național al Informațiilor Secrete de Stat
(Romanian NSA – ORNISS National Registry Office for Classified Information)
4 Mures Street
012275 Bucharest
Tel. +40 212245830
Fax +40 212240714
E-mail: nsa.romania@nsa.ro
Website: www.orniss.ro

SLOVENIA

Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
1000 Ljubljana
Tel. +386 14781390
Fax +386 14781399
E-mail: gp.uvtp@gov.si

SLOVAKIA

Národný bezpečnostný úrad
(National Security Authority)
Budatínska 30
P.O. Box 16
850 07 Bratislava
Tel. +421 268692314
Fax +421 263824005
Website: www.nbusr.sk

FINLAND

National Security Authority
Ministry for Foreign Affairs
P.O. Box 453
FI-00023 Government
Tel. 16055890
Fax +358 916055140
E-mail: NSA@formin.fi

SWEDEN

Utrikesdepartementet
(Ministry for Foreign Affairs)
SSSB
S-103 39 Stockholm
Tel. +46 84051000
Fax +46 87231176
E-mail: ud-nsa@foreign.ministry.se

UNITED KINGDOM

UK National Security Authority
Room 335, 3rd Floor
70 Whitehall
London
SW1A 2AS
Tel. 1: +44 2072765649
Tel. 2: +44 2072765497
Fax +44 2072765651
E-mail: UK-NSA@cabinet-office.x.gsi.gov.uk

2.13. 2019 M. SPALIO 17 D. KOMISIJOS SPRENDIMAS (ES, EURATOMAS) 2019/1961 DĖL SLAPTUMO ŽYMOMIS CONFIDENTIEL UE/ES CONFIDENTIAL IR SECRET UE/ES SECRET PAŽYMĖTOS INFORMACIJOS TVARKYMO ĮGYVENDINIMO TAISYKLIŲ

KOMISIJOS SPRENDIMAS (ES, Euratomas) 2019/1961

2019 m. spalio 17 d.

dėl slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėtos informacijos tvarkymo įgyvendinimo taisyklių

EUROPOS KOMISIJA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo, ypač į jos 249 straipsnį,

atsižvelgdama į Europos atominės energijos bendrijos steigimo sutartį, ypač į jos 106 straipsnį,

atsižvelgdama į 2015 m. kovo 13 d. Komisijos sprendimą (ES, Euratomas) 2015/443 dėl saugumo Komisijoje ([1]),

atsižvelgdama į 2015 m. kovo 13 d. Komisijos sprendimą (ES, Euratomas) 2015/444 dėl ES įslaptintos informacijos apsaugai užtikrinti skirtų saugumo taisyklių ([2]),

atsižvelgdama į 2017 m. sausio 10 d. Komisijos sprendimą (ES, Euratomas) 2017/46 dėl Europos Komisijos ryšių ir informacinių sistemų saugumo ([3]),

kadangi:

(1) Sprendimas (ES, Euratomas) 2015/444 taikomas visiems Komisijos padaliniams ir visose Komisijos patalpose;
(2) ES įslaptintos informacijos (toliau – ESĮI) apsaugai užtikrinti skirtos saugumo priemonės visą savo gyvavimo ciklą turi atitikti jos slaptumo žymos lygį;
(3) Sprendimo (ES, Euratomas) 2015/444 4 straipsnio 3 dalyje, 19 straipsnio 1 dalies c punkte ir 22 straipsnyje nustatyta, kad išsamesnės nuostatos, skirtos sprendimui papildyti ir jo įgyvendinimui sustiprinti, numatomos įgyvendinimo taisyklėse, reglamentuojančiose klausimus, kaip antai slaptumo žymų vadovo, kompensacinių priemonių, kai ESĮI tvarkoma ne saugioje ar administracinėje zonoje, ir rengėjo atsakomybę;
(4) įgyvendinimo taisyklės, skirtos Sprendimui (ES, Euratomas) 2015/444 papildyti ar sustiprinti, prireikus nustatomos remiantis to sprendimo 60 straipsniu;
(5) šiam sprendimui įgyvendinti skirtos saugumo priemonės atitinka Komisijos saugumo principus, nustatytus Sprendimo (ES, Euratomas) 2015/443 3 straipsnyje;
(6) remdamiesi deklaracijomis, pridėtomis prie Tarybos posėdžio, kuriame buvo priimtas Tarybos sprendimas 2013/488/ES ([4]), protokolo, Taryba, Komisija ir Europos Sąjungos vyriausiasis įgaliotinis užsienio reikalams ir saugumo politikai susitarė užtikrinti kuo didesnį nuoseklumą taikant saugumo taisykles, kad jų ESĮI būtų apsaugota kartu atsižvelgiant į konkrečius jų institucinius ir organizacinius poreikius;
(7) 2016 m. gegužės 4 d. Komisija priėmė sprendimą ([5]), kuriuo už saugumo klausimus atsakingam Komisijos nariui suteikiami įgaliojimai Komisijos vardu ir jos atsakomybe patvirtinti įgyvendinimo taisykles, numatytas Sprendimo (ES, Euratomas) 2015/444 60 straipsnyje,

PRIĖMĖ ŠĮ SPRENDIMĄ:

1 SKYRIUS

BENDROSIOS NUOSTATOS

1 straipsnis

Dalykas ir taikymo sritis

1. Šiuo sprendimu nustatomos slaptumo žymomis lygiais CONFIDENTIEL UE/ES CONFIDENTIAL ([6]) ir SECRET UE/ES SECRET ([7]) pažymėtos ES įslaptintos informacijos (toliau – ESĮI) tvarkymo sąlygos laikantis Sprendimo (ES, Euratomas) 2015/444.

2. Šis sprendimas taikomas visiems Komisijos padaliniams ir visose Komisijos patalpose.

2 straipsnis

Galimybės susipažinti su slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėta informacija kriterijai

1. Galimybė susipažinti su informacija, kurios slaptumo žymos yra CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET, gali būti suteikiama:

a) nustačius, kad asmeniui reikia turėti galimybę susipažinti su tam tikra slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėta informacija, kad jis galėtų atlikti Europos Komisijai reikalingą profesinę funkciją arba užduotį;
b) asmenį informavus apie taisykles ir atitinkamus saugumo standartus ir gaires, skirtus slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėtai informacijai apsaugoti;
c) asmeniui pripažinus savo atsakomybę už atitinkamos informacijos apsaugą;
d) kai pagal Sprendimo (ES, Euratomas) 2015/444 10 straipsnio 1 dalies 3 punktą Komisijos saugumo institucija asmeniui suteikė leidimą susipažinti su atitinkamo lygio ESĮI iki nurodytos datos.

2. Pareigos, dėl kurių reikia susipažinti su slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėta informacija, nepavedamos Komisijos stažuotojams.

3. Kitų kategorijų darbuotojams galimybė susipažinti su tokia informacija nesuteikiama arba suteikiama pagal priede pateikiamą lentelę.

2 SKYRIUS

SLAPTUMO ŽYMOMIS *CONFIDENTIEL UE/ES CONFIDENTIAL* IR *SECRET UE/ES SECRET* PAŽYMĖTOS INFORMACIJOS RENGIMAS

3 straipsnis

Rengėjas

Nors pagal Sprendimo (ES, Euratomas) 2015/444 1 straipsnį rengėjas yra Europos Sąjungos institucija, agentūra ar įstaiga, valstybė narė, trečioji valstybė ar tarptautinė organizacija, kurios atsakomybe įslaptinta informacija buvo parengta ir (arba) pateikta naudoti Europos Sąjungos struktūrose, slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėtos informacijos rengėjas nebūtinai bus tas pats asmuo.

4 straipsnis

Slaptumo žymos lygio suteikimas

1. Darbuotojai, kurie rengia dokumentą, remdamiesi 1 straipsnyje nurodyta informacija, visada sprendžia, ar jų dokumentas turi būti įslaptintas. Siekdamas įslaptinti dokumentą, kaip ESĮI, rengėjas vertina ir sprendžia, ar dokumento atskleidimas leidimo neturintiems asmenims pakenktų Europos Sąjungos arba vienos ar daugiau valstybių narių interesams. Jeigu rengėjams kyla kokių nors abejonių dėl to, ar dokumentą, kurį jie rengia, yra pagrindo žymėti slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET, jie turėtų konsultuotis su atsakingu skyriaus vadovu arba direktoriumi.

2. Dokumentas žymimas bent jau slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL, jeigu be leidimo atskleidžiama informacija galėtų, *inter alia*:

a) iš esmės pakenkti diplomatiniams santykiams, t. y. būti oficialaus protesto ar kitokių sankcijų priežastis;
b) pakenkti asmens saugumui arba laisvei;
c) pakenkti valstybių narių ar kitų įnašų mokėtojų komandiruotų darbuotojų veiklos veiksmingumui arba saugumui arba svarbių saugumo ar žvalgybos operacijų veiksmingumui;
d) iš esmės pakenkti pagrindinių organizacijų finansiniam gyvybingumui;
e) sutrukdyti sunkaus nusikaltimo tyrimui ar palengvinti jo įvykdymą;
f) iš esmės pakenkti Europos Sąjungos ar valstybių narių finansiniams, pinigų politikos, ekonominiams ir prekybos interesams;
g) stipriai sutrukdyti formuoti ar vykdyti pagrindinę Europos Sąjungos politiką;
h) nutraukti arba kitaip iš esmės sužlugdyti svarbią Europos Sąjungos veiklą;
i) privesti prie aukštesnio lygio įslaptintos informacijos atskleidimo.

3. Informacija žymima bent jau slaptumo žyma SECRET UE/ES SECRET, jeigu be leidimo atskleidžiama informacija galėtų, *inter alia*:

a) sukelti tarptautinę įtampą;
b) labai pakenkti santykiams su trečiosiomis valstybėmis ar tarptautinėmis organizacijomis;
c) sukelti tiesioginį pavojų gyvybei arba didelę žalą viešajai tvarkai arba asmens saugumui ar laisvei;
d) labai pakenkti valstybių narių ar kitų įnašų mokėtojų komandiruotų darbuotojų veiklos veiksmingumui arba saugumui arba tolesniam labai svarbių saugumo ar žvalgybos operacijų veiksmingumui;
e) padaryti didelę materialinę žalą Europos Sąjungos ar valstybių narių finansiniams, pinigų politikos, ekonominiams ir prekybos interesams;
f) privesti prie aukštesnio lygio įslaptintos informacijos atskleidimo.

4. Rengėjai gali nuspręsti tam tikrų kategorijų informacijai, kurią jie reguliariai rengia, suteikti standartinę slaptumo žymą. Tačiau jie užtikrina, kad atskiroms informacijos dalims būtų suteikta tinkama slaptumo žyma.

5 straipsnis

Darbas su projektais

1. Informacija įslaptinama iškart, kai tik ji parengiama. Asmeniniai užrašai, preliminarūs projektai arba pranešimai, kuriuose yra informacijos, kurią yra pagrindo žymėti slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES, nuo pat pradžių taip pažymimi ir rengiami bei tvarkomi pagal šį sprendimą.

2. Jei nėra pagrindo galutinį dokumentą žymėti pradine slaptumo žyma jo slaptumas sumažinamas arba jis išslaptinamas.

6 straipsnis

Pradinės medžiagos registravimas

Siekiant suteikti galimybę rengėjui vykdyti kontrolę pagal 14 straipsnį, slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėtų dokumentų rengėjai, kiek tai įmanoma, registruoja visus įslaptintus šaltinius, naudojamus įslaptintiems dokumentams rengti, įskaitant išsamią informaciją apie ES valstybių narių, tarptautinių organizacijų arba trečiųjų valstybių kilmės šaltinius. Prireikus bendra įslaptinta informacija žymima taip, kad būtų galima apsaugoti naudotos įslaptintos pradinės medžiagos rengėjų tapatybę.

7 straipsnis

Dokumento dalių įslaptinimas

1. Pagal Sprendimo (ES, Euratomas) 2015/444 22 straipsnio 6 dalį dokumento bendras slaptumo žyma nustatoma bent pagal aukščiausią slaptumo žymos lygį turinčią jo dalį. Kai informacija renkama iš įvairių šaltinių, visas galutinis dokumentas peržiūrimas siekiant nustatyti jo bendrą slaptumo žymą, nes gali prireikti jam suteikti aukštesnį slaptumo žymos lygį nei jo dalims.

2. Dokumentams, kuriuose yra įslaptintų ir neįslaptintų dalių, suteikiama tokia struktūra ir jie pažymimi taip, kad skirtingo lygio įslaptinimo ir (arba) slaptumo žymomis pažymėtas dalis būtų galima lengvai nustatyti ir prireikus atskirti. Kai dalis atskiriama nuo kitų dalių, kiekvieną dalį galima tvarkyti tinkamai.

8 straipsnis

Visais žodžiais nurodyta slaptumo žyma

1. Informacija, kurią yra pagrindo įslaptinti, atitinkamai pažymima ir tvarkoma, kad ir kokia būtų jos fizinė forma. Įslaptinimo lygis, arba slaptumo žyma, aiškiai nurodomas gavėjams jeigu informacija pateikiama raštu ant popieriaus, ant išimamųjų duomenų saugojimo laikmenų arba ryšių ir informacinėje sistemoje (RIS), arba pranešimu, jeigu informacija pateikiama žodžiu, pavyzdžiui, per pokalbį arba pristatymą. Įslaptinta medžiaga fiziškai žymima taip, kad būtų galima lengvai nustatyti jos slaptumo žymą.

2. Remiantis 3 dalimi, ant dokumentų slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET nurodoma didžiosiomis raidėmis prancūzų ir anglų kalbomis (pirma prancūzų kalba) visais žodžiais. Žyma neverčiama į kitas kalbas.

3. Slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET nurodoma taip:

a) centre, dokumento kiekvieno puslapio viršuje ir apačioje;
b) visais žodžiais nurodyta slaptumo žyma vienoje eilutėje, nepaliekant tarpų nė iš vienos pasvirojo brūkšnio pusės;
c) didžiosiomis raidėmis, juodu paryškintuoju šriftu „Times New Roman 16“ (jei įmanoma, bet bent jau 14) ir apvestais iš abiejų pusių kraštais.

4. Rengiant slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėtą dokumentą:

a) kiekvienas puslapis aiškiai pažymimas slaptumo žyma;
b) kiekvienas puslapis numeruojamas;
c) dokumente nurodomas nuorodos numeris, registracijos numeris ir dalykas, kuris nėra įslaptinta informacija, išskyrus tuo atveju, kai jis pažymėtas kaip įslaptinta informacija;
d) visi priedai ir priedėliai išvardijami, jeigu įmanoma, pirmame puslapyje;
e) dokumente nurodoma jo parengimo data.

5. Jei įmanoma, slaptumo žyma SECRET UE/ES SECRET žymima raudona spalva.

9 straipsnis

Žymų santrumpos *C-UE/EU-C* ir *S-UE/EU-S*

Žymų santrumpas C-UE/EU-C ir S-UE/EU-S galima naudoti siekiant nurodyti atitinkamai slaptumo žyma C-UE/EU-C arba S-UE/EU-S pažymėto dokumento atskirų dalių slaptumo žymos lygį arba ten, kur slaptumo žymos negalima nurodyti visais žodžiais, pavyzdžiui, ant mažos išimamosios duomenų saugojimo laikmenos. Santrumpa gali būti naudojama pagrindinėje teksto dalyje, kai slaptumo žymas sudėtinga pakartotinai nurodyti visais žodžiais. Santrumpa nenaudojama dokumento antraštėje ir poraštėje vietoj visais žodžiais nurodomos slaptumo žymos.

10 straipsnis

Kitos slaptumo žymos galiojimo žymos

1. Slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėti dokumentai gali būti žymimi kitais ženklais arba slaptumo žymos galiojimo žymomis, nurodant, pavyzdžiui, veiklos sritį, su kuria dokumentas susijęs, arba nurodant konkretų jo platinimą vadovaujantis principu „būtina žinoti“. Pavyzdžiui:

RELEASABLE TO LIECHTENSTEIN

2. Slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėti dokumentai gali turėti saugumo apribojimą, kuriame pateikiami konkretūs nurodymai, kaip tvarkyti ir valdyti dokumentus.

3. Jeigu įmanoma, bet kokie nurodymai, kaip sumažinti dokumento slaptumą arba jį išslaptinti, turi būti nurodomi dokumento pirmame puslapyje tuo metu, kai jis parengiamas. Pavyzdžiui, galima naudoti tokią žymą:

SECRET UE/ES SECRET iki [mmmm mm dd] ir **RESTREINT UE/ES RESTRICTED** vėliau

11 straipsnis

Elektroninis apdorojimas

1. Slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėti dokumentai parengiami naudojant elektronines priemones, jeigu jų yra.

2. Rengdami slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėtą informaciją, Komisijos darbuotojai naudoja atitinkamam arba aukštesniam slaptumo žymos lygiui akredituotą RIS. Jeigu kyla abejonių, kokią RIS naudoti, darbuotojai konsultuojasi su vietos saugumo pareigūnu (VSP). Konsultuojantis su Komisijos saugumo institucija, ekstremalios padėties atvejais arba specifinių techninių konfigūracijų atvejais galima taikyti specialias procedūras.

3. Kaip reikalaujama pagal 5 straipsnį, slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėti dokumentai, įskaitant projektus, nesiunčiami el. laišku, nespausdinami arba neskenuojami standartiniais spausdintuvais arba skeneriais, arba netvarkomi darbuotojų asmeniniais prietaisais. Slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėti dokumentai spausdinami tik spausdintuvais arba kopijavimo aparatais, prijungtais prie atskirų nuo elektromagnetinės spinduliuotės apsaugotų kompiuterių arba akredituotų sistemų.

12 straipsnis

Registracija saugumo tikslais

1. Slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėta informacija saugumo tikslais registruojama prieš ją platinant ir ją gavus. Ji registruojama:
– kai ji pasiekia organizacinį subjektą ar iš jo išsiunčiama;
– kai ji pasiekia RIS ar iš jos išsiunčiama.

2. Tokia registracija gali būti atliekama popieriuje arba elektroninėse registrų knygose.

3. Jeigu informacija tvarkoma elektroniniu būdu RIS, šios registravimo procedūros gali būti atliekamos vykdant procedūras pačioje RIS. Šiuo atveju RIS apima priemones, kuriomis užtikrinamas įrašų registruose vientisumas.

4. Registro kontrolės pareigūnas tvarko registrą, kuriame apie kiekvieną dokumentą pateikiama bent ši informacija:

a) galutinio įslaptinto dokumento registracijos data;
b) slaptumo žymos lygis;
c) jei taikoma, slaptumo žymos lygio galiojimo pabaigos data;
d) parengusio padalinio pavadinimas;
e) gavėjas arba gavėjai;
f) dalykas;
g) parengusio padalinio suteiktas dokumento nuorodos numeris;
h) registracijos numeris;
i) išplatintų kopijų skaičius;
j) jei įmanoma, dokumentui parengti panaudotų šaltinių registras;
k) dokumento slaptumo sumažinimo arba išslaptinimo data;
l) informacija apie sunaikinimą (vieta, data, metodas, priežiūra, sunaikinimo pažymėjimas).

13 straipsnis

Platinimas

Slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėtų dokumentų siuntėjas nusprendžia, kam platinti informaciją, vadovaudamasis principu „būtina žinoti“. Siekiant užtikrinti tolesnį principo „būtina žinoti“ laikymąsi, sudaromas platinimo sąrašas.

3 SKYRIUS

DARBAS SU TURIMA SLAPTUMO ŽYMOMIS *CONFIDENTIEL UE/ES CONFIDENTIAL* IR *SECRET UE/ES SECRET* PAŽYMĖTA INFORMACIJA

14 straipsnis

Rengėjo vykdoma kontrolė

1. Rengėjas vykdo savo parengtos slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėtos informacijos kontrolę. Išankstinio rašytinio rengėjo sutikimo prašoma prieš informaciją:

a) išslaptinant arba sumažinant slaptumą;
b) naudojant kitais nei rengėjo nustatytais tikslais;
c) suteikiant trečiajai valstybei ar tarptautinei organizacijai;
d) atskleidžiant ne Komisijoje, bet ES esančiai šaliai;
e) atskleidžiant trečiojoje valstybėje esančiam rangovui arba galimam rangovui.

2. Slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėtos informacijos turėtojai yra tinkamai įgalioti asmenys, kuriems galimybė susipažinti su įslaptinta informacija suteikiama tam, kad jie galėtų vykdyti savo pareigas. Jie yra atsakingi už tinkamą jos tvarkymą, saugojimą ir apsaugą pagal Sprendimą (ES, Euratomas) 2015/444. Kitaip nei įslaptintos informacijos rengėjai, turėtojai neturi teisės nuspręsti dėl slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėtos informacijos slaptumo sumažinimo, išslaptinimo arba vėlesnio jos suteikimo.

3. Jeigu slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėtos informacijos dalies rengėjo tapatybės nustatyti negalima, informacijos rengėjo kontrolę vykdo tą įslaptintą informaciją turintis Komisijos padalinys. Prieš suteikiant slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėtą informaciją trečiajai valstybei ar tarptautinei organizacijai, konsultuojamasi su Komisijos saugumo ekspertų grupe.

15 straipsnis

Slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėtai informacijai tvarkyti tinkamos RIS

1. Slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėta informacija tvarkoma ir perduodama naudojant elektronines priemones, jeigu jų yra. Atitinkamu arba aukštesniu slaptumo žymos lygiu pažymėtai informacijai tvarkyti naudojamos tik Komisijos saugumo akreditavimo institucijos akredituotos RIS ir įranga.

2. Jei Komisijos padalinys turi tinkamą įrangą šių lygių įslaptintai informacijai tvarkyti ir siųsti, jis padeda kitiems Komisijos subjektams tinkamai tvarkyti ir siųsti informaciją, jei tik jis tai gali padaryti.

16 straipsnis

Slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėtai informacijai išimamosiose duomenų saugojimo laikmenose taikomos specialiosios priemonės

1. Išimamųjų duomenų saugojimo laikmenų naudojimas griežtai kontroliuojamas ir apskaitomas. Naudojamos tik Komisijos pateiktos išimamosios duomenų saugojimo laikmenos, užšifruotos Komisijos saugumo institucijos patvirtintu produktu. Asmeninės išimamosios duomenų saugojimo laikmenos ir konferencijose, seminaruose ir pan. nemokamai dalinamos išimamosios duomenų saugojimo laikmenos nenaudojamos įslaptintai informacijai perduoti. Jei įmanoma, atsižvelgiant į Komisijos saugumo institucijos rekomendacijas, turėtų būti naudojamos TEMPEST išbandytos išimamosios duomenų saugojimo laikmenos.

2. Jei įslaptintas dokumentas tvarkomas arba saugomas elektroniniu būdu išimamosiose duomenų saugojimo laikmenose, pavyzdžiui, USB atmintinėse, kompaktiniuose diskuose arba atminties kortelėse, slaptumo žyma turi būti aiškiai matoma ant pačios pateikiamos informacijos, taip pat rinkmenos pavadinime ir ant išimamos duomenų saugojimo laikmenos.

3. Darbuotojai turi turėti omenyje, kad išimamosiose duomenų saugojimo laikmenose saugojant didelius įslaptintos informacijos kiekius, yra pagrindo prietaisus žymėti aukštesne slaptumo žyma.

4. Slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėtai informacijai perkelti į išimamąsias duomenų saugojimo laikmenas ar iš jų naudojama tik tinkamai akredituota RIS.

5. Perkeliant tokią informaciją į išimamąsias duomenų saugojimo laikmenas, ypač svarbu užtikrinti, kad prieš perkeliant duomenis laikmenose nebūtų virusų ar kenkimo programinės įrangos.

6. Jei taikoma, išimamosios duomenų saugojimo laikmenos tvarkomos laikantis visų saugios eksploatacijos taisyklių, susijusių su naudojama šifravimo sistema.

7. Dokumentai išimamosiose duomenų saugojimo laikmenose, kurių nebereikia arba kurie buvo perkelti į atitinkamą RIS, saugiai pašalinami arba ištrinami naudojant patvirtintus produktus arba metodus. Jeigu nebereikalingos išimamosios duomenų saugojimo laikmenos nesaugomos tinkamame seife, jos sunaikinamos. Bet koks sunaikinimas arba ištrynimas atliekamas taikant metodą, kuris atitinka Komisijos saugumo taisykles. Išimamosios duomenų saugojimo laikmenos inventorizuojamos, o jų sunaikinimas registruojamas.

17 straipsnis

Slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėtos informacijos tvarkymas ir saugojimas

1. Pagal Sprendimo (ES, Euratomas) 2015/444 19 straipsnio 3 dalies a punktą slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėta informacija tvarkoma saugioje zonoje ([8]).

2. Pagal Sprendimo (ES, Euratomas) 2015/444 19 straipsnio 3 dalies b punktą ši informacija gali būti tvarkoma administracinėje zonoje ([9]), jeigu ESĮI yra apsaugota taip, kad su ja negalėtų susipažinti leidimo neturintys asmenys.

3. Ši informacija gali būti tvarkoma ne saugioje ar administraci-

nėje zonoje, jeigu turėtojas yra įsipareigojęs, kaip reikalaujama pagal Sprendimo (ES, Euratomas) 2015/444 19 straipsnio 3 dalies c punktą, taikyti kompensacines priemones, kurios apima bent šias priemones:

– slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėti dokumentai neskaitomi viešose vietose;
– turėtojas visą laiką asmeniškai kontroliuoja ESĮI;
– jei dokumentai pateikiami popierine forma, turėtojas atitinkamai registratūrai yra pranešęs, kad įslaptinti dokumentai tvarkomi ne saugioje ir ne administracinėje zonoje;
– dokumentai slepiami tinkamame seife, kai jie nėra skaitomi arba aptariami;
– kol dokumentas skaitomas ar aptarinėjamas, kabineto durys turi būti uždarytos;
– dokumento detalės neaptariamos telefonu nesaugia linija arba el. laiške;
– turėtojas dokumento nekopijuoja ir neskenuoja – papildomų kopijų gali suteikti tik registratūra;
– dokumentas tvarkomas ir laikinai laikomas ne administracinėje ar saugioje zonoje tik būtiną minimalų laiką, po to jis grąžinamas į registratūrą;
– kai dokumentas grąžinamas, patvirtinama parašu;
– turėtojas neišmeta arba nesunaikina įslaptinto dokumento.

4. Slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėta informacija saugoma saugioje zonoje esančioje apsauginėje talpykloje arba saugykloje.

5. Išsamesnių rekomendacijų galima kreiptis į atitinkamo Komisijos padalinio vietos saugumo pareigūną (VSP).

6. Apie visus su dokumentu susijusius įtariamus arba faktinius saugumo incidentus kuo greičiau pranešama VSP.

18 straipsnis

Slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėtos informacijos kopijavimas ir vertimas

1. Slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėta informacija gali būti kopijuojama

arba verčiama turėtojo nurodymu, įsitikinus, kad rengėjas nenustatė jokių apribojimų. Tačiau nedaroma daugiau kopijų, nei tikrai būtina.

2. Jeigu kopijuojama tik įslaptinto dokumento dalis, taikomos tos pačios sąlygos kaip ir viso dokumento kopijavimui. Ištraukos taip pat pažymimos tokia pačia slaptumo žyma, išskyrus atvejus, kai rengėjas konkrečiai pažymi jas mažesne slaptumo žyma arba nurodo, kad jos yra neįslaptintos.

3. Pirminei informacijai taikomos saugumo priemonės taip pat taikomos jų kopijoms ir vertimams.

19 straipsnis

Slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėtos informacijos gabenimui taikomi bendrieji principai

1. Jeigu įmanoma, slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėta informacija, kurią reikia perduoti už saugios ar administracinės zonos ribų, siunčiama elektroninėmis tinkamai akredituotomis priemonėmis ir (arba) saugoma naudojant patvirtintas kriptografines priemones.

2. Atsižvelgiant į turimas priemones arba konkrečias aplinkybes, slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėta informacija gali būti fiziškai gabenama popieriniuose dokumentuose arba išimamosiose duomenų saugojimo laikmenose. Pirmenybė teikiama slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėtos informacijos perdavimui išimamosiose duomenų saugojimo laikmenose, o ne popieriniuose dokumentuose.

3. Gali būti naudojamos tik Komisijos saugumo institucijos patvirtintu produktu užšifruotos išimamosios duomenų saugojimo laikmenos. Slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėta informacija išimamojoje duomenų saugojimo laikmenoje, kuri nėra apsaugota Komisijos saugumo institucijos patvirtintu šifravimo produktu, tvarkoma taip pat kaip ir popierinės kopijos.

4. Siuntoje gali būti daugiau nei viena ESĮI dalis, jeigu laikomasi

principo „būtina žinoti“.

5. Naudojama pakuotė užtikrina, kad turinys būtų uždengtas. Slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėta informacija gabenama dviguboje nepermatomoje pakuotėje, pavyzdžiui, voke, nepermatome aplanke arba portfelyje. Ant išorinės pakuotės nepateikiama jokių nuorodų į jos turinio pobūdį ar slaptumo žymos lygį. Vidinė pakuotė žymima slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET. Ant abiejų pakuočių nurodomas numatomo gavėjo vardas, pavardė, pareigos ir adresas, taip pat atgalinis adresas tuo atveju, kai siuntos negalima pristatyti.

6. Darbuotojai arba kurjeriai, gabenantys slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėtą informaciją, turi saugumo leidimą ir jiems išduodamas kurjerio pažymėjimas.

7. Vokas arba pakuotė neatidaromi pakeliui. Kurjeriui išduotas saugumo leidimas nesuteikia jam leidimo susipažinti su įslaptintos informacijos turiniu.

8. Apie visus saugumo incidentus, susijusius su slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėta informacija, kurią gabena darbuotojai arba kurjeriai, tolesnio tyrimo reikmėms pranešama Žmogiškųjų išteklių ir saugumo generalinio direktorato Saugumo direktoratui per atitinkamo Komisijos padalinio VSP.

20 straipsnis

Išimamųjų duomenų saugojimo laikmenų gabenimas naudojantis kurjerio paslaugomis

1. Prie išimamųjų duomenų saugojimo laikmenų, kurios naudojamos slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėtai informacijai gabenti, pridedamas išsiuntimo pranešimas, kuriame nurodoma, kad išimamojoje duomenų saugojimo laikmenoje yra įslaptinta informacija, taip pat visos joje esančios rinkmenos, kad gavėjas galėtų atlikti reikiamus patikrinimus ir patvirtinti, kad jas gavo.

2. Laikmenose saugomi tik teiktini dokumentai. Visa įslaptinta infor-

macija, pavyzdžiui, vienoje USB atmintinėje, turėtų būti skirta tam pačiam gavėjui. Siuntėjas turi omenyje, kad, tokiuose prietaisuose saugojant didelius įslaptintos informacijos kiekius, yra pagrindo visą prietaisą žymėti aukštesniu slaptumo žymos lygiu.

3. Slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėtai informacijai gabenti naudojamos tik tos išimamosios duomenų saugojimo laikmenos, kurios pažymėtos tinkama slaptumo žyma.

4. Slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėta informacija, išsaugota išimamojoje duomenų saugojimo laikmenoje, saugumo tikslais registruojama.

21 straipsnis

Slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėtų dokumentų gabenimas Komisijos pastatuose

1. Saugumo leidimą turintys darbuotojai gali gabenti slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėtus dokumentus Komisijos pastate, tačiau dokumentai nepaliekami be juos gabenančio asmens priežiūros arba neskaitomi viešai.

2. Slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėti dokumentai nesiunčiami vidiniu paštu.

22 straipsnis

Slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėtų dokumentų gabenimas Europos Sąjungoje

1. Komisijos darbuotojai arba kurjeriai gali gabenti slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėtą informaciją bet kur Europos Sąjungoje, jeigu jie laikosi šių nurodymų:

a) slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėtai informacijai perduoti naudojami dvigubi nepermatomi vokai arba pakuotės. Ant išorinės dalies nepateikiama jokių nuorodų į jos turinio pobūdį ar slaptumo žymos lygį;
b) slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėta informacija nepaliekama be ją gabenančio asmens priežiūros;
c) vokas arba pakuotė neatidaromi pakeliui, o informacija neskaitoma viešose vietose.

2. Registratūros darbuotojai, pageidaujantys išsiųsti slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL pažymėtą informaciją į kitas Europos Sąjungos vietas, gali pasirūpinti, kad ji būtų perduota vienu iš toliau nurodytų būdų:

– per nacionalines pašto tarnybas, kurios atseka siuntą, arba per tam tikras komercines kurjerių pašto tarnybas, kurios užtikrina, kad siuntą asmeniškai gabena kurjeris, jeigu jos atitinka šio sprendimo 24 straipsnyje nustatytus reikalavimus,
– per karinį, vyriausybinį ar diplomatinį kurjerį.

3. Darbuotojai, norintys išsiųsti slaptumo žyma SECRET UE/ES SECRET pažymėtą informaciją į kitas ES valstybes nares, ją gali išsiųsti per savo registratūrą tik per karinį, vyriausybinį ar diplomatinį kurjerį, bet ne per pašto tarnybas ar komercinius kurjerius.

4. Komisijos darbuotojai arba oficialūs Komisijos kurjeriai, gabenantys slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėtą informaciją, su savimi turi atitinkamo padalinio registratūros išduotą kiekvienos siuntos kurjerio pažymėjimą, patvirtinantį, kad ją gabenantis asmuo turi leidimą gabenti siuntą.

23 straipsnis

Slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėtos informacijos gabenimas iš trečiosios valstybės teritorijos ar į ją

1. Slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėtą informaciją darbuotojai gali gabenti iš Europos Sąjungos teritorijos į trečiosios valstybės teritoriją ir

atvirkščiai.

2. Registratūros darbuotojai gali ją išsiųsti per karinį ar diplomatinį kurjerį.

3. Gabendami slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėtus tiek popierinius dokumentus, tiek išimamąsias duomenų saugojimo laikmenas, darbuotojai laikosi visų šių papildomų priemonių:

– keliaujant viešuoju transportu, įslaptinta informacija laikoma portfelyje ar krepšyje, kurio priežiūra rūpinasi pats gabenantis asmuo. Ji nėra gabenama bagažo skyriuje;
– vidinė pakuotė paženklinama oficialiu spaudu, nurodančiu, kad tai yra oficiali siunta ir jos saugumo patikra neatliekama;
– siuntą gabenantis asmuo su savimi turi atitinkamo padalinio registratūros išduotą kurjerio pažymėjimą, kuriuo patvirtinama, kad siuntą gabenančiam asmeniui leidžiama gabenti slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėtą siuntą.

24 straipsnis

Gabenimas naudojantis komercinių kurjerių paslaugomis

1. Šiame sprendime komerciniai kurjeriai yra nacionalinės pašto tarnybos ir komercinės kurjerių bendrovės, kurios siūlo paslaugą pristatyti informaciją už mokestį arba ją gabenant asmeniškai, arba ją atsekant.

2. Komerciniai kurjeriai gali perduoti slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL pažymėtą informaciją valstybėje narėje arba iš vienos valstybės narės į kitą. Komerciniai kurjeriai gali perduoti slaptumo žyma SECRET UE/ES SECRET pažymėtą informaciją tik valstybėje narėje, bet ne užsienyje.

3. Komercinėms kurjerių pašto tarnyboms nurodoma, kad jos gali pristatyti slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėtas siuntas tik registracijos kontrolės pareigūnui arba jo tinkamai įgaliotam pavaduojančiam pareigūnui ar numatytam gavėjui.

4. Komerciniai kurjeriai gali naudotis subrangovų paslaugomis. Tačiau atsakomybė už šio sprendimo laikymąsi tenka kurjerių bendrovei.

5. Slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba

SECRET UE/ES SECRET pažymėtai informacijai nenaudojamos komercinių kurjerių siūlomos elektroninio dokumentų siuntimo registruotu paštu paslaugos.

25 straipsnis

ESĮI parengimas gabenti naudojantis komercinių kurjerių pašto tarnybų paslaugomis

1. Kai rengiama įslaptinta siunta, siuntėjas atsižvelgia į tai, kad komercinės kurjerių pašto tarnybos pristato slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėtas siuntas tik numatytam gavėjui, jo tinkamai įgaliotam pavaduojančiam asmeniui, registracijos kontrolės pareigūnui arba jo tinkamai įgaliotam pavaduojančiam pareigūnui ar registratoriui.

2. Kai tokia informacija siunčiama per patvirtintą komercinę kurjerių pašto tarnybą, siunta parengiama ir supakuojama taip:

a) siuntai siųsti naudojami dvigubi vokai (vidinis vokas turi būti toks, kad bet kokia pastanga jį atidaryti būtų akivaizdi) ar kita atitinkamai saugi pakavimo medžiaga;
b) slaptumo žymos lygis aiškiai matomas ant vidinio voko arba vidinės pakuotės;
c) slaptumo žyma ant išorinio voko arba išorinės pakuotės nenurodoma;
d) tiek vidinis, tiek išorinis vokas arba pakuotė aiškiai adresuojami nurodytam asmeniui numatyto gavėjo įstaigoje ir nurodomas atgalinis adresas;
e) į vidinį voką arba vidinę pakuotę įdedama gavimo registracijos forma, ją gavėjas užpildo ir grąžina. Pati gavimo registracijos forma nėra įslaptinta ir joje nurodomas nuorodos numeris, data ir dokumento kopijos numeris, bet ne dalykas;
f) pristatymo patvirtinimo formą reikalaujama pateikti ant išorinio voko arba ant išorinės pakuotės. Pati pristatymo patvirtinimo forma nėra įslaptinta ir joje nurodomas nuorodos numeris, data ir dokumento kopijos numeris, bet ne dalykas;
g) kurjerių pašto tarnyba turi gauti ir pateikti siuntėjui pasirašytą ir užregistruotą dokumentą, patvirtinantį, kad siunta pristatyta, arba kurjeris turi gauti pristatymo patvirtinimus arba pakuočių numerius.

3. Siuntėjas susisiekia su nurodytu gavėju prieš išsiųsdamas siuntą,

kad susitartų dėl tinkamos pristatymo datos ir laiko.

4. Tik siuntėjas yra atsakingas už visas siuntas, siunčiamas per komercinę kurjerių pašto tarnybą. Tuo atveju, kai siunta prarandama arba nepristatoma laiku, siuntėjas apie tai praneša Komisijos saugumo institucijai, o ši atlieka paskesnį saugumo incidento tyrimą.

26 straipsnis

Kitos specialiosios tvarkymo sąlygos

1. Laikomasi visų gabenimo sąlygų, nustatytų susitarime dėl informacijos saugumo arba administraciniuose susitarimuose. Jei kyla abejonių, darbuotojai konsultuojasi su savo atitinkama registratūra arba Žmogiškųjų išteklių ir saugumo generalinio direktorato Saugumo direktoratu.

2. Dvigubos pakuotės reikalavimas gali būti netaikomas įslaptintai informacijai, kuri yra apsaugota patvirtintomis kriptografinėmis priemonėmis. Tačiau adresavimo tikslais, taip pat dėl to, kad išimamosiose duomenų saugojimo laikmenose aiškiai nurodoma slaptumo žyma, laikmena gabenama bent jau įprastame voke, bet gali reikėti papildomų fizinės apsaugos priemonių, pvz., vokų su oro apsauga.

4 SKYRIUS

SUSITIKIMAI, KURIUOSE APTARIAMA ĮSLAPTINTA INFORMACIJA

27 straipsnis

Susitikimo, kuriame aptariama slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėta informacija, rengimas

1. Susitikimai, kuriuose turi būti aptariama slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėta informacija, rengiami tik atitinkamo ar aukštesnio

lygio akredituotoje posėdžių salėje. Jeigu jos nėra, darbuotojai kreipiasi patarimo į Komisijos saugumo instituciją.

2. Paprastai darbotvarkės neturėtų būti įslaptintos. Jeigu susitikimo darbotvarkėje minimi įslaptinti dokumentai, pati darbotvarkė nėra automatiškai įslaptinama. Darbotvarkės klausimai formuluojami taip, kad nekiltų pavojaus Europos Sąjungos arba vienos ar kelių valstybių narių interesų apsaugai.

3. Susitikimo organizatoriai dalyviams primena, kad bet kokios pastabos dėl susitikimo, kuriame aptariama slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėta informacija, darbotvarkės klausimo neturi būti siunčiamos el. laiškais arba kitomis priemonėmis, kurios nebuvo tinkamai akredituotos pagal šio sprendimo 11 straipsnį.

4. Siekiant užtikrinti sklandų susitikimo darbą, susitikimo organizatoriai stengiasi darbotvarkėje iš eilės sugrupuoti slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėtus klausimus. Diskusijose įslaptintais klausimais gali dalyvauti tik tie asmenys, kuriems „būtina žinoti“, kurių patikimumas patikrintas atitinkamu lygiu ir kuriems, kai taikoma, suteiktas leidimas.

5. Pačiame kvietime dalyviai įspėjami, kad susitikime bus aptariamos įslaptintos temos ir kad bus taikomos atitinkamos saugumo priemonės.

6. Dalyviams primenama, kad, svarstant slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėtus klausimus, nešiojamuosius elektroninius prietaisus reikia palikti už posėdžių salės ribų.

7. Prieš susitikimą susitikimo rengėjai parengia išsamų dalyvių sąrašą.

28 straipsnis

Dalyvių galimybės dalyvauti susitikime, kuriame aptariama slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėta informacija

1. Susitikimo organizatoriai informuoja Komisijos saugumo instituciją apie visus išorės lankytojus, kurie dalyvaus Komisijos patalpose rengiamame susitikime, kuriame aptariama slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES

SECRET pažymėta informacija.

2. Dalyviai turės įrodyti, kad turi tinkamo lygio galiojantį asmens patikimumo pažymėjimą, kad galėtų dalyvauti diskusijoje darbotvarkės klausimais, kuriuose aptariama slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėta informacija.

29 straipsnis

Elektroninė įranga posėdžių salėje, kurioje aptariama slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėta informacija

1. Kai perduodama įslaptinta informacija, pavyzdžiui, reikalinga perskaityti pranešimui, kuriame atskleidžiama slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėta informacija, arba rengti vaizdo konferencijoms, gali būti naudojamos tik pagal šio sprendimo 11 straipsnį akredituotos IT sistemos.

2. Pirmininkas užtikrina, kad nešiojamieji elektroniniai prietaisai, kuriems nesuteiktas leidimas, būtų palikti už posėdžių salės ribų.

30 straipsnis

Tvarka, kurios turi būti laikomasi per susitikimą, kuriame aptariama slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėta informacija

1. Diskusijos, kurioje aptariama įslaptinta informacija, pradžioje pirmininkas praneša susitikimo dalyviams apie tai, kad pradedama svarstyti įslaptinta informacija. Durys turi būti uždarytos.

2. Prireikus diskusijos pradžioje dalyviams ir vertėjams žodžiu, patvirtinus parašu, pateikiama tik tiek dokumentų, kiek būtina.

3. Per visas susitikimo pertraukas slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėti dokumentai nepaliekami be priežiūros.

4. Susitikimo pabaigoje dalyviams ir vertėjams žodžiu primenama,

kad jie salėje be priežiūros negali palikti jokių įslaptintų dokumentų arba savo padarytų įslaptintų užrašų. Visi slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėti dokumentai, kurių dalyviams nereikia pasibaigus susitikimui, ir bet kokiu atveju visi vertėjų žodžiu dokumentai, patvirtinus parašu, grąžinami registracijos kontrolės pareigūnui sunaikinti atitinkamuose smulkintuvuose.

5. Per susitikimą sudaromas dalyvių sąrašas ir bet kokios įslaptintos informacijos, kuria dalytasi su valstybėmis narėmis ir kuri suteikta žodžiu trečiosioms valstybėms ar tarptautinėms organizacijoms, aprašymas, kad ši informacija būtų įrašyta į susitikimo rezultatus.

31 straipsnis

Vertėjai žodžiu ir raštu

Susipažinti su slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėta informacija gali tik tie vertėjai žodžiu ir raštu, kurių patikimumas patikrintas, kuriems suteiktas leidimas ir kuriems taikomi Europos Sąjungos pareigūnų tarnybos nuostatai ir kitų tarnautojų įdarbinimo sąlygos arba kurie su Komisija turi sutartinių ryšių.

5 SKYRIUS

DALIJIMASIS IR KEITIMASIS SLAPTUMO ŽYMOMIS *CONFIDENTIEL UE/ES CONFIDENTIAL* IR *SECRET UE/ES SECRET* PAŽYMĖTA INFORMACIJA

32 straipsnis

Rengėjo sutikimas

Jeigu Komisija nėra įslaptintos informacijos, kurią prašoma suteikti arba kuria prašoma pasidalinti, arba pradinės medžiagos, kuri gali būti įtraukta į tą informaciją, rengėja, tą įslaptintą informaciją turintis Komisijos padalinys pirmiausia prašo jos rengėjo pateikti rašytinį sutikimą suteikti šią informaciją. Jeigu rengėjo tapatybės nustatyti negalima, informacijos rengėjo kontrolę vykdo tą įslaptintą informaciją turintis Komisijos padalinys.

33 straipsnis

Dalijimasis slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėta informacija su kitais Europos Sąjungos subjektais

1. Slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėta informacija dalijamasi su kita Europos Sąjungos institucija, agentūra, įstaiga ar organu tik tuo atveju, jeigu gavėjui „būtina žinoti“ ir subjektas yra sudaręs atitinkamą teisinį susitarimą su Komisija.

2. Generalinio sekretoriato valdoma Komisijos ESĮI registratūra paprastai yra pagrindinis įslaptintos informacijos, kuria keičiamasi su kitomis Europos Sąjungos institucijomis, agentūromis, įstaigomis ir organais, gavimo ir išsiuntimo punktas. Su Komisijos saugumo institucija konsultuojamasi tais atvejais, kai esama saugumo, organizacinių ar veiklos priežasčių, dėl kurių vietos ESĮI registratūroms labiau tinka būti gavimo ir išsiuntimo punktais, klausimais, kurie yra susiję su atitinkamo padalinio kompetencija.

34 straipsnis

Keitimasis slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėta informacija su valstybėmis narėmis

1. Slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėta informacija gali būti keičiamasi su valstybėmis narėmis, jeigu gavėjui „būtina žinoti“ ir jo patikimumas patikrintas.

2. Valstybių narių įslaptintai informacijai, kuri yra pažymėta lygiaverte nacionaline slaptumo žyma ([10]) ir kuri buvo pateikta Komisijai, suteikiamas toks pats apsaugos lygis kaip ir slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėtai informacijai.

35 straipsnis

Keitimasis slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėta informacija su trečiosiomis valstybėmis ir tarptautinėmis organizacijomis

1. Slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėta informacija suteikiama trečiajai valstybei ar tarptautinei organizacijai tik tuo atveju, jeigu gavėjui „būtina žinoti“, o valstybė ar tarptautinė organizacija turi atitinkamą teisinę ar administracinę sistemą, pavyzdžiui, yra sudariusi susitarimą dėl informacijos saugumo arba administracinį susitarimą su Komisija. Tokio susitarimo nuostatos yra viršesnės už šio sprendimo nuostatas.

2. Generalinio sekretoriato valdoma ESĮI registratūra paprastai yra pagrindinis visos įslaptintos slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėtos informacijos, kuria Komisija keičiasi su trečiosiomis valstybėmis ir tarptautinėmis organizacijomis, gavimo ir išsiuntimo punktas. Su Komisijos saugumo institucija konsultuojamasi tais atvejais, kai esama saugumo, organizacinių ar veiklos priežasčių, dėl kurių vietos ESĮI registratūroms labiau tinka būti gavimo ir išsiuntimo punktais, klausimais, kurie yra susiję su

atitinkamo padalinio kompetencija.

3. Visa iš trečiųjų valstybių ar tarptautinių organizacijų gauta įslaptinta informacija saugumo tikslais registruojama. Todėl, gavę įslaptintos informacijos ne įprastu registracijos kanalu, darbuotojai susisiekia su registratūra.

4. Siekiant užtikrinti atsekamumą, slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėta informacija registruojama:

– kai ji pasiekia organizacinį subjektą ar iš jo išsiunčiama;
– kai ji pasiekia RIS ar iš jos išsiunčiama.

5. Toks registravimas gali būti atliekamas popieriuje arba elektroninėse registrų knygose.

6. Įslaptintos informacijos, kuri tvarkoma akredituotoje RIS, registravimo procedūros gali būti atliekamos vykdant procedūras pačioje RIS. Tokiu atveju RIS apima priemones, kuriomis užtikrinamas vientisumas įrašų registruose.

7. Iš trečiųjų valstybių ar tarptautinių organizacijų gautai įslaptintai informacijai suteikiamas lygiavertis apsaugos lygis kaip ir ESĮI, nurodant lygiavertę slaptumo žymą, kaip nustatyta atitinkamame susitarime dėl informacijos saugumo arba administraciniame susitarime.

36 straipsnis

Slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėtos informacijos *ad hoc* suteikimas išimtine tvarka

1. Jeigu Komisija arba vienas iš jos padalinių nustato, kad slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėtą informaciją išimtine tvarka reikia suteikti trečiajai valstybei, tarptautinei organizacijai arba ES subjektui, bet nėra sudaryto susitarimo dėl informacijos saugumo arba administracinio susitarimo, laikomasi informacijos *ad hoc* suteikimo išimtinės tvarkos.

2. Komisijos padaliniai kreipiasi į Komisijos saugumo instituciją, o ji konsultuojasi su Komisijos saugumo ekspertų grupe.

3. Pasikonsultavusi su Komisijos saugumo ekspertų grupe, Komisija, remdamasi už saugumą atsakingo Komisijos nario pasiūlymu, gali leisti suteikti atitinkamą informaciją.

6 SKYRIUS

SLAPTUMO ŽYMOMIS *CONFIDENTIEL UE/ES CONFIDENTIAL* IR *SECRET UE/ES SECRET* PAŽYMĖTOS INFORMACIJOS ĮSLAPTINIMO PABAIGA

37 straipsnis

Kada sumažinti slaptumą arba išslaptinti

1. Informacija lieka įslaptinta tik tol, kol ją būtina apsaugoti. Slaptumo mažinimas – slaptumo žymos lygio mažinimas. Išslaptinimas reiškia, kad informacija visiškai nebelaikoma įslaptinta. Įslaptintos informacijos rengėjas, rengdamas ESĮI, nurodo, jei įmanoma, ar tam tikrą dieną arba po tam tikro įvykio galima sumažinti ESĮI slaptumą arba ją išslaptinti. Kitu atveju bent kas penkerius metus rengėjas peržiūri informaciją ir įvertina riziką, kad nustatytų, ar pradinės slaptumo žymos lygis tebėra pagrįstas.

2. Komisijos dokumentų slaptumas taip pat gali būti sumažintas arba jie gali būti išslaptinti *ad hoc* pagrindu, pavyzdžiui, visuomenei pateikus prašymą leisti susipažinti su informacija.

38 straipsnis

Atsakomybė už slaptumo sumažinimą ir išslaptinimą

1. Slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėtos informacijos slaptumas nesumažinamas ar tokia informacija nėra išslaptinama be rengėjo leidimo.

2. Komisijos padalinys, kuris parengia įslaptintą dokumentą, atsako už sprendimą, ar galima sumažinti jo slaptumą arba jį išslaptinti. Komisijoje visi prašymai dėl slaptumo sumažinimo ir išslaptinimo pateikiami pasikonsultavus su parengusio padalinio skyriaus vadovu arba direktoriumi. Jei padalinys surinko įslaptintą informaciją iš įvairių šaltinių, pirmiausia jis siekia gauti bet kurios kitos šalies, kuri pateikė pradinės medžiagos, įskaitant valstybes nares, kitas ES įstaigas, trečiąsias valstybes ar tarptautines organizacijas, sutikimą.

3. Jeigu informaciją parengusio Komisijos padalinio nebėra ir jo at-

sakomybę perėmė kita tarnyba, sprendimą dėl slaptumo sumažinimo ir išslaptinimo priima ši tarnyba. Jeigu parengusio padalinio nebėra ir jo atsakomybės neperėmė kita tarnyba, sprendimą dėl slaptumo sumažinimo ar išslaptinimo kartu priima informaciją gavusių generalinių direktoratų skyrių vadovai arba direktoriai.

4. Padalinys, atsakingas už slaptumo sumažinimą ar išslaptinimą, bendradarbiauja su savo atitinkama registratūra dėl praktinių slaptumo sumažinimo ar išslaptinimo priemonių.

39 straipsnis

Neskelbtina neįslaptinta informacija

Kai peržiūrėjus dokumentą priimamas sprendimas jį išslaptinti, atsižvelgiama į tai, ar dokumentas turėtų būti pažymėtas neskelbtinos neįslaptintos informacijos platinimo žyma, kaip apibrėžta Sprendimo (ES, Euratomas) 2015/443 9 straipsnyje.

40 straipsnis

Kaip nurodyti, kad dokumento slaptumas buvo sumažintas ar jis buvo išslaptintas

1. Kiekvieno puslapio viršuje ir apačioje esanti originali slaptumo žyma matomai perbraukiama (nepašalinama), naudojant perbraukimo funkciją elektroninėje formoje arba perbraukiant ranka popierinėje kopijoje.

2. Pirmasis puslapis (viršelis) užantspauduojamas kaip sumažinto slaptumo ar išslaptintas, ir užrašomi už slaptumo sumažinimą ar išslaptinimą atsakingos institucijos duomenys ir atitinkama data.

3. Apie slaptumo sumažinimą ar išslaptinimą pranešama pirminiams slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėtos informacijos gavėjams. Pirminiai gavėjai yra atsakingi už visų vėlesnių adresatų, kuriems jie išsiuntė arba kopijavo pirminę slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėtą informaciją, informavimą.

4. Komisijos istorinių archyvų tarnybai pranešama apie visus priimtus išslaptinimo sprendimus.

5. Visiems įslaptintos informacijos vertimams taikomos tokios pačios slaptumo sumažinimo ar išslaptinimo procedūros kaip ir versijai originalo kalba.

41 straipsnis

Slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėtos informacijos dalinis slaptumo sumažinimas ar išslaptinimas

1. Taip pat įmanomas dalinis slaptumo sumažinimas ar išslaptinimas (pvz., tik priedai, kai kurios pastraipos). Procedūra identiška viso dokumento slaptumo sumažinimo ar išslaptinimo procedūrai.

2. Kai slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėta informacija išslaptinama (iškarpoma) iš dalies, parengiama išslaptinta ištrauka.

3. Dalys, kurios lieka įslaptintos, pakeičiamos įrašu

NEIŠSLAPTINTINA DALIS

arba pačiame tekste, jei dalis, kuri lieka įslaptinta, yra pastraipos dalis, arba pateikiamos kaip pastraipa, jei dalis, kuri lieka įslaptinta, yra konkreti pastraipa ar daugiau kaip viena pastraipa.

4. Tekste daroma konkreti nuoroda, jei visas priedas negali būti išslaptintas ir todėl nebuvo įtrauktas į ištrauką.

42 straipsnis

Slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėtos informacijos reguliarus sunaikinimas ir ištrynimas

1. Komisija nekaupia didelių įslaptintos informacijos kiekių.

2. Parengę padaliniai bent kas penkerius metus peržiūri sunaikinti arba ištrinti skirtus dokumentus. Reguliariais intervalais peržiūrima tiek informacija, kuri saugoma popieriuje, tiek RIS saugoma informacija.

3. Darbuotojai nesunaikina nė vieno popierinės formos slaptumo

žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėto dokumento, kurio nebereikia, tačiau prašo savo registracijos kontrolės pareigūno dokumentus sunaikinti, atsižvelgdami į visus dokumento originalo archyvavimo reikalavimus.

4. Iš darbuotojų nereikalaujama informuoti rengėjo, jeigu jie ištrina slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėtų dokumentų kopijas.

5. Medžiagos, kurioje yra įslaptintos informacijos, projektui taikomi tie patys sunaikinimo metodai kaip ir galutiniams įslaptintiems dokumentams.

6. Slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėtiems dokumentams naikinti naudojami tik patvirtinti smulkintuvai. Slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL pažymėtiems dokumentams naikinti tinka 5 lygio DIN 66399 smulkintuvai. Slaptumo žyma SECRET UE/ES SECRET pažymėtiems dokumentams naikinti tinka 6 lygio DIN 66399 smulkintuvai.

7. Patvirtinto smulkintuvo atliekas galima šalinti kaip įprastas biuro atliekas.

8. Registracijos kontrolės pareigūnas parengia sunaikinimo pažymėjimus ir atitinkamai atnaujina registrų knygas ir kitą registracijos informaciją.

9. Visos laikmenos ir prietaisai, kuriuose yra slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėtos informacijos, tinkamai sunaikinami, kai baigiasi jų naudojimo trukmė. Elektroniniai duomenys sunaikinami arba ištrinami iš informacinių technologijų išteklių ir su jais susijusių duomenų saugojimo laikmenų taip, kad būtų galima pagrįstai užtikrinti, kad informacijos nebūtų galima atkurti. Ištrinant iš kaupiklio pašalinami duomenys, taip pat pašalinami visi ženklai, žymos ir veiklos registrai.

10. Kompiuterinės duomenų saugojimo laikmenos pateikiamos VSP arba vietos informatikos saugumo pareigūnui ir (arba) registro kontrolės pareigūnui sunaikinti ir pašalinti.

43 straipsnis

Slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėtos informacijos evakuacija ir sunaikinimas ekstremaliosios padėties atveju

1. Padalinio vadovas parengia, patvirtina ir, jei būtina, pradeda įgyvendinti evakuacijos ir sunaikinimo ekstremaliosios padėties atveju planus, kad apsaugotų ESĮI, kai kyla didelis pavojus, kad ji per krizę gali patekti į leidimo neturinčių asmenų rankas. Pirmumo tvarka ir atsižvelgiant į ekstremaliosios padėties pobūdį, svarstoma:

1) ESĮI pergabenti į alternatyvią saugią vietą, jei įmanoma, į tame pačiame pastate esančią saugią zoną;
2) ESĮI evakuoti į alternatyvią saugią vietą, jei įmanoma, į saugią zoną, esančią kitame pastate, jei įmanoma, Komisijos pastate;
3) ESĮI sunaikinti, jei įmanoma, naudojant patvirtintas sunaikinimo priemones.

2. Kai planai ekstremaliosios padėties atveju pradedami įgyvendinti, pirmenybė teikiama pirma slaptumo žyma SECRET UE/ES SECRET pažymėtos informacijos, o tada bet kokios slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL pažymėtos informacijos pergabenimui arba sunaikinimui.

3. Patys operatyviniai duomenys apie evakuacijos ir sunaikinimo ekstremaliosios padėties atveju planus įslaptinami kaip RESTREINT UE/ES RESTRICTED. Jų kopija laikoma kiekviename seife, kuriame saugoma slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėta informacija, kad ji būtų prieinama ekstremaliosios padėties atveju.

44 straipsnis

Archyvavimas

1. Sprendimai dėl to, ar ir kada archyvuoti, ir atitinkamos praktinės priemonės, kurių reikia imtis, turi atitikti Komisijos dokumentų tvarkymo politiką.

2. Slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėti dokumentai nesiunčiami į Europos Sąjungos istorinius archyvus Florencijoje.

7 SKYRIUS

BAIGIAMOSIOS NUOSTATOS

45 straipsnis

Skaidrumas

Apie šį sprendimą informuojami Komisijos darbuotojai ir visi asmenys, kuriems jis taikomas, ir jis paskelbiamas *Europos Sąjungos oficialiajame leidinyje*.

46 straipsnis

Įsigaliojimas

Šis sprendimas įsigalioja dvidešimtą dieną po jo paskelbimo *Europos Sąjungos oficialiajame leidinyje*.

Priimta Briuselyje 2019 m. spalio 17 d.

Komisijos vardu,

Pirmininko pavedimu

Komisijos narys

Günther OETTINGER

([1]) OL L 72, 2015 3 17, p. 41.

([2]) OL L 72, 2015 3 17, p. 53.

([3]) OL L 6, 2017 1 11, p. 40.

([4]) 2013 m. rugsėjo 23 d. Tarybos sprendimas 2013/488/ES dėl ES įslaptintos informacijos apsaugai užtikrinti skirtų saugumo taisyklių (OL L 274, 2013 10 15, p. 1).

([5]) 2016 m. gegužės 4 d. Komisijos sprendimas dėl įgaliojimo, susijusio su saugumu, C(2016) 2797 *final*.

([6]) Pagal Sprendimo (ES, Euratomas) 2015/444 3 straipsnį slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL pažymėta informacija – „informacija ir medžiaga, kurią neteisėtai atskleidus galėtų būti pakenkta Europos Sąjungos arba vienos ar kelių valstybių narių esminiams interesams“.

([7]) Pagal Sprendimo (ES, Euratomas) 2015/444 3 straipsnį slaptumo žyma SECRET UE/ES SECRET pažymėta informacija – „informacija ir medžiaga, kurią neteisėtai atskleidus galėtų būti rimtai pakenkta Europos Sąjungos arba vienos ar kelių valstybių narių esminiams interesams“.

([8]) Kaip apibrėžta Sprendimo (ES, Euratomas) 2015/444 18 straipsnyje.

([9]) Kaip apibrėžta Sprendimo (ES, Euratomas) 2015/444 18 straipsnyje.

([10]) Valstybių narių žymų atitikmenų lentelė pateikta Sprendimo (ES, Euratomas) 2015/444 I priede.

PRIEDAS

Darbuotojų, kurie prireikus gali susipažinti su slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėta informacija, kad galėtų atlikti savo profesines užduotis, kategorijos

Komisijos darbuotojų kategorijos	**Galimybė susipažinti su slaptumo žymomis C-UE/EU- C ir S-UE/EU-S pažymėta informacija**	**Sąlygos**
Pareigūnai	Taip	Patikimumo patikrinimas + informacinis susirinkimas + patvirtinimas + leidimas + principas „būtina žinoti“
Laikinieji darbuotojai	Taip	Patikimumo patikrinimas + informacinis susirinkimas + patvirtinimas + leidimas + principas „būtina žinoti“
Sutartininkai	Taip	Patikimumo patikrinimas + informacinis susirinkimas + patvirtinimas + leidimas + principas „būtina žinoti“
Deleguotieji nacionaliniai ekspertai (DNE)	Taip	Tik jeigu prieš jų paskyrimą jų patikimumą patikrino ES valstybės narės + Komisijos surengtas informacinis susirinkimas + patvirtinimas + Komisijos išduotas leidimas + principas „būtina žinoti“
Stažuotojai	Ne	Išimčių nenumatyta
Visų kitų kategorijų darbuotojai (per laikinojo įdarbinimo įmonę įdarbinti laikinieji darbuotojai, *intra muros* išorės darbuotojai ir pan.)	Ne	Dėl visų išimčių kreiptis į Komisijos saugumo instituciją

2.14. COMMISSION DECISION (EU, EURATOM) 2019/1961 OF 17 OCTOBER 2019 ON IMPLEMENTING RULES FOR HANDLING CONFIDENTIEL UE/EU CONFIDENTIAL AND SECRET UE/EU SECRET INFORMATION

COMMISSION DECISION (EU, Euratom) 2019/1961

of 17 October 2019

on implementing rules for handling CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 249 thereof,

Having regard to the Treaty establishing the European Atomic Energy Community, and in particular Article 106 thereof,

Having regard to Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on security in the Commission ([1]),

Having regard to Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information ([2]),

Having regard to Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission ([3]),

Whereas:

(1) Decision (EU, Euratom) 2015/444 applies to all Commission departments and in all premises of the Commission.
(2) Security measures for protecting EU classified information (EUCI) throughout its life-cycle are to be commensurate in particular with its security classification.
(3) Articles 4(3), 19(1)(c) and 22 of Decision (EU, Euratom) 2015/444 provide that more detailed provisions to supplement and support implementation of the Decision are to be laid down in implementing rules, governing issues such as a classification guide, compensatory measures for handling EUCI outside a Secured Area or an Administrative Area, and originator responsibilities.
(4) Where necessary, implementing rules to supplement or support Decision (EU, Euratom) 2015/444 are to be adopted in accordance with Article 60 of that Decision.
(5) Security measures taken to implement this Decision are to comply with the principles for security in the Commission set out in Article 3 of Decision (EU, Euratom) 2015/443.
(6) The Council, the Commission and the High Representative of the Union for Foreign Affairs and Security Policy have agreed to ensure maximum consistency in the application of security rules regarding their protection of EUCI while taking into account their specific institutional and organisational needs, in accordance with the declarations attached to the minutes of the Council session at which Council Decision 2013/488/EU ([4]).
(7) On 4 May 2016 the Commission adopted a decision ([5]) empowering the Member of the Commission responsible for security matters to adopt, on behalf of the Commission and under its responsibility, the implementing rules provided for in Article 60 of Decision (EU, Euratom) 2015/444,

HAS ADOPTED THIS DECISION:

CHAPTER 1

GENERAL PROVISIONS

Article 1

Subject matter and scope

1. This Decision sets out the handling conditions for EU classified information (EUCI) of CONFIDENTIEL UE/EU CONFIDENTIAL ([6]) and SECRET UE/EU SECRET ([7]) level in compliance with Decision (EU, Euratom) 2015/444.

2. This Decision shall apply to all Commission departments and in all premises of the Commission.

Article 2

Criteria for access to CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information

1. Access to information classified as CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET may be granted after:

(a) The need for an individual to have access to certain CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information in order to be able to perform a professional function or task for the European Commission has been determined;

(b) The individual has been briefed on the rules and the relevant security standards and guidelines for protecting CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information;

(c) The individual has acknowledged their responsibilities for protecting the information concerned; and

(d) The individual has been authorised by the Commission security authority to access EUCI up to the relevant level and until a specified date in accordance with Article 10(1)3 of Decision (EU, Euratom) 2015/444.

2. Commission trainees shall not be given duties that require them to have access to CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information.

3. Access shall be withheld or permitted for other categories of staff in accordance with the table set out in the Annex.

CHAPTER 2

CREATING CONFIDENTIEL UE/EU CONFIDENTIAL AND SECRET UE/EU SECRET INFORMATION

Article 3

Originator

While the originator within the meaning of Article 1 of Decision (EU, Euratom) 2015/444 is the Union institution, agency or body, Member State, third state or international organisation under whose authority classified information has been created and/or introduced into the Union's structures, the drafter of CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information will not necessarily be the same.

Article 4

Assigning a classification level

1. Staff drafting a document on the basis of information within the meaning of Article 1 shall always consider whether their document needs to be classified. Classifying a document as EUCI shall involve an assessment and a decision by the originator as to whether the disclosure of the document to unauthorised persons would cause prejudice to the interests of the European Union or of one or more of the Member States. If drafters are in any doubt as to whether the document they are drafting warrants being classified as CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET they should consult the Head of Unit or Director responsible.

2. A document shall be classified as at least CONFIDENTIEL UE/EU CONFIDENTIAL if its unauthorised disclosure could, inter alia:

(a) materially damage diplomatic relations, i.e. cause formal protest or other sanctions;

(b) prejudice individual security or liberty;
(c) cause damage to the operational effectiveness or security of Member States' or other contributors' deployed personnel, or to the effectiveness of valuable security or intelligence operations;
(d) substantially undermine the financial viability of major organisations;
(e) impede the investigation of or facilitate serious crime;
(f) work substantially against the Union's or Member States' financial, monetary, economic and commercial interests;
(g) seriously impede the development or operation of major Union policies;
(h) shut down or otherwise substantially disrupt significant Union activities;
(i) lead to the discovery of information classified at a higher level.

3. Information shall be classified as at least SECRET UE/EU SECRET if its unauthorised disclosure could, inter alia:
(a) raise international tensions;
(b) seriously damage relations with third countries or international organisations;
(c) threaten life directly or seriously prejudice public order or individual security or liberty;
(d) cause serious damage to the operational effectiveness or security of Member States' or other contributors' deployed personnel, or to the continuing effectiveness of highly valuable security or intelligence operations;
(e) cause substantial material damage to the Union's or Member States' financial, monetary, economic or commercial interests;
(f) lead to the discovery of information classified at a higher level.

4. Originators may decide to attribute a standard classification level to categories of information that they create on a regular basis. However, they shall ensure that individual pieces of information are given the appropriate classification level.

Article 5

Working with drafts

1. Information shall be classified as soon as it is produced. Personal notes, preliminary drafts or messages containing information that warrants classification at the level of CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET shall be marked as such from the outset

and shall be produced and handled in accordance with this Decision.

2. If the final document no longer warrants the initial classification level it shall be downgraded or declassified.

Article 6

Record of source material

In order to enable the exercise of originator control in accordance with Article 14, originators of CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET documents shall keep a record of any classified sources used for producing classified documents, including details of sources originally from EU Member States, international organisations or third countries. Where appropriate, aggregated classified information shall be marked in such a way as to preserve the identification of the originators of the classified source materials used.

Article 7

Classifying parts of a document

1. In accordance with Article 22(6) of Decision (EU, Euratom) 2015/444, the overall classification level of a document shall be at least as high as that of its most highly classified component. When information from various sources is collated, the final aggregated document shall be reviewed to determine its overall security classification level, since it may warrant a higher classification than its component parts.

2. Documents containing classified and non-classified parts shall be structured and marked so that components with different classification and/or sensitivity levels can be easily identified and detached if necessary. This shall enable each part to be handled appropriately when detached from the other components.

Article 8

Full classification marking

1. Information that warrants classification shall be marked and handled as such regardless of its physical form. The classification level

shall be clearly communicated to recipients, either by a classification marking, if the information is delivered in written form, whether this is on paper, on removable storage media or in a Communication and Information System (CIS), or by an announcement, if the information is delivered in oral form, such as in a conversation or a presentation. Classified material shall be physically marked so as to allow for easy identification of its security classification.

2. On documents, the full classification marking CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET shall be written in block capitals, in full in French and English (French first), in accordance with paragraph 3. The marking shall not be translated into other languages.

3. The CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET classification marking shall be affixed as follows:

(a) centred at the top and bottom of every page of the document;
(b) the complete classification marking on one line, with no spaces either side of the forward slash;
(c) in capitals, black, font Times New Roman 16 (when possible, but at least 14), bold and surrounded by a border on each side.

4. When creating a CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET document:

(a) each page shall be marked clearly with the classification level;
(b) each page shall be numbered;
(c) the document shall bear a reference number, a registration number and a subject, which itself shall not be classified information unless it is marked as such;
(d) all the annexes and enclosures shall be listed, whenever possible on the first page; and
(e) the document shall have the date of its creation on it.

5. When possible, the SECRET UE/EU SECRET marking shall appear in red.

Article 9

Abbreviated C-UE/EU-C and S-UE/EU-S classification markings

The abbreviations C-UE/EU-C and S-UE/EU-S may be used to indicate the classification level of individual parts respectively of a CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET document or where the full classification marking cannot be inserted, for example on a small removable storage medium. It may be used in the body of text where repeated use of the full classification markings is cumbersome. The abbreviation shall not be used instead of the full classification markings in the header and footer of the document.

Article 10

Other security designators

1. CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET documents may bear other markings, or 'security designators', specifying, for example, the field to which the document relates, or indicating a particular distribution on a need-to-know basis. An example is:

RELEASABLE TO LIECHTENSTEIN

2. CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET documents may bear a security caveat that gives specific instructions on how to handle and manage the documents.

3. Whenever possible, any indications for downgrading or declassifying shall be affixed on the first page of the document at the time it is created. For example, the following marking may be used:

SECRET UE/EU SECRET until [dd.mm.yyyy] and **RESTREINT UE/EU RESTRICTED** thereafter

Article 11

Electronic processing

1. CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET documents shall be created using electronic means, where these are available.

2. When creating CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information, Commission staff shall use CIS accredited for the corresponding classification level or for a higher classification level. Staff shall consult their Local Security Officer (LSO) if there is any doubt as to which CIS may be used. In consultation with the Commission security authority specific procedures may be applied in emergencies or in specific technical configurations.

3. CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET documents, including drafts, as required by Article 5, shall not be sent by email, printed or scanned on standard printers or scanners, or handled on the personal devices of members of staff. Only printers or copiers connected to standalone computers protected from electromagnetic emissions or to an accredited system shall be used to print out CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET documents.

Article 12

Registration for security purposes

1. Information classified as CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET shall be registered for security purposes prior to distribution and on receipt. It shall be registered:
- when it arrives in or leaves an organisational entity; and
- when it arrives in or leaves a CIS.

2. This registration may be carried out in paper or in electronic logbooks.

3. If the information is handled electronically within a CIS, these recording procedures may be performed by processes within the CIS itself. In this case, the CIS shall include measures to guarantee the integrity of the log records.

4. The Registry Control Officer shall keep a register that contains at least the following information for each document:
(a) the date the final classified document was registered;
(b) the classification level;
(c) where applicable, the expiry date of the classification level;
(d) the name of the originating department;
(e) the recipient or recipients;
(f) the subject;
(g) the originating department's reference number for the document;
(h) the registration number
(i) the number of copies circulated;
(j) where possible, the log of sources used for creating the document;
(k) the date of downgrading or declassification of the document; and
(l) destruction details (place, date, method, supervision, destruction certificate).

Article 13

Distribution

The sender of CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET documents shall decide who to distribute the information to, based on their need-to-know. A distribution list shall be drawn up in order to further enforce the need-to-know principle.

CHAPTER 3

WORKING WITH EXISTING CONFIDENTIEL UE/EU CONFIDENTIAL AND SECRET UE/EU SECRET INFORMATION

Article 14

Originator control

1. The originator shall have 'originator control' over CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information which it has created. The originator's prior written consent shall be sought before the information can be:

(a) declassified or downgraded;
(b) used for purposes other than those established by the originator;
(c) released to a third country or international organisation;
(d) disclosed to a party outside the Commission but within the EU; or
(e) disclosed to a contractor or prospective contractor located in a third country.

2. Holders of CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information are duly authorised individuals that have been given access to the classified information in order to be able to perform their duties. They are responsible for the correct handling, storage and protection of it in accordance with Decision (EU, Euratom) 2015/444. Unlike originators of classified information, holders shall not be authorised to decide on the downgrading, declassification or onward release of CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information.

3. If the originator of a piece of CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information cannot be identified, the Commission department holding that classified information shall exercise originator control. The Commission Security Expert Group shall be consulted before CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information is released to a third country or international organisation.

Article 15

CIS suitable for handling CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information

1. CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information shall be handled and transmitted by electronic means, where these are available. Only CIS and equipment that has been accredited by the Commission security accreditation authority for handling information classified at the relevant level or a higher classification level shall be used.

2. Where a Commission department has the appropriate equipment to handle and send information classified at these levels it shall assist other Commission entities in handling and sending information appropriately, as far as it is able to do so.

Article 16

Specific measures for CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information on removable storage media

1. The use of removable storage media shall be strictly controlled and accounted for. Only removable storage media provided by the Commission and encrypted by a product approved by the Commission security authority shall be used. Personal removable storage media and those given freely at conferences, seminars, etc. shall not be used for transferring classified information. Where possible, Tempest-proof removable storage media should be used, in accordance with the guidance from the Commission security authority.

2. Where a classified document is handled or stored electronically on removable storage media, such as USB sticks, CDs or memory cards, the classification marking shall be clearly visible on the displayed information itself, as well as in the filename and on the removable storage medium.

3. Staff shall bear in mind that when large amounts of classified information are stored on removable storage media the device may warrant a higher classification level.

4. Only CIS that have been appropriately accredited shall be used to transfer CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information onto or from removable storage media.

5. When downloading such information on removable storage media, particular care shall be taken to ensure that the media does not contain viruses or malware prior to the transfer of the data.

6. Where applicable, removable storage media shall be handled in accordance with any security operating procedures relating to the encryption system used.

7. Documents on removable storage media that are either no longer required, or have been transferred onto an appropriate CIS, shall be securely removed or deleted using approved products or methods. Unless stored in an appropriate safe, removable storage media shall be destroyed when no longer needed. Any destruction or deletion shall use a method that is in accordance with the Commission security rules. An

inventory shall be kept of the removable media, and their destruction shall be registered.

Article 17

Handling and storage of CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information

1. In accordance with Article 19(3)(a) of Decision (EU, Euratom) 2015/444, CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information shall be handled in a Secured Area ([8]).

2. Pursuant to Article 19(3)(b) of Decision (EU, Euratom) 2015/444, this information may be handled in an Administrative Area ([9]), provided the EUCI is protected from access by unauthorised persons.

3. This information may be handled outside a Secured Area or an Administrative Area provided the holder has undertaken to comply with compensatory measures as required under Article 19(3)(c) of Decision (EU, Euratom) 2015/444, which shall include at least the following:

- CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET documents shall not be read in public places.
- The EUCI shall be kept at all times under the personal control of the holder.
- In the case of documents in paper form, the holder has notified the relevant registry of the fact that the classified documents are being handled outside a Secured Area and Administrative Area.
- The documents shall be stowed in an appropriate safe when they are not being read or discussed.
- The doors to the room shall be closed while the document is being read or discussed.
- The details of the document shall not be discussed over the phone on a non-secured line or in an email.
- The document shall not be photocopied or scanned by the holder. Only the registry may provide any further copies.
- The document shall only be handled and temporarily held outside an Administrative or Secured Area for the minimum time necessary, after which it shall be returned to the registry.
- Return of the document shall be signed for.
- The holder shall not throw the classified document away or destroy it.

4. CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/

EU SECRET information shall be stored in a Secured Area in a security container or a strong room.

5. Further advice can be sought from the Local Security Officer (LSO) of the relevant Commission department.

6. Any suspected or actual security incidents involving the document shall be reported to the LSO as soon as possible.

Article 18

Copying and translating CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information

1. CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information may be copied or translated on instruction from the holder, provided the originator has not imposed any caveats. However, no more copies shall be made than are strictly necessary.

2. Where only part of a classified document is reproduced, the same conditions shall apply as for copying the full document. Extracts shall also be classified at the same level, unless the originator has specifically classified them at a lower level, or marked them as unclassified.

3. The security measures applicable to the original information shall also be applied to copies and translations thereof.

Article 19

General principles for carrying CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information

1. Whenever possible, CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information that needs to be taken outside Secured Areas or Administrative Areas shall be sent electronically by appropriately accredited means and/or protected by approved cryptographic products.

2. Depending on the means available or the particular circumstances, CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information may be physically carried by hand in the form of paper documents or on removable storage media. The use of removable storage media to transfer CONFIDENTIEL UE/EU CONFIDENTIAL

and SECRET UE/EU SECRET information shall be given preference to sending paper documents.

3. Only removable storage media encrypted by a product approved by the Commission security authority may be used. CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information on removable storage media that is not protected by an encryption product that has been approved by the Commission security authority shall be handled in the same manner as paper copy.

4. A consignment may contain more than one piece of EUCI, provided the need-to-know principle is respected.

5. The packaging used shall ensure that the contents are covered from view. CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information shall be carried in two layers of opaque packaging, such as envelopes, opaque folders or a briefcase. The outer packaging shall not bear any indication of the nature or classification level of its contents. The inner layer of packaging shall be marked as CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET. Both layers shall state the intended recipient‘s name, job title and address, as well as a return address in case delivery cannot be made.

6. Staff or couriers hand-carrying CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information shall be security authorised and shall be issued with a courier certificate.

7. The envelope/package shall not be opened *en route*. The security authorisation for the courier does not authorise him/her to access the content of the classified information.

8. Any security incidents involving CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information that is carried by staff or couriers shall be reported for subsequent investigation to the Security Directorate of the Directorate-General for Human Resources and Security, via the LSO of the relevant Commission department.

Article 20

Hand carriage of removable storage media

1. Removable storage media that are used to transport CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information shall be accompanied by a dispatch note, detailing the removable storage media containing the classified information, as well as all files contained on them, to allow the recipient to make the necessary verifications and to confirm receipt.

2. Only the documents to be provided shall be stored on the media. All the classified information on a single USB stick, for instance, would have to be intended for the same recipient. The sender shall bear in mind that large amounts of classified information stored on such devices may warrant a higher classification level for the device as a whole.

3. Only removable storage media bearing the appropriate classification marking shall be used to carry CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information.

4. Any CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information saved on removable storage media shall be registered for security purposes.

Article 21

Carriage of CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET documents within Commission buildings

1. Security authorised staff may carry CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET documents within a Commission building, but the documents shall not leave the possession of the bearer or be read in public.

2. CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET documents shall not be sent through internal mail.

Article 22

Carriage of CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET documents within the Union

1. CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information may be carried by staff or Commission couriers anywhere within the Union provided they comply with the following instructions:

(a) opaque double envelopes or packaging shall be used to convey CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information. The outside shall not bear any indication of the nature or classification level of its contents;

(b) the CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information shall not leave the possession of the bearer; and

(c) the envelope or package shall not be opened *en route* and the information shall not be read in public places.

2. Registry staff wishing to send CONFIDENTIEL UE/EU CONFIDENTIAL information to other locations in the Union may arrange for it to be conveyed by one of the following means:

– by national postal services that track the consignment or certain commercial courier services that guarantee personal hand carriage, provided that they meet the requirements set out in Article 24 of this Decision;

– by military, government or diplomatic courier.

3. Staff wishing to send SECRET UE/EU SECRET information to other Member States in the EU may only arrange with their Registry for it to be conveyed by military, government or diplomatic courier, but not by postal services or commercial couriers.

4. Commission staff or official Commission couriers bearing CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information shall carry a courier certificate for each consignment, issued by the respective department‘s registry, which certifies that the bearer is authorised to carry the consignment.

Article 23

Carriage of CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information from or to the territory of a third country

1. Information classified as CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET may be hand-carried by staff between the territory of the Union and the territory of a third country.

2. Registry staff may arrange for carriage by military or diplomatic courier.

3. When hand-carrying either paper documents or removable storage media classified as CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET, staff shall comply with all of the following additional measures:

– When travelling by public transport the classified information shall be placed in a briefcase or bag that is kept in the bearer's personal custody. It shall not be consigned to a baggage hold.
– The inner layer of packaging shall bear an official seal to indicate that it is an official consignment and is not to undergo security scrutiny.
– The bearer shall carry a courier certificate, which certifies that the bearer is authorised to carry the CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET consignment, issued by the relevant department's registry.

Article 24

Transport by commercial couriers

1. For the purposes of this Decision, 'commercial couriers' include national postal services and commercial courier companies that offer a service where information is delivered for a fee and is either personally hand carried or tracked.

2. Commercial couriers may convey CONFIDENTIEL UE/EU CONFIDENTIAL information within a Member State or from one Member State to another Member State. Commercial couriers may convey SECRET UE/EU SECRET information only within a Member State, but not abroad.

3. Commercial courier services shall be instructed that they may

deliver CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET consignments only to the Registry Control Officer, to his duly authorised substitute or to the intended recipient.

4. Commercial couriers may use the services of a sub-contractor. However, responsibility for complying with this Decision shall remain with the courier company.

5. Services offered by commercial couriers providing electronic transmission of registered delivery documents shall not be used for CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information.

Article 25

Preparation of EUCI for transport by commercial courier services

1. When classified consignments are being prepared the sender shall bear in mind that commercial courier services shall only deliver CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET consignments to the intended recipient, a duly authorised substitute, the registry control officer or his/her duly authorised substitute or a receptionist.

2. When such information is sent by an approved commercial courier service the consignment shall be prepared and packaged as follows:

(a) The consignment shall be sent using double envelopes (the inner envelope being such that any attempt to open it will be evident) or other suitably secure packing material.
(b) The classification level shall be clearly visible on the inner envelope or inner layer of packaging.
(c) The classification shall not be indicated on the outer envelope or the outer layer of packaging.
(d) Both the inner and outer envelopes or layers of packaging shall be clearly addressed to a named individual at the intended recipient, and shall include a return address.
(e) A registration receipt form shall be placed inside the inner envelope or inner layer of packaging for the recipient to complete and return. The registration receipt, which shall not itself be classified, shall quote the reference number, date and copy number of the document, but not the subject.

(f) Delivery receipts are required in the outer envelope or outer packaging. The delivery receipt, which itself shall not be classified, shall quote the reference number, date and copy number of the document, but not the subject.

(g) The courier service must obtain and provide the sender with proof of delivery of the consignment on the signature and tally record, or the courier must obtain receipts or package numbers.

3. The sender shall liaise with the named recipient before the consignment is sent to agree a suitable date and time for delivery.

4. The sender is solely responsible for any consignment sent by a commercial courier service. In the event that the consignment is lost or not delivered on time, the sender shall report it to the Commission security authority, which will follow up the security incident.

Article 26

Other specific handling conditions

1. Any carriage conditions set out in a security of information agreement or in administrative arrangements shall be complied with. If in doubt, staff shall consult their respective registry or the Security Directorate in the Directorate-General for Human Resources and Security.

2. The double packaging requirement can be waived for classified information that is protected by approved cryptographic products. However, for addressing purposes, and also as the removable storage medium bears an explicit security classification marking, the medium shall be carried in at least an ordinary envelope but may require additional physical protection measures, such as bubble wrap envelopes.

CHAPTER 4

CLASSIFIED MEETINGS

Article 27

Preparing for a CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET meeting

1. Meetings where CONFIDENTIEL UE/EU CONFIDENTIEL or SECRET UE/EU SECRET information is due to be discussed shall only be held in a meeting room that has been accredited at the appropriate level or higher. Where these are not available, staff shall seek the advice of the Commission security authority.

2. As a general rule, agendas should be not classified. If the agenda of a meeting mentions classified documents, the agenda itself shall not automatically be classified. Agenda items shall be worded in a way that avoids jeopardising the protection of the Union or one or more of the Member States‘ interests.

3. Meeting organisers shall remind participants that any comments sent in on a CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET agenda item must not be sent through email, or through other means that have not been appropriately accredited in accordance with Article 11 of this Decision.

4. Meeting organisers shall endeavour to group CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET items consecutively on the agenda in order to facilitate the smooth functioning of the meeting. Only persons with a need-to-know, who are security cleared to the appropriate level, and authorised where applicable, may be present during discussions of classified items.

5. The invitation itself shall forewarn the participants that the meeting will discuss classified topics, and that corresponding security measures will apply.

6. Participants shall be reminded that portable electronic devices are to be left outside the meeting room during discussion of CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET items.

7. Meeting organisers shall prepare a complete list of participants prior to the meeting.

Article 28

Participants' access to a CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET meeting

1. Meeting organisers shall inform the Commission security authority of any external visitors who will attend a CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET meeting on Commission premises.

2. Participants will be required to prove they hold a valid Personnel Security Clearance at the appropriate level in order to be able to attend the discussion of CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET agenda items.

Article 29

Electronic equipment in a CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET meeting room

1. Only accredited IT systems in accordance with Article 11 of this Decision may be used where classified information is conveyed, such as to give a presentation that displays CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information or for videoconferences.

2. The Chair shall ensure that unauthorised portable electronic devices have been left outside the meeting room.

Article 30

Procedures to be followed during a CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET meeting

1. At the start of the classified discussion, the Chair shall announce to the meeting that it is moving into classified mode. The doors shall be closed.

2. Only the necessary number of documents shall be signed for and issued to participants and interpreters, as appropriate, at the start of the discussion.

3. CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET documents shall not be left unattended during any breaks in the meeting.

4. At the end of the meeting, the participants and interpreters shall be reminded not to leave any classified documents or classified notes they might have made lying unattended in the room. Any CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET documents not required by the participants at the end of the meeting, and in any case all interpreters‘ documents, shall be signed for and returned to the Registry Control Officer for destruction in appropriate shredders.

5. The list of participants and an outline of any classified information shared with Member States and released orally to third countries or international organisations shall be noted down during the meeting in order to be recorded in the outcome of proceedings.

Article 31

Interpreters and translators

Only security-cleared and authorised interpreters and translators who are subject to the Staff regulations or the Conditions of Employment of other servants of the European Union or who have a contractual link to the Commission shall have access to CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information.

CHAPTER 5

SHARING AND EXCHANGING CONFIDENTIEL UE/EU CONFIDENTIAL AND SECRET UE/EU SECRET INFORMATION

Article 32

Originator consent

If the Commission is not the originator of the classified information for which release or sharing is desired, or of the source material it may contain, the Commission department which holds this classified information shall first seek the originator‘s written consent to release. If the originator cannot be identified, the Commission department holding that classified information shall exercise originator control.

Article 33

Sharing CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information with other Union entities

1. CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information shall only be shared with another Union institution, agency, body or office if the recipient has a need-to-know and the entity has a corresponding legal arrangement with the Commission.

2. Within the Commission, the EUCI Registry managed by the Secretariat-General shall as a general rule be the main point of entry and exit for classified information exchanges with other Union institutions, agencies, bodies and offices. The Commission security authority shall be consulted where there are security, organisational or operational grounds for it to be more appropriate for local EUCI registries to operate as the point of entry and exit for matters within the competence of the department concerned.

Article 34

Exchanging CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information with Member States

1. CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information may be shared with Member States if the recipient has a need-to-know and has been security cleared.

2. Member States' classified information that bears an equivalent national classification marking ([10]) and which has been provided to the Commission shall be afforded the same level of protection as CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information.

Article 35

Exchanging CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information with third countries and international organisations

1. CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information shall only be released to a third country or international organisation if the recipient has a need-to-know and the country or international organisation has an appropriate legal or administrative framework in place, such as a security of information agreement or an administrative arrangement with the Commission. The provisions of such an agreement or arrangement shall prevail over the provisions of this Decision.

2. The EUCI registry managed by the Secretariat-General shall as a general rule act as the main point of entry and exit for all information classified CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET exchanged between the Commission and third countries and international organisations. The Commission security authority shall be consulted where there are security, organisational or operational grounds which make it more appropriate for local EUCI registries to operate as the point of entry and exit for matters within the competence of the department concerned.

3. Any classified information received from a third country or an international organisation shall be registered for security purposes. Staff

shall therefore contact the registry if they receive classified information from outside the usual registry circuit.

4. To ensure traceability, CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information shall be registered:
– when it arrives in or leaves an organisational entity; and
– when it arrives in or leaves a CIS.

5. Such registration may be carried out on paper or in electronic logbooks.

6. Registration procedures for classified information handled within an accredited CIS may be performed by processes within the CIS itself. In that case, the CIS shall include measures to guarantee the integrity of the log records.

7. Classified information received from third countries or international organisations shall be afforded an equivalent level of protection as EUCI bearing the equivalent classification marking as set out in the respective security of information agreement or administrative arrangement.

Article 36

Exceptional ad hoc release of CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information

1. Where the Commission or one of its departments determines that there is an exceptional need to release CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information to a third country, international organisation or an EU entity but no security of information agreement or administrative arrangement is in place, the exceptional *ad hoc* release procedure shall be followed.

2. Commission departments shall contact the Commission security authority, which shall consult the Commission Security Expert Group.

3. After consulting the Commission Security Expert Group, the Commission may, on the basis of a proposal by the member of the Commission responsible for security matters, authorise release of the information concerned.

CHAPTER 6

END OF LIFE FOR CONFIDENTIEL UE/EU CONFIDENTIAL AND SECRET UE/EU SECRET INFORMATION

Article 37

When to downgrade or declassify

1. Information shall remain classified only for as long as it requires protection. Downgrading means a reduction in the level of security classification. Declassification means that the information shall no longer be considered as classified at all. At the time of its creation, the originator shall indicate, where possible, whether the EUCI can be downgraded or declassified on a given date or following a specific event. Otherwise, the originator shall review the information and assess the risks at least every 5 years in order to determine whether the original classification level is still appropriate.

2. Commission documents may also be downgraded or declassified on an *ad hoc* basis, for example following a request for access from the public.

Article 38

Responsibility for downgrading and declassifying

1. CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information shall not be downgraded or declassified without the permission of the originator.

2. The Commission department that creates a classified document shall be responsible for deciding whether it can be downgraded or declassified. Within the Commission, all requests for downgrading and declassifying shall be subject to consultation of the Head of Unit or Director of the originating department. If the department has compiled classified information from various sources it shall first seek the consent of any other parties that provided source material, including in Member States, other EU bodies, third countries or international organisations.

3. Where the originating Commission department no longer exists and its responsibilities have been taken on by another service, the decision on downgrading and declassifying shall be taken by this service. Where the originating department no longer exists and its responsibilities have not been taken on by another service, the decision to downgrade or declassify shall be taken jointly by the Heads of Unit or Directors of the recipient Directorates-General.

4. The department responsible for downgrading or declassifying shall work with its respective registry on the practical arrangements for carrying out downgrading or declassification.

Article 39

Sensitive non-classified information

When reviewing a document results in a decision to declassify, consideration shall be given as to whether the document should bear a sensitive non-classified information distribution marking within the meaning of Article 9 of Decision (EU, Euratom) 2015/443.

Article 40

How to indicate that a document has been downgraded or declassified

1. The original classification marking at the top and bottom of every page shall be visibly crossed out (not removed) using the 'strikethrough' functionality for electronic formats, or manually for print-outs.

2. The first (cover) page shall be stamped as downgraded or declassified and completed with the details of the authority responsible for downgrading or declassifying and the corresponding date.

3. The original recipients of the CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information shall be informed of the downgrading or declassification. The initial recipients shall be responsible for informing any subsequent addressees to whom they have sent or copied the original CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information.

4. The Commission's Historical Archives Service shall be informed of all declassification decisions taken.

5. All translations of classified information shall be subject to the same downgrading or declassification procedures as the original language version.

Article 41

Partial downgrading or declassification of CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information

1. Partial downgrading or declassification shall also be possible (e.g. annexes, some paragraphs only). The procedure shall be identical to that for downgrading or declassifying an entire document.

2. Upon partial declassification ('sanitising') of CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information, a declassified extract shall be produced.

3. The parts that remain classified shall be replaced by:

PART NOT TO BE DECLASSIFIED

either in the body of the text itself, if the part that remains classified is a part of a paragraph, or as a paragraph, if the part that remains classified is a specific paragraph or more than one paragraph.

4. Specific mention shall be made in the text if a complete annex cannot be declassified and has therefore been withheld from the extract.

Article 42

Routine destruction and deletion of CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information

1. The Commission shall not amass large quantities of classified information.

2. Originating departments shall review documents at least every 5 years for destruction or deletion. A review shall take place both for information stored on paper and for information stored in CIS at regular intervals.

3. Staff shall not destroy any hard copy CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET documents that they no longer require, but shall instead ask their Registry Control Officer to destroy the documents, subject to any archiving requirements for the original document.

4. Staff shall not be required to inform the originator if they delete copies of CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET documents.

5. Draft material containing classified information shall be subject to the same disposal methods as finalised classified documents.

6. Only approved shredders shall be used for destroying CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET documents. Level 5 of DIN 66399 shredders are suitable for destroying CONFIDENTIEL UE/EU CONFIDENTIAL documents. Level 6 of DIN 66399 shredders are suitable for destroying SECRET UE/EU SECRET documents.

7. The shred from approved shredders may be disposed of as normal office waste.

8. The Registry Control Officer shall create destruction certificates and update the logbooks and other registration information accordingly.

9. All media and devices containing CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information shall be properly sanitised when they reach the end of their lifetime. The electronic data shall be destroyed or erased from information technology resources and associated storage media in a manner that gives reasonable assurance that the information cannot be recovered. Sanitisation shall remove data from the storage device, and also remove all labels, markings and activity logs.

10. Computer storage media shall be given to the LSO or Local Informatics Security Officer and/or Registry Control Officer for destruction and disposal.

Article 43

Evacuation and destruction of CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information in an emergency

1. The Head of Department shall develop, approve and if necessary activate emergency evacuation and destruction plans to safeguard EUCI that is at significant risk of falling into unauthorised hands during a crisis. In order of priority, and depending on the nature of the emergency, consideration shall be given to:

(1) moving EUCI to an alternative safe place, where possible a Secured Area within the same building;

(2) evacuating EUCI to an alternative safe place, where possible a Secured Area in a different building, where possible a Commission building;

(3) destroying EUCI, where possible using the approved means of destruction.

2. When emergency plans have been activated, priority shall be given to moving or destroying SECRET UE/EU SECRET information first, and any CONFIDENTIEL UE/EU CONFIDENTIAL thereafter.

3. The operational details of emergency evacuation and destruction plans shall themselves be classified as RESTREINT UE/EU RESTRICTED. A copy shall be kept in each safe that stores CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information so as to be accessible in the event of an emergency.

Article 44

Archiving

1. Decisions on whether and when to archive, and the corresponding practical measures to be taken, shall be in accordance with the Commission‘s policy on document management.

2. CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET documents shall not be sent to the Historical Archives of the European Union in Florence.

CHAPTER 7

FINAL PROVISIONS

Article 45

Transparency

This Decision shall be brought to the attention of Commission staff and to all individuals to whom it applies, and shall be published in the *Official Journal of the European Union*.

Article 46

Entry into force

This Decision shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

Done at Brussels, 17 October 2019.

For the Commission,

On behalf of the President,

Günther OETTINGER

Member of the Commission

([1]) OJ L 72, 17.3.2015, p. 41.

([2]) OJ L 72, 17.3.2015, p. 53.

([3]) OJ L 6, 11.1.2017, p. 40.

([4]) Council Decision 2013/488/EU of 23 September 2013 on the security rules for protecting EU classified information (OJ L 274, 15.10.2013, p. 1).

([5]) Commission Decision of 4 May 2016 on an empowerment relating to security, C(2016) 2797 final.

([6]) Pursuant to Article 3 of Decision (EU, Euratom) 2015/444, CONFIDENTIEL UE/

EU CONFIDENTIAL information shall mean ‘information and material the unauthorised disclosure of which could harm the essential interests of the European Union or of one or more of the Member States’.

([7]) Pursuant to Article 3 of Decision (EU, Euratom) 2015/444, SECRET UE/EU SECRET information shall mean ‘information and material the unauthorised disclosure of which could seriously harm the essential interests of the European Union or of one or more of the Member States’.

([8]) As defined in Article 18 of Decision (EU, Euratom) 2015/444.

([9]) As defined in Article 18 of Decision (EU, Euratom) 2015/444.

([10]) The table of equivalence for Member State markings is set out in Annex I to Decision (EU, Euratom) 2015/444.

ANNEX

Categories of staff who may have access to CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information if needed in order to perform their professional tasks

Categories of Commission personnel	Access to C-UE/ EU- C and S-UE/EU-S information	Conditions
Officials	Yes	Vetting + briefing + acknowledge + authorisation + need-to-know
Temporary agents	Yes	Vetting + briefing + acknowledge + authorisation + need-to-know
Contractual agents	Yes	Vetting + briefing + acknowledge + authorisation + need-to-know
Seconded national experts (SNEs)	Yes	Only when cleared by EU Member States prior to taking up their assignment + briefed by the Commission + acknowledge + authorised by the Commission + need-to-know
Trainees	No	No exceptions possible
Any other category of personnel (interim, intra-muros externals etc.)	No	Consult the Commission security authority for any exceptions

2.15. 2017 M. RUGSĖJO 19 D. EUROPOS SĄJUNGOS VYRIAUSIOJO ĮGALIOTINIO UŽSIENIO REIKALAMS IR SAUGUMO POLITIKAI SPRENDIMAS DĖL EUROPOS IŠORĖS VEIKSMŲ TARNYBOS SAUGUMO TAISYKLIŲ ADMIN(2017) 10

2017 m. rugsėjo 19 d. Europos Sąjungos vyriausiojo įgaliotinio užsienio reikalams ir saugumo politikai sprendimas dėl Europos išorės veiksmų tarnybos saugumo taisyklių

ADMIN(2017) 10

(2018/C 126/01)

EUROPOS SĄJUNGOS VYRIAUSIASIS ĮGALIOTINIS UŽSIENIO REIKALAMS IR SAUGUMO POLITIKAI,

atsižvelgdamas į 2010 m. liepos 26 d. Tarybos sprendimą 2010/427/ES, kuriuo nustatoma Europos išorės veiksmų tarnybos ([1]) (*EIVT*) struktūra ir veikimas,

atsižvelgdamas į 2011 m. birželio 15 d. Vyriausiojo įgaliotinio sprendimo dėl Europos išorės veiksmų tarnybos saugumo taisyklių 9 straipsnio 6 dalyje nurodyto komiteto nuomonę ([2]),

kadangi:

(1) EIVT, kaip funkciniu požiūriu savarankiška Europos Sąjungos įstaiga, turėtų turėti saugumo taisykles, kaip numatyta Tarybos sprendimo 2010/427/ES 10 straipsnio 1 dalyje;

(2) Europos Sąjungos vyriausiasis įgaliotinis užsienio reikalams ir saugumo politikai (toliau – vyriausiasis įgaliotinis) turėtų nuspręsti dėl EIVT saugumo taisyklių, kurios apimtų visus saugumo aspektus, susijusius su EIVT veikimu, kad EIVT veiksmingai valdytų riziką, kylančią darbuotojams, už kurių įdarbinimą atsakinga EIVT, jos fiziniams ištekliams, informacijai ir lankytojams, ir kad šiuo atžvilgiu ji vykdytų su rūpestingu elgesiu susijusius įsipareigojimus;

(3) turėtų būti užtikrintas toks darbuotojų, už kurių įdarbinimą atsakinga EIVT, EIVT fizinių išteklių, įskaitant ryšių ir informacijos sistemas, informacijos ir lankytojų apsaugos lygis, kuris atitiktų Tarybos, Komisijos, valstybių narių ir, jei taikytina, tarptautinių organizacijų geriausią praktiką;

(4) EIVT saugumo taisyklės turėtų padėti užtikrinti labiau suderintą visapusišką bendrą sistemą Europos Sąjungos viduje, kad būtų apsaugota ES įslaptinta informacija (toliau – ESĮI), remiantis Europos Sąjungos Tarybos (toliau – Taryba) saugumo taisyklėmis ir Komisijos saugumo nuostatomis ir siekiant kuo didesnio suderinamumo su jomis;

(5) EIVT, Taryba ir Komisija yra įsipareigojusios taikyti lygiaverčius ESĮI apsaugą užtikrinančius saugumo standartus;

(6) šis sprendimas priimamas nedarant poveikio Sutarties dėl Europos Sąjungos veikimo (SESV) 15 ir 16 straipsniams ir jų įgyvendinamiesiems aktams;

(7) reikia nustatyti EIVT saugumo organizavimą ir paskirstyti saugumo užduotis EIVT struktūrose;

(8) vyriausiasis įgaliotinis prireikus turėtų atsižvelgti į atitinkamą valstybių narių, Tarybos generalinio sekretoriato ir Komisijos patirtį;

(9) vyriausiasis įgaliotinis turėtų imtis visų reikiamų priemonių, kad įgyvendintų šias taisykles, padedamas valstybių narių, Tarybos generalinio sekretoriato ir Komisijos;

(10) EIVT generalinis sekretorius yra EIVT saugumo institucija, o 2015 m. rugsėjo 14 d. Europos išorės veiksmų tarnybos generalinio sekretoriaus sprendimo ADMIN(2015) 34 1 straipsnyje numatyta, kad saugumo institucijos saugumo funkcijas, kaip nustatyta EIVT saugumo taisyklėse, vykdo biudžeto ir administracijos generalinis direktorius,

PRIĖMĖ ŠĮ SPRENDIMĄ:

1 straipsnis

Tikslas ir taikymo sritis

Šiuo sprendimu nustatomos Europos išorės veiksmų tarnybos saugumo taisyklės (toliau – *EIVT saugumo taisyklės*).

Pagal 2010 m. liepos 26 d. Tarybos sprendimo 2010/427/ES, kuriuo nustatoma Europos išorės veiksmų tarnybos struktūra ir veikimas, 10 straipsnio 1 dalį jos taikomos visiems EIVT darbuotojams ir visiems Europos Sąjungos delegacijų darbuotojams, nepaisant jų administracinio statuso ar to, kokia administracija juos paskyrė. Jomis taip pat nustatoma bendroji reglamentavimo sistema, kad būtų veiksmingai valdoma rizika, kuri iškyla darbuotojams, už kurių įdarbinimą atsakinga EIVT pagal 2 straipsnį, EIVT patalpoms, fiziniams ištekliams, informacijai ir lankytojams.

2 straipsnis

Apibrėžtys

Šiame sprendime vartojamų terminų apibrėžtys:

a) **EIVT darbuotojai** – EIVT pareigūnai ir kiti tarnautojai, įskaitant valstybių narių diplomatinių tarnybų darbuotojus, kurie paskiriami laikinaisiais darbuotojais, taip pat komandiruoti nacionaliniai ekspertai pagal 2010 m. liepos 26 d. Tarybos sprendimo 2010/427/ES, kuriuo nustatoma Europos išorės veiksmų tarnybos struktūra ir veikimas, 6 straipsnį;

b) **darbuotojai, už kurių įdarbinimą atsakinga EIVT,** – būstinėje ir Europos Sąjungos delegacijose dirbantys EIVT darbuotojai ir kiti Europos Sąjungos delegacijų darbuotojai, nepaisant jų administracinio statuso ar to, kokia administracija juos paskyrė, taip pat, kaip nustatyta šiame sprendime, vyriausiasis įgaliotinis ir, jei taikytina, kiti darbuotojai, kurie dirba EIVT būstinės patalpose;

c) **išlaikytiniai** – darbuotojų, už kurių įdarbinimą Europos Sąjungos delegacijose atsakinga EIVT, šeimos nariai, kurie yra darbuotojų namų ūkio dalyviai, kaip pranešta priimančiosios valstybės užsienio reikalų ministerijai;

d) **EIVT patalpos** – visos EIVT įstaigos, įskaitant pastatus, biurus,

kabinetus ir kitas zonas, taip pat zonos, kuriose saugomos ryšių ir informacinės sistemos (įskaitant zonas, kuriose tvarkoma ES įslaptinta informacija (ESĮI)) ir kuriose EIVT vykdo nuolatinę ar laikiną veiklą;

e) **EIVT saugumo interesai** – darbuotojai, už kurių įdarbinimą atsakinga EIVT, EIVT patalpos, išlaikytiniai, fiziniai ištekliai, įskaitant ryšių ir informacines sistemas, informacija ir lankytojai;

f) **ES įslaptinta informacija (ESĮI)** – bet kuri informacija arba medžiaga, kuriai Europos suteikta ES slaptumo žyma ir kurią neteisėtai atskleidus galėtų būti padaryta tam tikro dydžio žala Europos Sąjungos arba vienos ar kelių valstybių narių interesams;

g) **Europos Sąjungos delegacija** – delegacijos į trečiąsias šalis ir tarptautines organizacijas, kaip nurodyta 2010 m. liepos 26 d. Tarybos sprendimo 2010/427/ES, kuriuo nustatoma Europos išorės veiksmų tarnybos struktūra ir veikimas, 1 straipsnio 4 dalyje.

Kitos terminų apibrėžtys pateiktos atitinkamuose prieduose ir A priedėlyje.

3 straipsnis

Su rūpestingu elgesiu susiję įsipareigojimai

1. EIVT saugumo taisyklėmis siekiama užtikrinti su rūpestingu elgesiu susijusių EIVT įsipareigojimų įgyvendinimą.

2. Su rūpestingu elgesiu susiję EIVT įsipareigojimai yra stropus visų protingų veiksmų vykdymas įgyvendinant priemones, kuriomis siekiama užkirsti kelią pagrįstai, iš anksto numatytai žalai EIVT saugumo interesams.

Jie apima ir saugos, ir saugumo aspektus, įskaitant tuos aspektus, kurie susiję su nepaprastosiomis situacijomis ar krizėmis, kad ir koks būtų jų pobūdis.

3. EIVT, atsižvelgdama į valstybių narių, ES institucijų ar įstaigų ir kitų šalių, kurių darbuotojai dirba Europos Sąjungos delegacijose ir (arba) Europos Sąjungos delegacijų patalpose, su rūpestingu elgesiu susijusius įsipareigojimus, taip pat atvejus, kai tokie įsipareigojimai tenka EIVT (kai Europos Sąjungos delegacijos lankosi pirmiau minėtų kitų šalių patalpose), EIVT su kiekvienu iš šių subjektų sudaro administracinius susitarimus, kuriuose nustatomos jų funkcijos ir pareigos, uždaviniai ir bendradarbiavimo mechanizmai.

4 straipsnis

Fizinis ir infrastruktūros saugumas

1. Visose EIVT patalpose EIVT nustato visas tinkamas fizinio saugumo priemones (laikinas ir nuolatines), įskaitant patekimo kontrolės priemones, kuriomis siekiama apsaugoti EIVT saugumo interesus. Į šias priemones atsižvelgiama projektuojant ir planuojant naujas patalpas, taip pat prieš išsinuomojant esamas patalpas.

2. Šiuo tikslu darbuotojams, už kurių įdarbinimą atsakinga EIVT, ir išlaikytiniams dėl su saugumu susijusių priežasčių tam tikrą laikotarpį ir tam tikrose zonose gali būti nustatyti specialūs įpareigojimai ar apribojimai.

3. 1 ir 2 dalyse nurodytos priemonės turi atitikti įvertintą riziką.

5 straipsnis

Parengties lygiai ir krizinių situacijų valdymas

1. I skirsnio 13 straipsnio 1 dalyje apibrėžta EIVT saugumo institucija atsako už tai, kad būtų parengtos parengties lygių priemonės, tinkamos grėsmėms ir incidentams, turintiems įtakos saugumui EIVT, numatyti ir reaguoti į juos, taip pat už priemones, būtinas krizinėms situacijoms valdyti.

2. 1 dalyje nurodytos parengties lygių priemonės atitinka grėsmės saugumui lygį. Parengties lygiai nustatomi glaudžiai bendradarbiaujant su kitų Europos Sąjungos institucijų, agentūrų ir įstaigų, taip pat valstybės (-ių) narės (-ių), kurioje (-se) yra EIVT patalpų, kompetentingomis tarnybomis.

3. EIVT saugumo institucija yra kontaktinis punktas parengties lygių ir krizių valdymo klausimais.

6 straipsnis

Įslaptintos informacijos apsauga

1. ESĮI apsauga reglamentuojama šio sprendimo, ypač jo A priedo, nuostatomis. Bet kokios ESĮI turėtojas yra atsakingas už tinkamą jos apsaugą.

2. EIVT užtikrina, kad galimybė susipažinti su įslaptinta informacija

būtų suteikta tik asmenims, kurie atitinka A priedo 5 straipsnyje nustatytas sąlygas.

3. Vietos darbuotojų susipažinimo su ESĮI sąlygas taip pat nustato vyriausias įgaliotinis pagal šio sprendimo A priede nustatytas ESĮI apsaugos taisykles.

4. Už saugumą atsakingas EIVT direktoratas tvarko visų darbuotojų, už kurių įdarbinimą atsakinga EIVT, ir visų EIVT rangovų darbuotojų patikimumo pažymėjimo statuso duomenų bazę.

5. Valstybėms narėms nacionaline slaptumo žyma pažymėtą įslaptintą informaciją perdavus į EIVT struktūras ar tinklus, EIVT tą informaciją saugo laikydamasi reikalavimų, taikomų lygiaverčio slaptumo žymos lygio ESĮI, kaip nustatyta šio sprendimo B priedėlyje pateiktoje slaptumo žymų atitikmenų lentelėje.

6. EIVT zonos, kuriose saugoma CONFIDENTIEL UE/EU CONFIDENTIAL arba atitinkamo ar aukštesnio lygio slaptumo žyma pažymėta informacija, įrengiamos kaip saugumo zonos pagal šio sprendimo A II priede nustatytas taisykles ir patvirtinamos EIVT saugumo institucijos.

7. Vyriausiojo įgaliotinio pareigų, susijusių su susitarimais ar administraciniais susitarimais su trečiosiomis valstybėmis ar tarptautinėmis organizacijomis dėl keitimosi ESĮI, vykdymo procedūros aprašytos šio sprendimo A ir A VI prieduose.

8. Generalinis sekretorius nustato sąlygas, kuriomis EIVT gali dalytis savo turima ESĮI su kitomis Europos Sąjungos institucijomis, įstaigomis, tarnybomis ar agentūromis. Tam sukuriama atitinkama sistema, be kita ko, prireikus tuo tikslu sudarant tarpinstitucinius ar kitokius susitarimus.

9. Pagal tokią sistemą užtikrinama, kad ESĮI būtų taikoma jos slaptumo žymos lygį atitinkanti apsauga, laikantis pagrindinių principų bei būtiniausių standartų, lygiaverčių nustatytiesiems šiame sprendime.

7 straipsnis

Saugumo incidentai ir nepaprastosios situacijos

1. Siekdama laiku ir veiksmingai reaguoti į saugumo incidentus, EIVT nustato pranešimų apie tokius incidentus ir nepaprastąsias situacijas procedūrą, kuria turi būti galima pasinaudoti dvidešimt keturias va-

landas per parą, septynias dienas per savaitę ir kuri apima visus saugumo incidentus ir grėsmes EIVT saugumo interesams (pvz., avarijas, konfliktus, piktavališkus veiksmus, nusikalstamus veiksmus, žmonių grobimą, įkaitų ėmimą, su sveikata susijusias nepaprastąsias situacijas, ryšių ir informacijos sistemos incidentus, kibernetinius išpuolius ir kt.).

2. EIVT būstinė, Europos Sąjungos delegacijos, Taryba, Komisija, ES specialieji įgaliotiniai ir valstybės narės tarpusavyje nustato ryšių kanalus, kurie naudojami esant nepaprastosioms situacijoms ir padeda valdyti su personalu susijusius saugumo incidentus ir jų padarinius, įskaitant nenumatytų atvejų planavimą.

3. Šį saugumo incidentų valdymą, be kita ko, sudaro:

– veiksmingos pagalbos priimant sprendimus dėl saugumo incidentų, susijusių su personalu, įskaitant sprendimus dėl misijų atšaukimo ar pristabdymo, procedūros;
– darbuotojų susigrąžinimo politika ir procedūros (pvz., dingus, pagrobus ar paėmus įkaitais darbuotojus), atsižvelgiant į konkrečią valstybių narių, ES institucijų ir EIVT atsakomybę šiuo klausimu. Dėl konkrečių pajėgumų poreikio vykdant šiuos veiksmus sprendžiama atsižvelgiant į išteklius, kuriuos gali suteikti valstybės narės.

4. EIVT nustato atitinkamą pranešimų apie saugumo incidentus Europos Sąjungos delegacijose teikimo administracinę tvarką. Jei reikia, informuojamos valstybės narės, Komisija, visos kitos atitinkamos institucijos, taip pat atitinkami Saugumo komitetai.

5. Incidentų valdymo procesai reguliariai išbandomi ir peržiūrimi.

8 straipsnis

Ryšių ir informacinių sistemų saugumas

1. Ryšių ir informacijos sistemose (toliau – RIS) EIVT saugo tvarkomą informaciją, užtikrindama konfidencialumą, vientisumą, prieinamumą, autentiškumą ir atsakomybės už veiksmus prisiėmimą.

2. Visų EIVT turimų ar naudojamų RIS apsaugos taisykles, saugumo gaires ir saugumo programą tvirtina EIVT saugumo institucija.

3. Šios taisyklės, politika ir programa turi atitikti atitinkamas Tarybos, Komisijos ir, jei taikytina, valstybių narių saugumo strategijas, o jų įgyvendinimas turi būti glaudžiai koordinuojamas su šiais subjektais.

4. Visos RIS, kuriose tvarkoma įslaptinta informacija, turi būti akre-

dituojamos. EIVT, konsultuodamasi su Tarybos generaliniu sekretoriatu ir Komisija, taiko saugumo akreditavimo valdymo sistemą.

5. Tais atvejais, kai EIVT tvarkomos ESĮI apsauga užtikrinama naudojant šifravimo priemones, tokias priemones tvirtina EIVT kriptografijos patvirtinimo institucija, gavusi atitinkamą Tarybos saugumo komiteto rekomendaciją.

6. EIVT saugumo institucija įsteigia šias informacijos saugumo užtikrinimo institucijas (tokio dydžio, koks reikalingas):
a) informacijos saugumo užtikrinimo instituciją;
b) TEMPEST instituciją;
c) kriptografijos patvirtinimo instituciją;
d) kriptografijos platinimo instituciją.

7. Atitinkamoms sistemoms tvarkyti EIVT saugumo institucija įsteigia šias institucijas:
a) saugumo akreditavimo instituciją;
b) informacijos saugumo užtikrinimo operacinę instituciją.

8. Šio straipsnio įgyvendinimo nuostatos, susijusios su ESĮI apsauga, išdėstytos A ir A IV prieduose.

9 straipsnis

Įslaptintos informacijos saugumo pažeidimai ir neteisėtas atskleidimas

1. Saugumo pažeidimu laikomas šiame sprendime nustatytoms saugumo taisyklėms ir (arba) saugumo strategijoms ar gairėms, kuriose nustatytos šių taisyklių įgyvendinimo priemonės (patvirtintos pagal 21 straipsnio 1 dalį), priešingas veiksmas arba neveikimas.

2. Įslaptintos informacijos neteisėtas atskleidimas įvyksta tada, kai ji visiškai ar iš dalies atskleidžiama leidimo neturintiems asmenims ar subjektams.

3. Apie bet kokį faktinį ar įtariamą saugumo pažeidimą ir apie bet kokį faktinį ar įtariamą įslaptintos informacijos neteisėtą atskleidimą nedelsiant pranešama už saugumą atsakingam EIVT direktoratui, kuris imasi tinkamų priemonių, kurios nurodytos A priedo 11 straipsnyje.

4. Bet kuriam asmeniui, kuris pažeidė šiame sprendime nustatytas saugumo taisykles ar neteisėtai atskleidė įslaptintą informaciją, gali būti taikomos drausminės ir (arba) teisinės priemonės pagal taikomus teisės ak-

tus, taisykles ir nuostatas, kaip nustatyta A priedo 11 straipsnio 3 dalyje.

10 straipsnis

Saugumo incidentų, pažeidimų ir (arba) neteisėto informacijos atskleidimo atvejų tyrimas ir taisomieji veiksmai

1. Nedarant poveikio Tarnybos nuostatų ([3]) 86 straipsniui (drausminės priemonės) ir IX priedui, patikimumo patikrinimus gali atlikti už saugumą atsakingas EIVT direktoratas:

a) ESĮI, Euratomo įslaptintos informacijos arba neskelbtinos neįslaptintos informacijos galimo nutekėjimo, netinkamo naudojimo arba neteisėto atskleidimo atveju;
b) kai siekiama atremti priešiškų žvalgybos tarnybų išpuolius prieš EIVT ir jos darbuotojus;
c) kai siekiama atremti teroristinius išpuolius prieš EIVT ir jos darbuotojus;
d) kibernetinių incidentų atveju;
e) kitų incidentų, įskaitant įtariamas nusikalstamas veikas, turinčių arba galinčių turėti poveikį bendram EIVT saugumui, atveju.

2. Už saugumą atsakingas EIVT direktoratas, padedamas valstybių narių ir (arba) atitinkamais atvejais kitų ES institucijų ir, prireikus, gavęs EIVT saugumo institucijos leidimą, atlieka tyrimų metu nustatytus reikiamus taisomuosius veiksmus tada, kai tai tikslinga.

Įgaliojimai atlikti ir koordinuoti EIVT patikimumo patikrinimus gali būti suteikti tik darbuotojams, turintiems leidimą pagal asmeninius įgaliojimus, kuriuos jiems suteikė EIVT saugumo institucija, ir turi būti atsižvelgiama į tų darbuotojų dabartines pareigas.

3. Tyrimus vykdantys asmenys gali naudotis visa informacija, kuri reikalinga tokiems tyrimams vykdyti, ir šioje srityje gauna visapusišką visų EIVT tarnybų ir darbuotojų pagalbą.

Tyrimus vykdantys asmenys gali imtis atitinkamų veiksmų, kad apsaugotų įrodymų pėdsakus tokiu būdu, kuris atitinka tiriamo atvejo rimtumą.

4. Jei reikia naudotis informacija, kuri susijusi su asmens duomenimis, įskaitant ryšių ir informacinėse sistemose saugomus asmens duomenis, ši galimybė susipažinti su duomenimis suteikiama laikantis Reglamento (EB) Nr. 45/2001 ([4]).

5. Jei būtina sukurti tyrimo duomenų bazę, kurioje ketinama saugoti asmens duomenis, apie tai pranešama Europos duomenų apsaugos priežiūros pareigūnui (EDAPP), kaip nustatyta pirmiau minėtame reglamente.

11 straipsnis

Saugumo rizikos valdymas

1. Siekdama nustatyti savo apsaugos poreikius, EIVT, glaudžiai bendradarbiaudama su Komisijos saugumo direktoratu ir, jei reikia, su Tarybos generalinio sekretoriato Saugumo tarnyba, parengia išsamią saugumo rizikos vertinimo metodiką.

2. EIVT saugumo interesams kylančios rizikos valdymas yra procesas. Šio proceso tikslas – nustatyti žinomą saugumo riziką, apibrėžti saugumo priemones tokiai rizikai sumažinti iki priimtino lygio ir taikyti šias priemones laikantis nuodugnios apsaugos sąvokos. Reguliariai atliekamas tokių priemonių efektyvumo ir rizikos lygio vertinimas.

3. Šiame sprendime nustatytos funkcijos, pareigos ir uždaviniai nepažeidžia kiekvieno darbuotojo, už kurio įdarbinimą atsakinga EIVT, pareigų; ES darbuotojai, esantys misijose trečiosiose šalyse, priimdami sprendimus dėl savo saugos ir saugumo privalo vadovautis sveika nuovoka ir protingumo principais, taip pat privalo laikytis visų taikytinų saugumo taisyklių, nuostatų, procedūrų ir instrukcijų.

4. Siekiant užtikrinti pavojų saugumui prevenciją ir kontrolę, įgaliotieji darbuotojai gali atlikti asmenų, kurie patenka į šio sprendimo taikymo sritį, patikrinimus, kad nustatytų, ar, tokiems asmenims leidus patekti į EIVT patalpas arba prieiti prie jos informacijos, kyla grėsmė saugumui. Tuo tikslu, laikydamiesi Reglamento (EB) Nr. 45/2001, atitinkami įgaliotieji darbuotojai gali:

a) naudoti bet kokį EIVT prieinamą informacijos šaltinį, atsižvelgdami į informacijos šaltinio patikimumą;

b) tinkamai pagrįstais atvejais susipažinti su asmens byla arba EIVT turimais joje dirbančių arba ketinamų įdarbinti asmenų arba rangovo darbuotojų duomenimis.

5. EIVT imasi visų protingų priemonių, kad užtikrintų savo saugumo interesų apsaugą ir kad užkirstų kelią pagrįstai, iš anksto numatomai žalai šiems saugumo interesams.

6. ESĮI apsaugai užtikrinti skirtos EIVT saugumo priemonės visą savo gyvavimo ciklą turi atitikti jos slaptumo žymos lygį, informacijos ar medžiagos formą ir kiekį, patalpų, kuriose laikoma ESĮI, vietos ir konstrukcijos reikalavimus ir grėsmę, įskaitant vietos lygiu įvertintą piktavališkos ir (arba) nusikalstamos veiklos, įskaitant šnipinėjimą, sabotažą ar terorizmą, keliamą grėsmę.

12 straipsnis

Informavimas apie saugumą ir saugumo mokymas

1. EIVT saugumo institucija užtikrina, kad būtų parengtos ir įgyvendinamos informavimo apie saugumą ir saugumo mokymo programos ir kad darbuotojams, už kurių įdarbinimą atsakinga EIVT ir, jei taikytina, jų išlaikytiniams, būtų pateikta informacinė medžiaga ir surengti mokymai, kurie atitinka jų darbo ar gyvenamosiose vietose esančią riziką.

2. Darbuotojai, prieš jiems suteikiant leidimą susipažinti su ESĮI, o vėliau – reguliariai, informuojami apie pareigą saugoti ESĮI pagal 6 straipsnyje pateiktas taisykles ir jie ją patvirtina.

13 straipsnis

Saugumo organizavimas EIVT

1. Generalinis sekretorius yra EIVT saugumo institucija. Vykdydamas šias funkcijas generalinis sekretorius užtikrina, kad:

a) sprendžiant visus EIVT veiklai svarbius saugumo klausimus, įskaitant klausimus, susijusius su pavojų EIVT saugumo interesams pobūdžiu ir apsaugos nuo jų priemonėmis, saugumo priemonės būtų derinamos su valstybių narių kompetentingomis institucijomis, Tarybos generaliniu sekretoriatu, Komisija ir, jei reikia, su trečiosiomis valstybėmis ar tarptautinėmis organizacijomis;
b) į saugumo aspektus būtų visiškai atsižvelgiama bet kokioje EIVT veikloje nuo pat jos pradžios;
c) galimybė susipažinti su įslaptinta informacija būtų suteikta tik asmenims, kurie atitinka A priedo 5 straipsnyje nustatytas sąlygas;

d) būtų sukurta registratūrų sistema, kuri užtikrintų, kad CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio lygio slaptumo žyma pažymėta informacija EIVT, pateikus ją ES valstybėms narėms, ES institucijoms, įstaigoms ir agentūroms ar kitiems įgaliotiesiems gavėjams, būtų tvarkoma pagal šį sprendimą. Visa ESĮI, kurią EIVT pateikė trečiosioms valstybėms ir tarptautinėms organizacijoms, ir visa įslaptinta informacija, gauta iš trečiųjų valstybių ir tarptautinių organizacijų, saugoma atskirame registre;

e) būtų vykdomi 16 straipsnyje nurodyti saugumo patikrinimai;

f) būtų vykdomi visų faktinių ar įtariamų saugumo pažeidimų, taip pat visų EIVT turimos ar parengtos įslaptintos informacijos faktinio ar įtariamo neteisėto atskleidimo arba praradimo atvejų tyrimai ir kad vykdant šiuos tyrimus būtų prašoma atitinkamų saugumo institucijų pagalbos;

g) būtų parengti atitinkami incidentų ir padarinių valdymo planai ir mechanizmai (siekiant laiku ir veiksmingai reaguoti į saugumo incidentus);

h) būtų vykdomos atitinkamos priemonės, jei asmenys nesilaiko šio sprendimo reikalavimų;

i) būtų nustatytos atitinkamos fizinės ir organizacinės priemonės, skirtos EIVT saugumo interesams apsaugoti.

Šiuo klausimu EIVT saugumo institucija:

– nustato Europos Sąjungos delegacijų saugumo kategorijas, konsultuodamasi su Komisija;

– pasikonsultavusi su vyriausiuoju įgaliotiniu sprendžia, kada evakuoti Europos Sąjungos delegacijos darbuotojus, jei tai būtina siekiant užtikrinti saugumą;

– priima sprendimus dėl išlaikytinių apsaugos priemonių, jei reikia, atsižvelgdamas į susitarimus su ES institucijomis, nurodytus 3 straipsnio 3 dalyje;

– tvirtina šifruotų ryšių politiką, konkrečiau – šifravimo produktų diegimo programą ir mechanizmą.

2. EIVT saugumo institucijai padeda *DGBA*, už saugumą atsakingas EIVT direktorius ir atitinkamais atvejais už bendrą saugumo ir gynybos politiką (BSGP) ir už reagavimą į krizes atsakingas generalinio sekretoriaus pavaduotojas.

3. Jei reikia, generalinis sekretorius, kaip EIVT saugumo institucija, gali deleguoti su šiais aspektais susijusias užduotis.

4. Visų padalinių ir skyrių vadovai atsakingi už ESĮI apsaugos taisy-

klių įgyvendinimą atitinkamuose padaliniuose ir skyriuose.

Visų padalinių ir skyrių vadovai ne tik vykdo pirmiau nurodytas funkcijas, bet ir skiria darbuotojus į padalinio saugumo koordinatorių pareigas. Šių koordinatorių ištekliai atitinka atitinkamo padalinio ar skyriaus tvarkomos ESĮI kiekį.

Jei reikia, padalinio saugumo koordinatoriai padeda savo padalinio ar skyriaus vadovui, vykdydami šiuos su saugumu susijusius uždavinius:

a) rengia papildomus saugumo reikalavimus, atitinkančius specialius padalinio ar skyriaus poreikius;
b) reguliariai teikia saugumo informaciją savo padalinio ar skyriaus darbuotojams;
c) užtikrina, kad jų padalinyje ar skyriuje būtų laikomasi principo „būtina žinoti“;
d) tvarko ir atnaujina saugos kodų ir raktų sąrašą;
e) užtikrina saugumo procedūrų ir saugumo priemonių vykdymą;
f) praneša apie visus saugumo pažeidimus ir (arba) ESĮI neteisėto atskleidimo atvejus savo direktoriui ir už saugumą atsakingam direktoratui;
g) apklausia iš EIVT atleidžiamus darbuotojus;
h) per savo vadovus reguliariai teikia ataskaitas dėl padalinio ar skyriaus saugumo reikalų;
i) palaiko ryšius saugumo klausimais su už saugumą atsakingu EIVT direktoratu.

Apie visus veiksmus ar problemas, kurios gali turėti poveikį saugumui, laiku pranešama už saugumą atsakingam EIVT direktoratui.

5. Delegacijos vadovas atsakingas už visų saugumo priemonių įgyvendinimą atitinkamoje Europos Sąjungos delegacijoje.

1. EIVT turi už saugumą atsakingą direktoratą. Jis:

a) valdo, koordinuoja, prižiūri ir (arba) įgyvendina visas saugumo priemones visose EIVT patalpose ir būstinėje, ES ir trečiosiose valstybėse;
b) užtikrina visų veiksmų, kurie gali turėti poveikį EIVT saugumo interesų apsaugai, suderinamumą su šiuo sprendimu ir jo įgyvendinimo nuostatomis;
c) veikia kaip vyriausiojo įgaliotinio, EIVT saugumo institucijos ir generalinio sekretoriaus pavaduotojo pagrindinis patarėjas visais su saugumu susijusiais klausimais;

d) veikia padedant valstybių narių kompetentingoms tarnyboms pagal Tarybos sprendimo 2010/427/ES, kuriuo nustatoma Europos išorės veiksmų tarnybos struktūra ir veikimas, 10 straipsnio 3 dalį;
e) EIVT saugumo akreditavimo institucijai padeda vykdyti ryšių ir informacijos sistemų, kuriose tvarkoma ESĮI, ir patalpų, kuriose ketinama leisti tvarkyti ir saugoti ESĮI, bendrosios saugumo aplinkos (BSA) ir vietos saugumo aplinkos (VSA) fizinio saugumo vertinimus.

2. Už saugumą atsakingas EIVT direktorius yra atsakingas už:
a) bendros EIVT saugumo interesų apsaugos užtikrinimą;
b) saugumo taisyklių rengimą, peržiūrą ir atnaujinimą, taip pat saugumo priemonių koordinavimą su valstybių narių kompetentingomis institucijomis ir, jei reikia, su trečiųjų valstybių kompetentingomis institucijomis ir tarptautinėmis organizacijomis, kurios su ES susietos saugumo sutartimis ir (arba) susitarimais;
c) dalyvavimą EIVT saugumo komiteto veikloje, kaip nustatyta šio sprendimo 15 straipsnio 1 dalyje;
d) jei reikia, bendradarbiavimą su visais partneriais ar kitomis institucijomis, jei nurodytos b punkte;
e) prioritetų nustatymą ir pasiūlymų dėl būstinės ir Europos Sąjungos delegacijų saugumo biudžeto valdymo teikimą.

3. Už saugumą atsakingo EIVT direktorato vadovas:
a) užtikrina, kad saugumo pažeidimai ir neteisėto informacijos atskleidimo atvejai būtų registruojami ir, jei reikia, būtų pradėti ir vykdomi tyrimai;
b) reguliariai ir pagal poreikį susitinka su Tarybos generalinio sekretoriato saugumo direktoriumi ir Komisijos saugumo direktorato direktoriumi aptarti bendrų klausimų.

4. Už saugumą atsakingas EIVT direktoratas užmezga ryšius ir glaudžiai bendradarbiauja su:
– už saugumą atsakingais valstybių narių užsienio reikalų ministerijų padaliniais;
– valstybių narių nacionalinėmis saugumo institucijomis (NSI) ir (arba) kitomis kompetentingomis saugumo institucijomis, siekdamas gauti jų pagalbą dėl informacijos, kuri reikalinga pavojams ir grėsmei, kuri iškyla EIVT, jos darbuotojams, veiklai, turtui, ištekliams ir įslaptintai informacijai įprastoje veiklos vietoje, įvertinti;
– valstybių narių ar priimančiųjų valstybių, kurių teritorijoje EIVT gali vykdyti savo veiklą, kompetentingomis saugumo institucijomis visais klausimais, susijusiais su EIVT darbuotojų, veiklos, turto, išteklių ir įslaptintos informacijos apsauga jų teritorijoje;

– Tarybos generalinio sekretoriato Saugumo tarnyba ir Komisijos Žmogiškųjų išteklių ir saugumo generalinio direktorato Saugumo direktoratu ir, jei reikia, kitų ES institucijų, įstaigų ir agentūrų saugumo padaliniais;
– trečiųjų valstybių ar tarptautinių organizacijų saugumo padaliniais, siekdamas bet kokių veiksmų naudingo koordinavimo;
– valstybių narių NSI visais klausimais, susijusiais su ESĮI apsauga.

1. Delegacijos vadovas atsakingas už visų priemonių, susijusių su EIVT saugumo interesų apsauga Europos Sąjungos delegacijos patalpose pagal Europos Sąjungos delegacijos kompetenciją, įgyvendinimą vietoje ir valdymą.

Delegacijos vadovas, jei reikia, konsultuodamasis su priimančiosios valstybės kompetentingomis institucijomis, vykdo visus tinkamus veiksmus, siekdamas užtikrinti, kad būtų nustatytos atitinkamos fizinės ir organizacinės priemonės, reikalingos šiam tikslui pasiekti.

Delegacijos vadovas nustato saugumo procedūras, skirtas išlaikytiniams pagal 2 straipsnio c punktą apsaugoti, jei reikia, atsižvelgdamas į visus administracinius susitarimus, nurodytus 3 straipsnio 3 dalyje. Delegacijos vadovas apie visus į jo kompetencijos sritį patenkančius su saugumu susijusius klausimus praneša už saugumą atsakingo EIVT direktorato vadovui.

Vykdyti šiuos uždavinius jam padeda už saugumą atsakingas EIVT direktoratas, Europos Sąjungos delegacijos saugumo valdymo grupė, kurią sudaro saugumo uždavinius ir funkcijas vykdantys darbuotojai, o prireikus – ir saugumo darbuotojai.

Europos Sąjungos delegacija užmezga reguliarius ryšius ir glaudžiai bendradarbiauja saugumo klausimais su valstybių narių diplomatinėmis atstovybėmis.

2. Be to, delegacijos vadovas:
– remdamasis bendrosiomis standartinėmis operacijų procedūromis, nustato išsamius Europos Sąjungos delegacijos saugumo ir nenumatytų atvejų planus;
– Europos Sąjungos delegacijos veikloje taiko veiksmingą, be pertraukų veikiančią saugumo incidentų ir nepaprastųjų situacijų valdymo sistemą;
– užtikrina, kad visi Europos Sąjungos delegacijos darbuotojai būtų apdrausti atsižvelgiant į konkrečios veiklos sąlygas;

– užtikrina, kad į Europos Sąjungos delegacijos pradinį mokymą, kuris teikiamas visiems Europos Sąjungos delegacijos darbuotojams, prieš jiems atvykstant ar atvykus į Europos Sąjungos delegaciją, būtų įtrauktas saugumo aspektas;
– užtikrina, kad būtų įgyvendintos visos rekomendacijos, pateiktos atliktus saugumo vertinimus, ir reguliariai teikia rašytines ataskaitas dėl jų įgyvendinimo ir kitų saugumo klausimų EIVT saugumo institucijai.

3. Delegacijos vadovas atsakingas ir atskaitingas ne vien už saugumo valdymo ir organizacijos atsparumo užtikrinimą – delegacijos vadovas gali paskirti vykdyti jo saugumo uždavinius delegacijos saugumo koordinatoriui, kuris yra ir delegacijos vadovo pavaduotojas (DVP) (jei toks nepaskirtas – tinkamam darbuotojui).

DVP gali būti patikėtos šios pareigos:
– koordinuoti saugumo funkcijas Europos Sąjungos delegacijoje;
– saugumo klausimais bendradarbiauti su priimančiosios valstybės kompetentingomis institucijomis ir atitinkamais valstybių narių ambasadų ir diplomatinių atstovybių darbuotojais;
– įgyvendinti saugumo valdymo procedūras, susijusias su EIVT saugumo interesais, įskaitant ESĮI apsaugą;
– užtikrinti, kad būtų laikomasi saugumo taisyklių ir instrukcijų;
– informuoti darbuotojus apie jiems taikomas saugumo taisykles ir apie konkrečius priimančiojoje valstybėje kylančius pavojus;
– teikti užklausas už saugumą atsakingam EIVT direktoratui dėl darbuotojų, kuriems taikoma asmens patikimumo patikrinimo (APP) procedūra;
– nuolat informuoti delegacijos vadovą, regiono saugumo pareigūną (RSP) ir už saugumą atsakingą EIVT direktoratą apie incidentus ar pokyčius srityje, kuri susijusi su EIVT saugumo interesų apsauga.

4. Delegacijos vadovas gali deleguoti administracinio ar techninio pobūdžio saugumo uždavinius administracijos vadovui ir kitiems delegacijos darbuotojams.

5. Europos Sąjungos delegacijai padeda RSP. RSP Europos Sąjungos delegacijose, atitinkančiose geografinius regionus, už kuriuos jie atsakingi, vykdo toliau nurodytas funkcijas.

Esant tam tikroms aplinkybėms, kai tai būtina dėl esamos saugumo padėties, specialus RSP gali būti paskirtas į konkrečią Europos Sąjungos delegaciją kaip nuolatinis darbuotojas.

Už saugumą atsakingo EIVT direktorato sprendimu RSP gali būti paskirtas į vietą, kuri yra ne jo atsakomybės zonoje, įskaitant būstinę, arba, atsižvelgiant į saugumo padėtį, į bet kokią šalį eiti nuolatines pareigas.

6. RSP veiklą tiesiogiai kontroliuoja EIVT būstinės tarnyba, atsakinga už saugumą vietoje, tačiau administracinę kontrolę dalijasi jų darbo vietos delegacijos vadovas ir už saugumą vietoje atsakinga būstinės tarnyba. RSP padeda delegacijos vadovui ir Europos Sąjungos delegacijos darbuotojams rengti ir įgyvendinti visas fizines, organizacines ir procedūrines priemones, susijusias su Europos Sąjungos delegacijos saugumu.

7. RSP konsultuoja delegacijos vadovą ir Europos Sąjungos delegacijos darbuotojus ir jiems padeda. Jei reikia ir tais atvejais, kai RSP yra nuolatinis darbuotojas, jis turėtų padėti Europos Sąjungos delegacijai vykdyti saugumo valdymo ir įgyvendinimo funkcijas, įskaitant saugumo sutarčių parengimą, akreditacijų ir patikimumo pažymėjimų tvarkymą.

14 straipsnis

BSGP operacijos ir ES specialieji įgaliotiniai

Už saugumą atsakingas EIVT direktoratas padeda ir pataria Krizių valdymo ir planavimo direktorato direktoriui, Europos Sąjungos karinio štabo (EUMS) generaliniam direktoriui, Civiliniam operacijų vadui, kuris vadovauja Civilinių operacijų planavimo ir vykdymo centrui (CPCC) ir ES karinių operacijų vadams BSGP operacijų saugumo klausimais, o ES specialiesiems įgaliotiniams – su jų mandatu susijusiais saugumo klausimais. Šios nuostatos papildo atitinkamas specialiąsias Tarybos strategijų nuostatas.

15 straipsnis

EIVT saugumo komitetas

1. Įsteigiamas EIVT saugumo komitetas.

Jam pirmininkauja EIVT saugumo institucija arba paskirtasis delegatas. Saugumo komitetas posėdžiauja pirmininko nurodymu ar bet kokio komiteto nario prašymu. Už saugumą atsakingas EIVT direktoratas padeda pirmininkui vykdyti šią funkciją ir, jei reikia, teikia administracinę pagalbą Komiteto veiklai.

2. EIVT saugumo komitetą sudaro šių subjektų atstovai:

– visų valstybių narių;
– Tarybos generalinio sekretoriato Saugumo tarnybos;
– Komisijos Žmogiškųjų išteklių ir saugumo generalinio direktorato Saugumo direktorato.

Valstybės narės delegaciją EIVT saugumo komitete gali sudaryti šių subjektų atstovai:
– nacionalinės saugumo institucijos ir (arba) paskirtosios saugumo institucijos;
– už saugumą atsakingų užsienio reikalų ministerijos padalinių.

3. Jei reikia, komiteto atstovai gali dirbti kartu su ekspertais ir naudotis jų konsultacijomis. Gali būti pakviesti kitų ES institucijų, agentūrų ar įstaigų atstovai, kai nagrinėjami šių institucijų saugumo požiūriu svarbūs klausimai.

4. Nepažeidžiant tolesnės 5 dalies, EIVT saugumo komitetas teikia pagalbą EIVT (konsultuoja) visais klausimais, kurie svarbūs EIVT veiklai, būstinei ir Europos Sąjungos delegacijoms.

Nepažeidžiant tolesnės 5 dalies, EIVT saugumo komitetas:
a) yra konsultuojamas šiais klausimais:

– saugumo strategijų, gairių, koncepcijų ar kitų su saugumu susijusių metodologinių dokumentų, ypač dokumentų, susijusių su įslaptintos informacijos apsauga ir priemonėmis, kurios numatytos, jei EIVT darbuotojai nesilaiko saugumo taisyklių;

– techninių saugumo aspektų, kurie gali daryti poveikį vyriausiojo įgaliotinio sprendimui teikti rekomendaciją Tarybai dėl derybų dėl susitarimų dėl informacijos saugumo, kurios nurodytos A priedo 10 straipsnio 1 dalies a punkte, pradžios;

– visų šio sprendimo pakeitimų;

b) gali būti konsultuojamas klausimais ar informuojamas apie klausimus, susijusius su EIVT būstinės ir Europos Sąjungos delegacijų darbuotojų bei turto saugumu, nepažeidžiant 3 straipsnio 3 dalies;
c) informuojamas apie visus EIVT įvykusius ESĮI neteisėto atskleidimo ar praradimo atvejus.

5. Visiems šiame sprendime ir jo A priede pateiktų ESĮI apsaugos taisyklių pakeitimams turi vieningai pritarti valstybės narės, atstovaujamos EIVT saugumo komitete. Toks vieningas pritarimas reikalingas priimant šiuos sprendimus:
– pradedant derybas dėl administracinių susitarimų, nurodytų A priedo 10 straipsnio 1 dalies b punkte;

– esant išskirtinėms aplinkybėms, nurodytoms A VI priedo 9, 11 ir 12 dalyse, suteikiant įslaptintą informaciją;
– esant aplinkybėms, nurodytoms A priedo 10 straipsnio 6 dalies paskutiniame sakinyje, prisiimant įslaptintos informacijos rengėjo atsakomybę.

Kai prašoma vieningai pritarti sprendimui, ši sąlyga laikoma įvykdyta, kai valstybių narių delegacijos per komiteto posėdžius nepateikia jokių prieštaravimų.

6. EIVT saugumo komitetas visiškai atsižvelgia į galiojančias Tarybos ir Komisijos saugumo strategijas ir gaires.

7. EIVT saugumo komitetas gauna metinių EIVT patikrinimų sąrašą ir atliktų patikrinimų ataskaitas.

8. Posėdžių organizavimas:
– EIVT saugumo komitetas posėdžiauja bent du kartus per metus. Pirmininkui įsakius arba paprašius Komiteto nariams, gali būti surengti papildomi posėdžiai. Tai gali būti viso formato arba NSI/PSI arba MFA saugumo formato posėdžiai.
– EIVT saugumo komitetas savo veiklą organizuoja taip, kad galėtų teikti rekomendacijas konkrečių saugumo sričių klausimais. Jei reikia, komitetas gali įsteigti kitus ekspertų pogrupius. Šis komitetas apibrėžia tokių ekspertų pogrupių įgaliojimus, o šie pogrupiai teikia jam savo veiklos ataskaitas.
– Už saugumą atsakingas EIVT direktoratas yra atsakingas ir už klausimų diskusijoms rengimą. Kiekvienam posėdžiui pirmininkas parengia preliminarią darbotvarkę. Komiteto nariai gali siūlyti diskutuoti apie kitus klausimus.

16 straipsnis

Saugumo patikrinimai

1. EIVT saugumo institucija užtikrina reguliarų saugumo patikrinimų vykdymą EIVT būstinėje ir Europos Sąjungos delegacijose, siekiant įvertinti saugumo priemonių tinkamumą ir patikrinti, kaip laikomasi šio sprendimo nuostatų. Jei reikia, už saugumą atsakingas EIVT direktoratas gali paskirti papildomus ekspertus, kurie dalyvautų saugumo patikrinimuose, kurie vykdomi ES agentūrose ir įstaigose, įsteigtose pagal ES sutarties V antraštinės dalies 2 skyrių.

2. EIVT saugumo patikrinimai vykdomi vadovaujant už saugumą at-

sakingam EIVT direktoratui ir, jei reikia, padedant kitų ES institucijų ar valstybių narių saugumo ekspertams, ypač kalbant apie 3 straipsnio 3 dalyje nurodytus susitarimus.

3. Jei reikia, EIVT gali atsižvelgti į valstybių narių, Tarybos generalinio sekretoriato ir Europos Komisijos patirtį.

Jei reikia, į Europos Sąjungos delegacijos saugumo patikrinimą gali būti pakviesti dalyvauti atitinkami valstybių narių misijų trečiosiose valstybėse saugumo ekspertai ir (arba) diplomatinių atstovybių saugumo padalinių atstovai.

4. Šio straipsnio įgyvendinimo nuostatos, susijusios su ESĮI apsauga, išdėstytos A III priede.

17 straipsnis

Įvertinimo vizitai

Įvertinimo vizitai rengiami siekiant įsitikinti, kad trečiojoje valstybėje arba tarptautinėje organizacijoje taikomos ESĮI, kuria keičiamasi pagal A priedo 10 straipsnio 1 dalies b punkte nurodytą administracinį susitarimą, apsaugos priemonės yra veiksmingos.

Už saugumą atsakingas EIVT direktoratas gali paskirti papildomus ekspertus, kurie dalyvautų įvertinimo vizitų metu trečiosiose valstybėse ar tarptautinėse organizacijose, su kuriomis ES sudarė susitarimus dėl informacijos saugumo, nurodytus A priedo 10 straipsnio 1 dalies a punkte.

18 straipsnis

Veiklos tęstinumo planavimas

Už saugumą atsakingas EIVT direktoratas padeda EIVT saugumo institucijai valdyti su saugumu susijusius EIVT veiklos tęstinumo procesų aspektus, kurie yra bendro EIVT veiklos tęstinumo planavimo dalis.

19 straipsnis

Kelionės patarimai, skirti misijoms, kurios vykdomos ne ES

Už saugumą atsakingas EIVT direktoratas užtikrina, kad būtų teikiami kelionės patarimai dėl darbuotojų, už kurių įdarbinimą atsakin-

ga EIVT, misijų į ne ES šalis, ir sutelkia visų atitinkamų EIVT tarnybų, ypač SITROOM, INTCEN, geografinių padalinių ir Europos Sąjungos delegacijų, išteklius.

Pateikus prašymą ir sutelkus pirmiau nurodytus išteklius, už saugumą atsakingas EIVT direktoratas teikia konkrečius kelionės patarimus dėl darbuotojų, už kurių įdarbinimą atsakinga EIVT, misijų į trečiąsias valstybes, kurių rizikos lygis yra labai didelis arba padidėjęs.

20 straipsnis

Sveikata ir sauga

EIVT saugumo taisyklės papildo vyriausiojo įgaliotinio patvirtintas EIVT sveikatos ir saugos užtikrinimo taisykles.

21 straipsnis

Įgyvendinimas ir peržiūra

1. EIVT saugumo institucija, jei reikia, pasikonsultavusi su EIVT saugumo komitetu, tvirtina saugumo strategijas ir gaires, kuriose nustatomos šių taisyklių įgyvendinimo EIVT priemonės, taip pat, glaudžiai bendradarbiaudama su valstybių narių kompetentingomis saugumo institucijomis ir padedama ES institucijų atitinkamų tarnybų, kuria pajėgumus, reikalingus visiems saugumo aspektams užtikrinti.

2. Pagal 2010 m. liepos 26 d. Tarybos sprendimo 2010/427/ES, kuriuo nustatoma Europos išorės veiksmų tarnybos struktūra ir veikimas, 4 straipsnio 5 dalį, jei reikia, sudarant tarnybų lygio susitarimus su atitinkamomis Tarybos generalinio sekretoriato tarnybomis, gali būti taikomos pereinamojo laikotarpio nuostatos.

3. Vyriausiasis įgaliotinis užtikrina bendrą šio sprendimo taikymo nuoseklumą ir nuolat peržiūri šias saugumo taisykles.

4. EIVT saugumo taisyklės įgyvendinamos glaudžiai bendradarbiaujant su kompetentingomis valstybių narių saugumo institucijomis.

5. EIVT užtikrina, kad EIVT reagavimo į krizę sistemoje būtų atsižvelgta į visus saugumo proceso aspektus.

6. Generalinis sekretorius, kaip saugumo institucija, ir už saugumą atsakingo EIVT direktorato vadovas užtikrina šio sprendimo įgyvendinimą.

22 straipsnis

Ankstesnių sprendimų pakeitimas

Šiuo sprendimu panaikinamas ir pakeičiamas 2013 m. balandžio 19 d. Europos Sąjungos vyriausiojo įgaliotinio užsienio reikalams ir saugumo politikai sprendimas dėl Europos išorės veiksmų tarnybos saugumo taisyklių ([5]).

23 straipsnis

Baigiamosios nuostatos

Šis sprendimas įsigalioja jo pasirašymo dieną.

Jis skelbiamas *Europos Sąjungos oficialiajame leidinyje*.

EIVT kompetentingos institucijos apie šį sprendimą, jo priedus, turinį, įsigaliojimą ir visus jo tolesnius pakeitimus tinkamai ir laiku praneša visiems darbuotojams, kurie patenka į jo taikymo sritį.

Priimta Briuselyje 2017 m. rugsėjo 19 d.

Federica MOGHERINI

Europos Sąjungos vyriausioji įgaliotinė užsienio reikalams ir saugumo politikai

---

([1]) OL L 201, 2010 08 03, p. 30.

([2]) OL C 304, 2011 10 15, p. 7.

([3]) Europos Sąjungos pareigūnų tarnybos nuostatai ir kitų Europos Sąjungos tarnautojų įdarbinimo sąlygos, nustatyti Tarybos reglamente (EEB, Euratomas, EAPB) Nr. 259/68 (OL L 56, 1968 03 04, p. 1), toliau – Tarnybos nuostatai.

([4]) 2000 m. gruodžio 18 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 45/2001 dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo (OL L 8, 2001 01 12, p. 1).

([5]) OL C 190, 2013 6 29, p. 1.

A PRIEDAS

ESĮI APSAUGOS PRINCIPAI IR STANDARTAI

1 straipsnis

Tikslas, taikymo sritis ir sąvokų apibrėžtys

1. Šiame priede nustatyti pagrindiniai ESĮI apsaugai užtikrinti skirti saugumo principai ir būtiniausi standartai.

2. Šie pagrindiniai principai ir būtiniausi standartai taikomi EIVT ir darbuotojams, už kurių įdarbinimą atsakinga EIVT, kaip atitinkamai nurodyta ir apibrėžta šio sprendimo 1 ir 2 straipsniuose.

2 straipsnis

ESĮI, slaptumo žymų ir kitų žymų apibrėžtis

1. ES įslaptinta informacija (ESĮI) – bet kuri informacija arba medžiaga, kuriai suteikta ES slaptumo žyma ir kurią neteisėtai atskleidus galėtų būti padaryta tam tikro dydžio žala Europos Sąjungos arba vienos ar kelių valstybių narių interesams.

2. ESĮI žymima viena iš šių slaptumo žymų:

a) **TRES SECRET UE/ES TOP SECRET**: informacija ir medžiaga, kurią neteisėtai atskleidus galėtų būti padaryta ypatingai didelė žala Europos Sąjungos arba vienos ar kelių valstybių narių esminiams interesams;

b) **SECRET UE/EU SECRET**: informacija ir medžiaga, kurią neteisėtai atskleidus galėtų būti rimtai pakenkta Europos Sąjungos arba vienos ar kelių valstybių narių esminiams interesams;

c) **CONFIDENTIEL UE/EU CONFIDENTIAL**: informacija ir medžiaga, kurią neteisėtai atskleidus galėtų būti pakenkta Europos Sąjungos arba vienos ar kelių valstybių narių esminiams interesams;

d) **RESTREINT UE/EU RESTRICTED**: informacija ir medžiaga, kurios neteisėtas atskleidimas galėtų būti nepalankus Europos Sąjungos arba vienos ar kelių valstybių narių interesams.

3. ESĮI žymima slaptumo žyma pagal 2 dalį. Ji gali būti pažymėta papildoma žyma, skirta nurodyti veiklos sritį, su kuria ji yra susijusi, nurodyti įslaptintos informacijos rengėją, apriboti jos platinimą, naudojimą ar suteikimą.

3 straipsnis

Įslaptinimo valdymas

1. EIVT užtikrina, kad ESĮI būtų žymima tinkama slaptumo žyma, būtų aiškiai nurodoma, kad tai yra įslaptinta informacija, ir jai būtų suteikta slaptumo žyma tik tokiam laikotarpiui, kuris yra būtinas.

2. ESĮI slaptumo žymos laipsnis nesumažinamas arba ji neišslaptinama ir nekeičiamos arba nepanaikinamos 2 straipsnio 3 dalyje nurodytos žymos be išankstinio įslaptintos informacijos rengėjo rašytinio sutikimo.

3. EIVT saugumo institucija, pasikonsultavusi su EIVT saugumo komitetu pagal šio sprendimo 15 straipsnio 5 dalį, patvirtina ESĮI rengimo saugumo politiką, kuri apima praktinį žymų vadovą.

4 straipsnis

Įslaptintos informacijos apsauga

1. ESĮI apsaugoma laikantis šio sprendimo.

2. Bet kokios ESĮI turėtojas yra atsakingas už jos apsaugą pagal šį sprendimą.

3. Valstybėms narėms nacionaline slaptumo žyma pažymėtą įslaptintą informaciją perdavus į EIVT struktūras ar tinklus, EIVT tą informaciją saugo laikydamasi reikalavimų, taikomų lygiaverčio slaptumo žymos lygio ESĮI, kaip nustatyta B priedėlyje pateiktoje slaptumo žymų atitikmenų lentelėje.

EIVT nustato tinkamas procedūras, skirtas tiksliam registravimui užtikrinti, kurios taikomos tokios informacijos rengėjams:

– įslaptintos informacijos, kurią gauna EIVT ir
– pradinės medžiagos, kuri yra EIVT parengtos įslaptintos informacijos dalis.

Apie šias procedūras pranešama EIVT saugumo komitetui.

4. Didelio ESĮI kiekio ar ESĮI rinkinio atveju gali būti reikalaujama užtikrinti tokio lygio apsaugą, kuri žymima aukštesnio lygio slaptumo

žyma nei šios informacijos sudedamosios dalys.

5 straipsnis

Personalo patikimumo užtikrinimo priemonės, taikomos tvarkant ES įslaptintą informaciją

1. Personalo patikimumas – priemonių taikymas, siekiant užtikrinti, kad galimybė susipažinti su ESĮI būtų suteikta tik asmenims:
- kuriems „būtina žinoti“;
- kurių patikimumas patikrintas atitinkamu lygiu ir suteikta teisė prieiti prie informacijos, pažymėtos CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio lygio saugumo žyma, arba kiti tinkami leidimai pagal nacionalinius įstatymus ir kitus teisės aktus ir
- kurie informuoti apie jų pareigas.

2. Taikant asmens patikimumo pažymėjimo (APP) išdavimo procedūras, nustatoma, ar asmeniui, atsižvelgiant į jo lojalumą ir patikimumą, gali būti leidžiama susipažinti su ESĮI.

3. Visi asmenys, prieš jiems suteikiant leidimą susipažinti su ESĮI, o vėliau – reguliariai, informuojami apie pareigą saugoti ESĮI pagal šį sprendimą ir jie ją raštu patvirtina.

4. Šio straipsnio įgyvendinimo nuostatos išdėstytos A I priede.

6 straipsnis

ES įslaptintos informacijos fizinis saugumas

1. Fizinis saugumas yra fizinių ir techninių apsaugos priemonių taikymas siekiant užkirsti kelią leidimo neturintiems asmenims susipažinti su ESĮI.

2. Fizinės saugumo priemonės skirtos sutrukdyti įsibrauti slaptai arba įsiveržti jėga, atgrasyti nuo neteisėtų veiksmų, sutrukdyti jiems bei juos nustatyti ir sudaryti sąlygas suskirstyti personalą pagal tai, kas gali susipažinti su ESĮI, vadovaujantis principu „būtina žinoti“. Tokios priemonės grindžiamos rizikos valdymo procesu.

3. Fizinio saugumo priemonės taikomos visose patalpose, pastatuose, kabinetuose, salėse ir kitose zonose, kuriose tvarkoma arba saugoma ESĮI, įskaitant zonas, kuriose įrengtos ryšių ir informacinės sistemos, kaip apibrėžta A priedo 8 straipsnio 2 dalyje.

4. Zonos, kuriose saugoma CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio lygio slaptumo žyma pažymėta ESĮI, įrengiamos kaip saugumo zonos pagal II A priedo nuostatas ir patvirtinamos EIVT saugumo institucijos.

5. CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėtos ESĮI apsaugai naudojama tik patvirtinta įranga ar prietaisai.

6. Šio straipsnio įgyvendinimo nuostatos išdėstytos A II priede.

7 straipsnis

Įslaptintos informacijos administravimas

1. Įslaptintos informacijos administravimas – administracinių ESĮI kontrolės visą jos gyvavimo ciklą priemonių taikymas siekiant papildyti 5, 6 ir 8 straipsniuose numatytas priemones ir tokiu būdu atgrasyti nuo tokios informacijos sąmoningo ar tikslingo atskleidimo arba praradimo, nustatyti tokius atvejus ir pašalinti jų padarinius. Tokios priemonės visų pirma yra susijusios su ESĮI rengimu, registravimu, kopijavimu, vertimu, gabenimu, tvarkymu, saugojimu ir naikinimu.

2. CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta informacija saugumo tikslais registruojama prieš ją platinant ir ją gavus. EIVT kompetentingos institucijos šiuo tikslu sukuria registratūrų sistemą. Slaptumo žyma TRES SECRET UE/ES TOP SECRET pažymėta informacija registruojama tam skirtose registratūrose.

3. Tarnybas ir patalpas, kuriose ESĮI tvarkoma arba saugoma, reguliariai tikrina EIVT saugumo institucija.

4. Už fiziškai apsaugotų zonų ribų ESĮI iš vienos tarnybos į kitą ir iš vienų patalpų į kitas perduodama šiais būdais:

a) paprastai ESĮI perduodama elektroninėmis priemonėmis, apsaugant informaciją šifravimo priemonėmis, patvirtintomis pagal šio sprendimo 7 straipsnio 5 dalį ir aiškiai apibrėžtas saugios eksploatacijos taisykles (SecOPs);

b) kai nenaudojamos a punkte nurodytos priemonės, ESĮI gabenama:

i) elektroninėse laikmenose (pvz., USB atmintinėse, kompaktiniuose diskuose, kietuosiuose diskuose), informaciją apsaugant pagal šio sprendimo 8 straipsnio 5 dalyje patvirtintas šifravimo priemones;

ii) visais kitais atvejais – EIVT saugumo institucijos nurodytu būdu, laikantis atitinkamų A III priedo V skyriuje nustatytų apsaugos priemonių.

5. Šio straipsnio įgyvendinimo nuostatos išdėstytos A III priede.

8 straipsnis

RIS tvarkomos ESĮI apsauga

1. Informacijos saugumo užtikrinimas (ISU) ryšių ir informacinių sistemų srityje – užtikrinimas, kad tokiose sistemose tvarkoma informacija bus apsaugota ir kad, valdant teisėtiems naudotojams, jos veiks taip, kaip turi veikti, ir tada, kada turi veikti. Veiksmingas ISU užtikrina tinkamą konfidencialumo, vientisumo, prieinamumo, atsakomybės už veiksmus prisiėmimo ir autentiškumo lygį. ISU grindžiamas rizikos valdymo procesu.

2. Ryšių ir informacinė sistema (RIS) – sistema, sudaranti sąlygas tvarkyti informaciją elektroniniu būdu. Ryšių ir informacinė sistema apima visas sistemos dalis, kurių reikia jos veikimui užtikrinti, įskaitant infrastruktūrą, organizavimą, personalą ir informacijos išteklius. Šis priedas taikomas visoms EIVT RIS, kuriose tvarkoma ESĮI.

3. RIS sistemose ESĮI tvarkoma laikantis ISU principo.

4. Visos RIS, kuriose tvarkoma ESĮI, turi būti akredituojamos. Akreditavimo tikslas – įsitikinti, kad įgyvendintos visos atitinkamos saugumo priemonės ir kad pasiektas pakankamas ESĮI ir RIS apsaugos lygis, vadovaujantis šiuo sprendimu. Pareiškime dėl akreditavimo nurodomas aukščiausias informacijos, kuri gali būti tvarkoma RIS, slaptumo žymos laipsnis ir atitinkami reikalavimai bei sąlygos.

5. RIS, kurioje tvarkoma CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta informacija, apsaugoma tokiu būdu, kad informacija negalėtų būti neteisėtai atskleista dėl netyčinio elektromagnetinio spinduliavimo (TEMPEST apsaugos priemonės).

6. Kai ESĮI apsauga užtikrinama šifravimo priemonėmis, tokios prie-

monės patvirtinamos pagal šio sprendimo 8 straipsnio 5 dalį.

7. Perduodant ESĮI elektroninėmis priemonėmis naudojamos patvirtintos šifravimo priemonės. Nepaisant šio reikalavimo, esant nepaprastosios padėties sąlygoms arba tam tikrų techninių konfigūracijų atvejais, kaip nurodyta A IV priede, gali būti taikomos specialios procedūros.

8. Pagal šio sprendimo 8 straipsnio 6 dalį įsteigiamos šios ISU institucijos (tokio dydžio, koks reikalingas):

a) ISU institucija (ISUI);
b) TEMPEST institucija (TEI);
c) Kriptografijos patvirtinimo institucija (KPI);
d) Kriptografijos platinimo institucija (KPLI).

9. Pagal šio sprendimo 8 straipsnio 7 dalį kiekvienoje sistemoje įsteigiamos šios institucijos:

a) Saugumo akreditavimo institucija (SAI);
b) ISU operacinė institucija.

10. Šio straipsnio įgyvendinimo nuostatos išdėstytos A IV priede.

9 straipsnis

Pramoninis saugumas

1. Pramoninis saugumas – priemonių, kurias rangovai arba subrangovai taiko derybų dėl sutarčių sudarymo metu ir visą įslaptintų sutarčių gyvavimo ciklą, siekdami užtikrinti ESĮI apsaugą, taikymas. Paprastai tokiose sutartyse nenumatoma galimybė susipažinti su slaptumo žyma TRES SECRET UE/EU TOP SECRET pažymėta informacija.

2. EIVT sutartimi gali patikėti pramonės arba kitiems subjektams, registruotiems valstybėje narėje arba trečiojoje valstybėje, kuri yra sudariusi susitarimą dėl informacijos saugumo arba administracinį susitarimą pagal A priedo 10 straipsnio 1 dalį, užduotis, kurioms atlikti reikia arba reikės susipažinti su ESĮI arba ją tvarkyti ar saugoti.

3. EIVT, kaip perkančioji institucija, užtikrina, kad sudarant įslaptintas sutartis su pramonės ar kitais subjektais būtų laikomasi šiame sprendime išdėstytų ir sutartyje nurodytų būtiniausių pramoninio saugumo standartų. Ji, pasitelkdama atitinkamas NSI/PSI, užtikrina atitiktį būtiniausiems standartams.

4. Valstybėje narėje įregistruoti rangovai ar subrangovai, dalyvaujantys įslaptintose sutartyse arba subrangos sutartyse, pagal kurias jas vykdant arba prieš jas sudarant šių subjektų patalpose tvarkoma ir saugo-

ma įslaptinta informacija, pažymėta slaptumo žyma CONFIDENTIEL UE/EU CONFIDENTIAL arba SECRET UE/EU SECRET, turi reikiamą slaptumo žymos lygį, atitinkantį Įmonės patikimumą patvirtinantį pažymėjimą (ĮPPP), išduotą atitinkamos valstybės narės NSI, PSI ar kitos kompetentingos saugumo institucijos.

5. Rangovo ar subrangovo darbuotojai, kuriems vykdant įslaptintą sutartį reikia susipažinti su slaptumo žyma CONFIDENTIEL UE/EU CONFIDENTIAL arba SECRET UE/EU SECRET pažymėta informacija, turi asmens patikimumo pažymėjimą (APP), išduotą atitinkamos nacionalinės saugumo institucijos (NSI), paskirtosios saugumo institucijos (PSI) ar kitos kompetentingos saugumo institucijos pagal nacionalinius įstatymus ir kitus teisės aktus bei A I priede nustatytus būtiniausius saugumo standartus.

6. Šio straipsnio įgyvendinimo nuostatos išdėstytos A V priede.

10 straipsnis

Keitimasis įslaptinta informacija su trečiosiomis valstybėmis ir tarptautinėmis organizacijomis

1. EIVT gali keistis ESĮI su trečiosiomis valstybėmis ar tarptautinėmis organizacijomis, jei:

a) galioja ES ir atitinkamos trečiosios valstybės ar tarptautinės organizacijos susitarimas dėl informacijos saugumo, sudarytas pagal ES sutarties 37 straipsnį ir SESV 218 straipsnį;
b) įsigaliojo vyriausiojo įgaliotinio ir atitinkamos trečiosios valstybės ar tarptautinės organizacijos saugumo institucijos administracinis susitarimas dėl keitimosi RESTREINT UE/EU RESTRICTED arba aukštesnio lygio slaptumo žyma pažymėta informacija, sudarytas pagal procedūrą, nustatytą šio sprendimo 15 straipsnio 5 dalyje;
c) taikytinas ES ir atitinkamos trečiosios valstybės bendrasis arba *ad hoc* dalyvavimo susitarimas BSGP krizių valdymo operacijos kontekste, sudarytas pagal ES sutarties 37 straipsnį ir SESV veikimo 218 straipsnį, ir įvykdytos šią priemonę reglamentuojančiose dokumentuose nustatytos sąlygos.

Pirmiau nurodytų pagrindinių taisyklių išimtys išdėstytos A VI priedo V skyriuje.

2. Į 1 dalies b punkte nurodytus administracinius susitarimus įtraukiamos nuostatos, kuriomis užtikrinama, jog, trečiosioms valstybėms

arba tarptautinėms organizacijoms gavus ESĮI, tai informacijai užtikrinama jos slaptumo žymos lygį atitinkanti apsauga, remiantis būtiniausiais standartais, kurie yra ne mažiau griežti nei šiame sprendime nustatyti standartai.

Informacija, kuria keičiamasi pagal 1 dalies c punkte sudarytus susitarimus, gali būti tik informacija, susijusi su BSGP operacijomis, kuriose atitinkama trečioji valstybė dalyvauja pagal šiuos susitarimus ir jų nuostatas.

3. Jeigu vėliau sudaromas Europos Sąjungos ir dalyvaujančiosios trečiosios valstybės ar tarptautinės organizacijos susitarimas dėl informacijos saugumo, šio susitarimo dėl informacijos saugumo nuostatos yra viršesnės už bet kokiuose susitarimuose dėl dalyvavimo bendrųjų sąlygų, *ad hoc* susitarimuose dėl dalyvavimo arba *ad hoc* administraciniuose susitarimuose išdėstytas nuostatas dėl keitimosi įslaptinta informacija, kiek tai susiję su keitimusi ESĮI ir jos apdorojimu.

4. BSGP operacijos vykdymui surinkta ESĮI gali būti suteikiama trečiųjų valstybių ar tarptautinių organizacijų į tą operaciją komandiruotam personalui, vadovaujantis 1–3 dalių ir A VI priedo nuostatomis. Kai tokiam personalui leidžiama susipažinti su ESĮI BSGP operacijos patalpose ar RIS, turi būti imamasi priemonių (įskaitant suteiktos ESĮI registravimą), kad būtų sumažinta rizika, jog informacija bus prarasta ar atskleista. Tokios priemonės nurodomos atitinkamuose planavimo ar misijos dokumentuose.

5. Šio sprendimo 17 straipsnyje nurodyti įvertinimo vizitai į trečiąsias valstybes ar tarptautines organizacijas rengiami siekiant įsitikinti, kad ten taikomos bet kokios ESĮI, kuria keičiamasi, apsaugos priemonės yra veiksmingos.

6. Sprendimą suteikti EIVT turimą ESĮI trečiajai valstybei ar tarptautinei organizacijai EIVT priima atskirai kiekvienu konkrečiu atveju, atsižvelgdama į tokios informacijos pobūdį ir turinį bei gavėjo atitiktį principui „būtina žinoti“ ir įvertinusi naudą ES.

EIVT prašo subjekto, pateikusio įslaptintą informaciją, kuri buvo panaudota kaip pradinė medžiaga ESĮI, kurią parengė EIVT, pateikti rašytinį sutikimą, patvirtinantį, kad subjektas neprieštarauja šios informacijos suteikimui.

Jeigu EIVT nėra įslaptintos informacijos, kurią prašoma suteikti, rengėja, EIVT pirmiausia prašo jos įslaptintos informacijos rengėjo pateikti rašytinį sutikimą suteikti šią informaciją.

Tačiau, jei EIVT negali nustatyti atitinkamos informacijos rengėjo,

EIVT saugumo institucija, gavusi vieningą valstybių narių, atstovaujamų EIVT saugumo komitete, pritarimą, perima rengėjo atsakomybę.

7. Šio straipsnio įgyvendinimo nuostatos išdėstytos A VI priede.

11 straipsnis

Įslaptintos informacijos saugumo pažeidimai ir neteisėtas atskleidimas

1. Apie bet kokį faktinį ar įtariamą saugumo pažeidimą ir apie bet kokį faktinį ar įtariamą įslaptintos informacijos neteisėtą atskleidimą nedelsiant pranešama už saugumą atsakingam EIVT direktoratui, kuris, prireikus, informuoja atitinkamą (-as) valstybę (-es) narę (-es) ar kitus atitinkamus subjektus.

2. Tais atvejais, kai žinoma arba yra pagrįstų priežasčių įtarti, kad įslaptinta informacija buvo neteisėtai atskleista arba prarasta, už saugumą atsakingas EIVT direktoratas informuoja atitinkamos (-ų) valstybės (-ių) narės (-ių) NSI ir, vadovaudamasis atitinkamais įstatymais ir kitais teisės aktais, imasi visų atitinkamų priemonių:

a) išsaugoti įrodymus;
b) užtikrinti, kad siekiant nustatyti faktus tokį atvejį nagrinėtų su pažeidimu tiesiogiai nesusijęs personalas;
c) nedelsiant informuoti informacijos rengėją arba kitą atitinkamą subjektą;
d) imtis atitinkamų priemonių, kad būtų užkirstas kelias pažeidimui pasikartoti;
e) įvertinti galimą ES ar valstybių narių interesams padarytą žalą;
f) pranešti atitinkamoms institucijoms apie faktinio ar įtariamo neteisėto informacijos atskleidimo padarinius ir veiksmus, kurių imtasi.

3. Bet kuriam darbuotojui, už kurio įdarbinimą atsakinga EIVT, kuris pažeidė šiame sprendime nustatytas saugumo taisykles, gali būti taikomos drausminės priemonės pagal taikomas taisykles ir teisės aktus.

Asmeniui, kuris atsakingas už įslaptintos informacijos neteisėtą atskleidimą ar praradimą, taikomos drausminės ir (arba) teisinės priemonės pagal taikomus įstatymus, taisykles ir kitus teisės aktus.

4. Vykdant tyrimą dėl pažeidimo ir (arba) neteisėtos informacijos atskleidimo, už saugumą atsakingo EIVT direktorato vadovas gali laikinai sustabdyti asmens leidimą susipažinti su ESĮI ir patekti į EIVT patalpas. Apie šį sprendimą nedelsiant pranešama Komisijos Žmogiškųjų iš-

teklių ir saugumo generalinio direktorato Saugumo direktoratui, Tarybos generalinio sekretoriato Saugumo tarnybai ir atitinkamų valstybių narių NSI ar kitiems atitinkamiems subjektams.

A I PRIEDAS

PERSONALO SAUGUMAS

I. ĮVADAS

1. Šiame priede pateiktos A priedo 5 straipsnio įgyvendinimo nuostatos. Jame nustatomi kriterijai, kuriais remdamasi EIVT nustato, ar asmeniui, atsižvelgiant į jo lojalumą ir patikimumą, gali būti leidžiama susipažinti su ESĮI, ir šiuo tikslu taikytinos tikrinimo bei administracinės procedūros.
2. Asmens patikimumo pažymėjimas (APP), kuriuo suteikiama teisė susipažinti su ESĮI – valstybės narės kompetentingos institucijos patvirtinimas, kuris pateikiamas valstybės narės kompetentingoms institucijoms baigus patikimumo tyrimą ir kuriuo pažymima, kad atitinkamam asmeniui, nustačius, kad jis atitinka principą „būtina žinoti“, suteikiamas leidimas iki nurodytos datos susipažinti su atitinkamo lygio slaptumo žyma (CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio lygio slaptumo žyma) pažymėta ESĮI. Laikoma, kad asmens, kuriam taikoma ši apibrėžtis, patikimumas patikrintas.
3. Asmens patikimumo pažymėjimą patvirtinanti pažyma (APPP) yra EIVT saugumo institucijos išduota pažyma, kurioje nurodoma, kad asmens patikimumas yra patikrintas, ir nurodomas ESĮI, su kuria tam asmeniui gali būti leista susipažinti, slaptumo žymos lygis, atitinkamo APP galiojimo laikas ir pačios pažymos galiojimo laikas.
4. Leidimas susipažinti su ESĮI – EIVT saugumo institucijos leidimas, kuris suteikiamas pagal šį sprendimą po to, kai valstybės narės kompetentingos institucijos suteikia APP, ir kuriuo pažymima, kad atitinkamam asmeniui, nustačius, kad jis atitinka principą „būtina žinoti“, suteikiamas leidimas iki nurodytos datos susipažinti su atitinkamo lygio slaptumo žyma (CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio lygio slaptumo žyma) pažymėta ESĮI. Laikoma, kad asmens, kuriam taikoma ši apibrėžtis, patikimumas patikrintas.

II. LEIDIMAS SUSIPAŽINTI SU ESĮI

5. Siekiant įgyti galimybę susipažinti su informacija, pažymėta slaptumo žyma RESTREINT UE/EU RESTRICTED, patikimumo pažymėjimas nebūtinas. Ši galimybė suteikiama:

   a) kai atsiranda asmens sąsaja su EIVT, pagrįsta teisės aktais ar sutartimi;

   b) kai nustatoma, kad asmuo atitinka principą „būtina žinoti“;

   c) kai asmeniui pateikiama informacija apie ESĮI apsaugai užtikrinti skirtas saugumo taisykles bei procedūras ir jis raštu patvirtina savo pareigą saugoti ESĮI pagal šį sprendimą.
6. Asmeniui leidžiama susipažinti su CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta ES įslaptinta informacija tik tuo atveju, kai:

   a) atsiranda asmens sąsaja su EIVT, pagrįsta teisės aktais ar sutartimi;

   b) nustatoma, kad jam „būtina žinoti“;

   c) dėl jo atliekamų funkcijų jam buvo išduotas atitinkamo slaptumo žymos laipsnio APP arba kiti tinkami leidimai pagal nacionalinius įstatymus ir kitus teisės aktus;

   d) jis buvo informuotas apie ESĮI apsaugai užtikrinti skirtas saugumo taisykles bei procedūras ir raštu patvirtino savo pareigą saugoti tokią informaciją.
7. EIVT savo struktūrose nustato tas pareigybes, kurias užimantiems asmenims reikia susipažinti su CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio lygio slaptumo žyma pažymėta informacija ir todėl jie turi turėti atitinkamo slaptumo žymos lygio APP, kaip nustatyta pirmiau pateiktoje 4 dalyje.
8. EIVT darbuotojai nurodo, ar jie turi daugiau kaip vienos šalies pilietybę.

EIVT taikoma prašymo dėl APP pateikimo procedūra

9. EIVT darbuotojų atveju EIVT saugumo institucija nusiunčia užpildytą asmens patikimumo tikrinimo klausimyną valstybės narės, kurios pilietis asmuo yra, NSI, prašydama atlikti patikimumo tyrimą, skirtą gauti leidimui naudotis tam tikro slaptumo žymos lygio ESĮI, su kuria asmeniui reikės susipažinti.

10. Jei asmuo turi daugiau kaip vienos šalies pilietybę, prašymas patikrinti patikimumą siunčiamas šalies, kurios pilietybė nurodyta asmenį įdarbinant, NSI.
11. Jei EIVT sužino patikimumo tyrimui svarbios informacijos apie asmenį, kuris pateikė prašymą dėl APP, EIVT, laikydamasi atitinkamų taisyklių ir teisės aktų, apie tai praneša atitinkamai NSI.
12. Užbaigusi patikimumo tyrimą, atitinkama NSI praneša už saugumą atsakingam EIVT direktoratui tokio patikrinimo rezultatus.

    a) Jei patikimumo tyrimo rezultatai užtikrintai rodo, kad neturima jokios nepalankios informacijos, kuri leistų abejoti asmens lojalumu ir patikimumu, EIVT saugumo institucija gali atitinkamam asmeniui leisti susipažinti su iki tam tikro lygio slaptumo žyma pažymėta ESĮI iki nustatytos datos.

    b) EIVT imasi visų tinkamų priemonių, kad užtikrintų, kad NSI taikomos sąlygos ar apribojimai būtų tinkamai įgyvendinami. NSI pranešama apie įgyvendinimo rezultatus.

    c) Jei patikimumo tyrimo rezultatai nėra tokie užtikrinantys, EIVT saugumo institucija apie tai praneša atitinkamam asmeniui, kuris gali prašyti, kad EIVT saugumo institucija jį išklausytų. EIVT saugumo institucija gali prašyti kompetentingos NSI pateikti daugiau paaiškinimų, kuriuos ji gali pateikti pagal savo nacionalinius įstatymus ir kitus teisės aktus. Jei rezultatai pasitvirtina, leidimas susipažinti su ESĮI neišduodamas. Tokiu atveju EIVT imasi visų tinkamų priemonių, kad užtikrintų, kad prašymo pateikėjui nebūtų suteikta jokia galimybė susipažinti su ESĮI.
13. Patikimumo tyrimui bei gautiems rezultatams, kuriais EIVT grindžia savo sprendimą suteikti leidimą susipažinti su ESĮI ar jo nesuteikti, taikomi atitinkamoje valstybėje narėje galiojantys įstatymai ir kiti teisės aktai, įskaitant su apskundimu susijusius įstatymus ir kitus teisės aktus. EIVT saugumo institucijos sprendimai gali būti apskųsti pagal Tarnybos nuostatus.
14. APP galioja visoms užduotims, kurias tas asmuo vykdo EIVT, Tarybos generaliniame sekretoriate ar Komisijoje, su sąlyga, kad tebegalioja jo išdavimą pagrindžiančios aplinkybės.
15. EIVT pripažįsta kitos Europos Sąjungos institucijos, įstaigos ar agentūros išduotą leidimą susipažinti su ESĮI, jei jis tebegalioja. Leidimai galioja visoms užduotims, kurias tas asmuo vykdo EIVT. Europos Sąjungos institucija, įstaiga ar agentūra, kurioje asmuo pradeda dirbti, praneša atitinkamai NSI apie darbdavio pasikeitimą.

16. Jeigu asmens tarnyba neprasideda per 12 mėnesių nuo patikimumo tyrimo rezultatų pranešimo EIVT saugumo institucijai arba jeigu asmens tarnyboje daroma 12 mėnesių pertrauka ir tuo laikotarpiu jis nėra priimtas į pareigas EIVT, kitoje ES institucijoje, agentūroje ar įstaigoje arba valstybės narės nacionalinėje administracinėje įstaigoje, kurias einant reikia susipažinti su įslaptinta informacija, atitinkamos NSI prašoma patvirtinti, kad rezultatai tebegalioja bei yra tinkami.
17. Jei EIVT sužino informacijos apie tai, kad asmuo, turintis leidimą susipažinti su ESĮI, kelia pavojų saugumui, EIVT, laikydamasi atitinkamų taisyklių ir teisės aktų, apie tai praneša atitinkamai NSI ir gali asmeniui laikinai nesuteikti galimybės susipažinti su ESĮI arba panaikinti leidimą susipažinti su ESĮI. Kai NSI informuoja EIVT apie tai, kad pagal 12 dalies a punktą suteiktas užtikrinimas, jog galiojantis asmens leidimas susipažinti su ESĮI panaikinamas, EIVT saugumo institucija gali paprašyti pateikti paaiškinimą, kurį NSI gali pateikti pagal nacionalinius įstatymus ir kitus teisės aktus. Jei nepalanki informacija patvirtinama, minėtas leidimas panaikinamas, o asmeniui neleidžiama susipažinti su ESĮI ir užimti pareigų, kurias eidamas jis galėtų susipažinti su ta informacija arba sukelti pavojų saugumui.
18. Apie bet kurį sprendimą panaikinti EIVT darbuotojo leidimą susipažinti su ESĮI ir, jei reikia, tokio panaikinimo priežastis pranešama atitinkamam asmeniui, kuris gali prašyti, kad EIVT saugumo institucija jį išklausytų. NSI teikiamą informaciją reglamentuoja atitinkamoje valstybėje narėje galiojantys įstatymai ir kiti teisės aktai, įskaitant su apeliacijomis susijusius įstatymus ir kitus teisės aktus. EIVT saugumo institucijos sprendimai gali būti apskųsti pagal Tarnybos nuostatus.
19. Į EIVT komandiruoti nacionaliniai ekspertai, siekiantys užimti pareigas, kurias einant reikia susipažinti su CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesne slaptumo žyma pažymėta įslaptinta informacija, EIVT saugumo institucijai prieš pradėdami tarnybą pateikia galiojantį APP, leidžiantį susipažinti su atitinkamo slaptumo lygio ESĮI. Pirmiau minėtą procesą administruoja išsiunčiančioji valstybė narė.

APP registrai

20. EIVT tvarko visų darbuotojų, už kurių įdarbinimą atsakinga EIVT, ir EIVT rangovų darbuotojų patikimumo pažymėjimo statuso duomenų bazę. Šiuose registruose nurodomas ESĮI, su kuria tam asmeniui gali būti leista susipažinti, slaptumo žymos lygis (CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio lygio slaptumo žyma), APP išdavimo data ir jo galiojimo laikas.
21. Valstybės narės ir kitos ES institucijos, agentūros ir įstaigos, siekdamos užtikrinti, kad EIVT turėtų tikslius ir išsamius visų darbuotojų, už kurių įdarbinimą atsakinga EIVT, ir EIVT rangovų darbuotojų patikimumo pažymėjimo statuso registrus, nustato atitinkamas koordinavimo procedūras.
22. EIVT saugumo institucija gali išduoti asmens patikimumo pažymėjimą patvirtinančią pažymą (APPP), kurioje nurodomas ESĮI, su kuria tam asmeniui gali būti leista susipažinti, slaptumo žymos lygis (CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio lygio slaptumo žyma), atitinkamo APP arba leidimo galiojimo laikas ir pačios pažymos galiojimo laikas.

Reikalavimo turėti APP taikymo išimtys

23. Jei reikia, už saugumą atsakingas EIVT direktoratas informuoja asmenis, kuriems dėl jų atliekamų funkcijų pagal nacionalinius įstatymus ir kitus teisės aktus suteikta teisė susipažinti su ESĮI, apie jų saugumo įsipareigojimus ESĮI apsaugos srityje.

III. ŠVIETIMAS SAUGUMO KLAUSIMAIS IR SAUGUMO SUPRATIMAS

24. Prieš asmenims suteikiant leidimą susipažinti su ESĮI, jie raštu patvirtina, kad supranta įsipareigojimus saugoti ESĮI ir ESĮI neteisėto atskleidimo padarinius. EIVT registruoja tokius rašytinius patvirtinimus.
25. Visi asmenys, kuriems leidžiama susipažinti su ESĮI arba kurie turi dirbti su ESĮI, yra iš pat pradžių informuojami ir paskui reguliariai informuojami apie grėsmes saugumui ir jie turi nedelsdami pranešti atitinkamoms saugumo tarnyboms apie bet kokius bandymus užmegzti kontaktą ar veiklą, kurie, jų nuomone, yra įtartini ar neįprasti.

26. Visiems asmenims, kuriems leidžiama susipažinti su EIVT, laikotarpį, per kurį jie tvarko ESĮI, taikomos nuolatinės asmens patikimumo užtikrinimo priemonės (t. y. priežiūra). Už nuolatinį asmens patikimumą atsakingi:

    a) asmenys, kuriems suteikta teisė susipažinti su ESĮI: jie yra asmeniškai atsakingi už savo patikimumą ir turi nedelsdami pranešti atitinkamoms saugumo institucijoms apie bet kokius bandymus užmegzti kontaktą ar veiklą, kuri, jų nuomone, yra įtartina ar neįprasta, ir visus jų asmeninių aplinkybių pokyčius, kurie gali turėti poveikį jų APP ar leidimui susipažinti su ESĮI;

    b) tiesioginiai vadovai: jie atsakingi už savo darbuotojų informavimą apie saugumo priemones ir pareigą apsaugoti ESĮI, darbuotojų patikimumo stebėjimą, problemiškų saugumo klausimų pateikimą patiems darbuotojams ir bet kokios neigiamos informacijos, kuri gali turėti poveikį jų darbuotojų APP ar leidimams susipažinti su ESĮI, pranešimą atitinkamoms saugumo institucijoms;

    c) EIVT saugumo organizacijos saugumo srities subjektai, nurodyti šio sprendimo 12 straipsnyje: jie atsakingi už saugumo informacijos teikimą siekiant užtikrinti reguliarų jų atsakomybės srityje dirbančių darbuotojų informavimą, stiprios darbo kultūros skatinimą jų atsakomybės srityje, priemonių, skirtų darbuotojų patikimumui stebėti, nustatymą ir bet kokios neigiamos informacijos, kuri gali turėti poveikį darbuotojo APP, pranešimą atitinkamoms saugumo institucijoms;

    d) EIVT ir valstybės narės: jos nustato reikalingus informacijos, kuri gali turėti poveikį bet kokio asmens APP ar leidimui susipažinti su ESĮI, perdavimo kanalus.

27. Visi asmenys, nebeinantys pareigų, kurias einant jiems reikia susipažinti su ESĮI, yra informuojami apie jų įsipareigojimus toliau saugoti ESĮI slaptumą ir atitinkamais atvejais jie tai patvirtina raštu.

IV. IŠSKIRTINĖS APLINKYBĖS

28. Dėl skubos priežasčių, kurios pagrįstos EIVT interesais, laukiant išsamaus patikimumo tyrimo pabaigos, EIVT saugumo institucija, pasikonsultavusi su valstybės narės, kurios pilietis yra atitinkamas asmuo, NSI ir atsižvelgusi į preliminaraus patikrinimo, skirto patikrinti, ar nėra žinomos nepalankios informacijos apie asmenį, rezultatus, gali EIVT pareigūnams ir kitiems tarnautojams išduoti laikiną leidimą susipažinti su ESĮI konkrečiai funkcijai atlikti. Išsamus patikimumo tyrimas turi būti baigtas kuo greičiau. Tokie laikini leidimai galioja ne ilgiau kaip šešis mėnesius ir nesuteikia teisės susipažinti su slaptumo žyma TRES SECRET UE/EU TOP SECRET pažymėta informacija. Visi asmenys, kuriems išduotas laikinas leidimas, raštu patvirtina, kad jie supranta savo įsipareigojimus saugoti ESSĮ ir ESĮI neteisėto atskleidimo pasekmes. EIVT registruoja tokius rašytinius patvirtinimus.
29. Kai asmuo turi būti paskirtas į pareigybę, kuriai užimti reikalingas vienu laipsniu aukštesnis nei turimas APP, jis gali būti paskirtas į tą pareigybę laikinai, jeigu:

    a) asmens vadovas raštu įtikinamai pagrindžia, kad būtina susipažinti su aukštesnio laipsnio ESĮI;

    b) suteikiama teisė susipažinti tik su konkrečia ESĮI, kurios reikia užduočiai atlikti;

    c) asmuo turi galiojantį APP;

    d) imtasi veiksmų pareigybei reikiamo laipsnio leidimui gauti;

    e) kompetentinga institucija atliko pakankamus patikrinimus, kad asmuo nėra rimtai ar pakartotinai pažeidęs saugumo nuostatų;

    f) asmens paskyrimą patvirtino kompetentinga institucija;

    g) pasikonsultuota su atitinkama NSI/PSI, kuri asmeniui išdavė APP, ir negauta jokių prieštaravimų;

    h) išimtis, įskaitant informacijos, su kuria leista susipažinti, aprašymą, registruoja atsakingos registratūros ar subregistratūros.
30. Pirmiau nurodytos procedūros laikomasi, kai reikia suteikti leidimą vieną kartą susipažinti su vienu laipsniu aukštesne slaptumo žyma pažymėta ESĮI nei ta, su kuria susipažinti jiems buvo leista atlikus patikimumo patikrinimą. Tokia procedūra neturi būti naudojama pakartotinai.

31. Itin išskirtinėmis aplinkybėmis, pvz., vykdant užduotis priešiškoje aplinkoje arba kylant tarptautinei įtampai, kai to reikia imantis neatidėliotinų priemonių, visų pirma siekiant išsaugoti žmonių gyvybes, vyriausiasis įgaliotinis, EIVT saugumo institucija arba *DGBA* gali, kai įmanoma, – raštu, suteikti galimybę susipažinti su slaptumo žyma CONFIDENTIEL UE/EU CONFIDENTIAL arba SECRET UE/EU SECRET pažymėta informacija asmenims, kuriems nėra išduotas reikiamas APP, jeigu tokio leidimo tikrai reikia. Toks leidimas registruojamas, kartu aprašant informaciją, su kuria leista susipažinti.
32. Slaptumo žyma TRES SECRET UE/EU TOP SECRET pažymėtos informacijos atveju toks leidimo suteikimas skubos tvarka taikomas tik tiems ES piliečiams, kuriems buvo leista susipažinti su nacionaline informacija, atitinkančia TRES SECRET UE/EU TOP SECRET slaptumo laipsnį, arba su slaptumo žyma SECRET UE/EU SECRET pažymėta informacija.
33. EIVT saugumo komitetas informuojamas apie atvejus, kai taikoma 31 ir 32 dalyse išdėstyta procedūra.
34. EIVT saugumo komitetui pateikiama šiame skirsnyje numatytų procedūrų taikymo metinė ataskaita.

V. DALYVAVIMAS EIVT BŪSTINĖJE IR EUROPOS SĄJUNGOS DELEGACIJOSE VYKSTANČIUOSE POSĖDŽIUOSE

35. Asmenys, paskirti dalyvauti EIVT būstinėje ir Europos Sąjungos delegacijose vykstančiuose posėdžiuose, kuriuose aptariama CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio lygio slaptumo žyma pažymėta informacija, gali tai daryti tik patvirtinus jų APP turėtojo statusą. Valstybių narių atstovų ir TGS bei Komisijos pareigūnų APPP ar kitus APP įrodymus atitinkamos institucijos siunčia už saugumą atsakingam EIVT direktoratui, Europos Sąjungos delegacijos saugumo koordinatoriui arba išimtiniais atvejais ją pateikia atitinkamas asmuo. Jei taikytina, gali būti naudojamas suvestinis pavardžių sąrašas, kuriame pateikiami atitinkami APP įrodymai.

36. Jei panaikinamas asmens, kuris eidamas savo pareigas turi dalyvauti EIVT būstinėje ir Europos Sąjungos delegacijose vykstančiuose posėdžiuose, kuriuose aptariama CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio lygio slaptumo žyma pažymėta informacija, APP, leidžiantis susipažinti su ESĮI, kompetentinga institucija apie tai praneša EIVT.

VI. GALIMA PRIEIGA PRIE ESĮI

37. Kai asmenys turi būti įdarbinti tokioje aplinkoje, kurioje jie gali turėti prieigą prie CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio lygio slaptumo žyma pažymėtos informacijos, jų patikimumas turi būti tinkamai patikrintas arba jie turi būti visą laiką lydimi.
38. Kurjerių, apsaugos darbuotojų ir lydinčių asmenų patikimumas turi būti patikrintas atitinkamu lygiu, arba jie turi būti kitaip deramai patikrinti vadovaujantis nacionaliniais įstatymais ir kitais teisės aktais. Jie yra reguliariai supažindinami su ESĮI apsaugai užtikrinti skirtomis saugumo procedūromis ir jiems išdėstomos jų pareigos jiems patikėtos tokios informacijos arba informacijos, su kuria jie susipažįsta per neapdairumą, apsaugos srityje.

A II PRIEDAS

ES ĮSLAPTINTOS INFORMACIJOS FIZINIS SAUGUMAS

I. ĮVADAS

1. Šiame priede pateiktos A priedo 6 straipsnio įgyvendinimo nuostatos. Jame išdėstyti būtiniausi reikalavimai, taikomi patalpų, pastatų, kabinetų, salių ir kitų zonų, kuriose tvarkoma ir saugoma ESĮI, įskaitant zonas, kuriose yra RIS, fizinei apsaugai.

2. Fizinio saugumo priemonės yra skirtos užkirsti kelią leidimo neturintiems asmenims susipažinti su ESĮI:

   a) užtikrinant, kad ESĮI būtų tinkamai tvarkoma ir saugoma;

   b) sudarant sąlygas suskirstyti personalą pagal tai, kas gali susipažinti su ESĮI, remiantis principu „būtina žinoti“ ir atitinkamais atvejais – darbuotojų patikimumo pažymėjimais;

   c) atgrasant nuo neteisėtų veiksmų, sutrukdant jiems bei juos nustatant ir

   d) sutrukdant asmenims įsibrauti slaptai ar įsiveržti jėga arba juos užlaikant.

II. FIZINIO SAUGUMO REIKALAVIMAI IR PRIEMONĖS

3. ESĮI apsaugai užtikrinti savo patalpose EIVT taiko rizikos valdymo procesą, kad užtikrintų, jog, atsižvelgiant į įvertintą riziką, būtų taikoma atitinkamo lygio fizinė apsauga. Rizikos valdymo procese atsižvelgiama į visus svarbius veiksnius, visų pirma:

   a) ESĮI slaptumo žymos lygį;

   b) ESĮI formą ir kiekį, atsižvelgiant į tai, kad dideliam ESĮI kiekiui ar rinkiniui apsaugoti gali reikėti taikyti griežtesnes apsaugos priemones;

   c) pastatus ar zonas, kuriose laikoma ESĮI, supančią aplinką ir jų struktūrą;

   d) trečiųjų šalių grėsmės įvertinimą, kurį, remdamasi daugiausia Europos Sąjungos delegacijos ataskaitomis, parengė INTCEN;

   e) įvertintą žvalgybos tarnybų, kurių veikla nukreipta prieš ES arba jos valstybes nares, keliamą grėsmę ir grėsmę dėl sabotažo, terorizmo, ardomosios arba kitų rūšių nusikalstamos veiklos.

4. EIVT saugumo institucija, taikydama nuodugnios apsaugos sąvoką, nustato tinkamas įgyvendintinas fizinio saugumo priemones. Tai gali būti viena (ar daugiau) iš šių priemonių:

   a) perimetro barjeras: fizinis barjeras, kuris skirtas zonos, kurioje reikalinga apsauga, ribos apsaugai užtikrinti;

   b) įsibrovimo aptikimo sistemos (ĮAS): ĮAS gali būti naudojama siekiant padidinti perimetro barjero teikiamo saugumo lygį arba patalpose ir pastatuose vietoj apsaugos personalo ar jam padėti;

   c) patekimo kontrolė: gali būti kontroliuojamas patekimas į objektą, pastatą ar pastatus objekte arba į zonas ar patalpas pastate. Kontrolė gali būti vykdoma elektroninėmis arba elektroninėmis-mechaninėmis priemonėmis, ją gali vykdyti apsaugos personalas ir (arba) priimamojo darbuotojas, arba ji gali būti vykdoma kitomis fizinėmis priemonėmis;

   d) apsaugos personalas: galima įdarbinti apmokytą ir prižiūrimą apsaugos personalą, jei reikia, tinkamai patikrinus jų patikimumą, *inter alia*, siekiant atgrasyti slaptą įsibrovimą planuojančius asmenis;

   e) apsauginės vaizdo stebėjimo sistemos (AVSS): apsaugos personalas gali naudotis AVSS, kad patikrintų incidentus ir ĮAS pavojaus signalus didelиuose objektuose ar ties perimetru;

   f) apsauginis apšvietimas: apsauginis apšvietimas ne tik skleidžia šviesą, būtiną veiksmingam stebėjimui, kurį tiesiogiai atlieka apsaugos personalas arba kuris netiesiogiai atliekamas per AVSS sistemą, bet jį taip pat galima naudoti siekiant atgrasyti potencialų įsibrovėlį;

   g) kitos tinkamos fizinės priemonės, skirtos atgrasyti asmenis be leidimo naudotis ESĮI, nustatyti tokio naudojimo atvejus arba užkirsti kelią tam, kad ESĮI būtų prarasta ar jai būtų padaryta žala.
5. Už saugumą atsakingam EIVT direktoratui leidžiama apieškoti įeinančius ir išeinančius asmenis siekiant atgrasyti, kad į patalpas arba pastatus be leidimo nebūtų įnešama medžiaga arba iš jų be leidimo nebūtų išnešama ESĮI.
6. Iškilus pavojui, kad ESĮI bus pamatyta, netgi atsitiktinai, imamasi tinkamų priemonių siekiant išvengti šio pavojaus.
7. Naujos infrastruktūros atveju infrastruktūros planavimo ir projektavimo metu apibrėžiami fizinio saugumo reikalavimai ir jos funkcinės specifikacijos. Esamos infrastruktūros atveju kiek įmanoma įgyvendinami fizinio saugumo reikalavimai.

III. ESĮI FIZINEI APSAUGAI SKIRTA ĮRANGA

8. Įsigydama ESĮI fizinei apsaugai užtikrinti skirtą įrangą (pavyzdžiui, apsaugines talpyklas, naikiklius, durų užraktus, elektronines patekimo kontrolės sistemas, įsibrovimo aptikimo sistemas, signalizacijos sistemas), EIVT saugumo institucija užtikrina, kad įranga atitiktų patvirtintus techninius standartus ir būtiniausius reikalavimus.
9. ESĮI fizinei apsaugai užtikrinti naudotinos įrangos techninės specifikacijos išdėstomos saugumo gairėse, kurias turi patvirtinti EIVT saugumo komitetas.
10. Saugumo sistemos reguliariai tikrinamos ir reguliariai atliekama įrangos priežiūra. Atliekant priežiūrą atsižvelgiama į patikrinimų rezultatus, kad būtų užtikrinta, jog įrenginiai toliau veiktų optimaliai.
11. Kiekvieno patikrinimo metu iš naujo vertinamas individualių saugumo priemonių ir visos saugumo sistemos veiksmingumas.

IV. FIZIŠKAI APSAUGOTOS ZONOS

12. ESĮI fizinės apsaugos tikslais nustatomos dviejų tipų fiziškai apsaugotos zonos arba nacionalinės lygiavertės zonos:

    a) administracinės zonos;

    b) saugios zonos (įskaitant techniniu požiūriu saugias zonas).
13. EIVT saugumo institucija nustato, kad zona atitinka reikalavimus, jog būtų klasifikuojama kaip administracinė zona, saugumo zona ar techniniu požiūriu saugi saugumo zona.
14. Administracinių zonų atveju:

    a) nustatomas aiškiai apribotas plotas, kad būtų galima tikrinti asmenis ir, jei įmanoma, transporto priemones;

    b) į šias zonas įeiti nelydimiems leidžiama tik tiems asmenims, kuriems už saugumą atsakingas EIVT direktoratas suteikė tinkamą leidimą;

    c) visi kiti asmenys turi būti visą laiką lydimi arba jiems turi būti taikomos lygiavertės kontrolės priemonės.

15. Saugių zonų atveju:

a) nustatoma aiškiai apibrėžta ir saugoma išorinė riba, per kurią kiekvienas įėjimas ir išėjimas yra kontroliuojamas naudojantis leidimų arba asmens atpažinimo sistema;

b) į zoną įeiti nelydimiems leidžiama tik tiems asmenims, kurių patikimumas tinkamai patikrintas ir kurie turi specialų leidimą įeiti į zoną pagal principą „būtina žinoti“;

c) visi kiti asmenys turi būti visą laiką lydimi arba jiems turi būti taikomos lygiavertės kontrolės priemonės.

16. Tais atvejais, kai įėjus į saugumo zoną galima visais praktiniais tikslais tiesiogiai susipažinti su joje laikoma įslaptinta informacija, taikomi tokie papildomi reikalavimai:

a) aiškiai nurodomas paprastai zonoje laikomos informacijos aukščiausio slaptumo žymos lygis;

b) visi lankytojai privalo turėti specialų leidimą, suteikiantį teisę įeiti į zoną, turi būti visą laiką lydimi ir jų patikimumas turi būti tinkamai patikrinamas, nebent imtasi priemonių užtikrinti, kad nebūtų įmanoma susipažinti su ESĮI;

c) į zoną draudžiama įnešti elektroninius prietaisus.

17. Nuo pasiklausymo apsaugotos saugios zonos klasifikuojamos kaip techniniu požiūriu saugios zonos. Taikomi šie papildomi reikalavimai:

a) tokiose zonose turi būti įdiegta ĮAS, ir kai jose nedirbama, jos turi būti rakinamos, o kai dirbama – saugomos. Visi raktai apskaitomi ir saugomi vadovaujantis šio priedo VI skyriumi;

b) visi į tokias zonas įeinantys asmenys ar įnešamos medžiagos kontroliuojami;

c) tokios zonos reguliariai fiziškai ir (arba) techniškai tikrinamos, kaip reikalauja EIVT saugumo institucija. Tokie patikrinimai atliekami, kai į zoną buvo įeita be leidimo ar įtariama apie tokį patekimą;

d) tokiose zonose negali būti ryšių linijų, kurioms nesuteiktas leidimas, telefonų, kuriems nesuteiktas leidimas, ar kitų ryšių prietaisų bei elektros ar elektroninės įrangos, kuriems nesuteiktas leidimas.

18. Nepaisant 17 dalies d punkto, prieš naudojantis ryšių prietaisais ir elektros ar elektronine įranga zonose, kuriose rengiami susitikimai ar atliekamas darbas, susijęs su SECRET UE/ES SECRET arba aukštesnio laipsnio slaptumo žyma pažymėta informacija, taip pat kai grėsmė ESĮI vertinama kaip didelė, tokius prietaisus ir įrangą visų pirma ištiria Komisijos saugumo institucija, siekdama užtikrinti, kad naudojantis šia įranga nebūtų galima perduoti jokios suprantamos informacijos per neapdairumą ar neteisėtai už saugios zonos ploto.
19. Saugumo zonos, kuriose nėra visą parą budinčio personalo, atitinkamais atvejais tikrinamos pasibaigus įprastai darbo dienai ir atsitiktiniais intervalais ne įprastomis darbo valandomis, išskyrus atvejus, kai įdiegta ĮAS.
20. Siekiant surengti susitikimą, kuriame naudojama įslaptinta informacija arba bet kokiu kitu panašiu tikslu administracinėje zonoje gali būti laikinai įrengtos saugumo zonos ir techniniu požiūriu saugios saugumo zonos.
21. Saugios eksploatacijos taisyklės rengiamos kiekvienai saugumo zonai ir jose nustatoma:

    a) ESĮI, kuri gali būti tvarkoma ir saugoma toje zonoje, slaptumo žymos lygis;

    b) įdiegtinos stebėjimo ir apsaugos priemonės;

    c) kokie asmenys turi leidimą nelydimi patekti į zoną, vadovaujantis principu „būtina žinoti“ ir asmens patikimumo pažymėjimu;

    d) atitinkamais atvejais palydos tvarka ir ESĮI apsaugos tvarka, kai kitiems asmenims leidžiama įeiti į zoną;

    e) bet kurios kitos atitinkamos priemonės ir procedūros.
22. Saugiose zonose įrengiamos saugyklos. Sienos, grindys, lubos, langai ir durys su užraktais patvirtinamos EIVT saugumo institucijos ir užtikrina apsaugą, kurią užtikrina apsauginės talpyklos, patvirtintos to paties lygio slaptumo žymos ESĮI saugoti.

V. FIZINĖS APSAUGOS PRIEMONĖS TVARKANT IR SAUGANT ESĮI

23. Slaptumo žyma RESTREINT UE/EU RESTRICTED pažymėta ESĮI gali būti tvarkoma:

a) saugiose zonose;

b) administracinėse zonose, jeigu ESĮI yra apsaugota taip, kad su ja negalėtų susipažinti leidimo neturintys asmenys;

c) ne saugumo zonose ar administracinėse zonose, jeigu turėtojas gabena ESĮI pagal A III priedo 30–42 dalis ir yra įsipareigojęs taikyti kompensacines priemones, nustatytas EIVT saugumo institucijos parengtose saugumo instrukcijose, kad būtų užtikrinta, jog ESĮI yra apsaugota taip, kad su ja negalėtų susipažinti leidimo neturintys asmenys.

24. Slaptumo žyma RESTREINT UE/EU RESTRICTED pažymėta ESĮI saugoma tinkamuose rakinamuose biuro balduose administracinėse zonose arba saugumo zonose. Laikinai ji gali būti saugoma ne saugumo zonose ar administracinėse zonose, jeigu turėtojas yra įsipareigojęs taikyti kompensacines priemones, nustatytas EIVT saugumo institucijos parengtose saugumo instrukcijose.

25. Slaptumo žyma CONFIDENTIEL UE/EU CONFIDENTIAL arba SECRET UE/EU SECRET pažymėta ESĮI gali būti tvarkoma:

a) saugiose zonose;

b) administracinėse zonose, jeigu ta ESĮI yra apsaugota taip, kad su ja negalėtų susipažinti leidimo neturintys asmenys;

c) ne saugiose zonose ar administracinėse zonose, jeigu turėtojas:

i) gabena ESĮI pagal A III priedo 30–42 dalis;

ii) yra įsipareigojęs taikyti kompensacines priemones, nustatytas EIVT saugumo institucijos parengtose saugumo instrukcijose, kad būtų užtikrinta, jog ESĮI yra apsaugota taip, kad su ja negalėtų susipažinti leidimo neturintys asmenys;

iii) visą laiką asmeniškai kontroliuoja šią ESĮI;

iv) jei dokumentai yra popieriniu pavidalu, apie tai pranešė atitinkamai registratūrai.

26. Slaptumo žyma CONFIDENTIEL UE/EU CONFIDENTIAL ir SECRET UE/EU SECRET pažymėta ESĮI saugoma saugumo zonose esančiose apsauginėse talpyklose arba saugyklose.
27. Slaptumo žyma TRES SECRET UE/EU TOP SECRET pažymėta ESĮI tvarkoma saugumo zonose.
28. Slaptumo žyma TRES SECRET UE/EU TOP SECRET pažymėta ESĮI saugoma būstinės saugumo zonose laikantis kurios nors iš toliau nurodytų sąlygų:

    a) apsauginėje talpykloje laikantis 8 dalies reikalavimų, taikant vieną ar kelias iš toliau nurodytų papildomų kontrolės priemonių:

    i) nuolatinė apsauga arba tikrinimas, kurį vykdo apsaugos personalas arba budintis personalas, kurio patikimumas patikrintas;

    ii) patvirtinta ĮAS kartu veikiant apsaugos reagavimo personalui;

    b) saugykloje su įrengta ĮAS kartu veikiant apsaugos reagavimo personalui.
29. ESĮI gabenimą už fiziškai apsaugotų zonų ribų reglamentuojančios taisyklės išdėstytos III priede.

VI. ESĮI APSAUGAI UŽTIKRINTI NAUDOJAMŲ RAKTŲ IR KODŲ KONTROLĖ

30. EIVT saugumo institucija nustato kabinetų, patalpų, saugyklų ir apsauginių talpyklų raktų bei kodų valdymo procedūras. Tokios procedūros apsaugo nuo neleistino susipažinimo su informacija.
31. Kodus įsimena kuo mažesnis asmenų, kuriems būtina juos žinoti, skaičius. Apsauginių talpyklų ir saugyklų, kuriose saugoma ESĮI, kodai keičiami:

    a) gavus naują talpyklą;

    b) pasikeitus kodus žinančiam personalui;

    c) neteisėtai atskleidus informaciją arba įtarus, kad tai padaryta;

    d) po spynos techninio patikrinimo ar taisymo;

    e) bent kas 12 mėnesių.

A III PRIEDAS

ĮSLAPTINTOS INFORMACIJOS ADMINISTRAVIMAS

I. ĮVADAS

1. Šiame priede pateiktos A priedo 7 straipsnio įgyvendinimo nuostatos. Jame išdėstytos administracinės ESĮI kontrolės visą jos gyvavimo ciklą priemonės siekiant atgrasyti nuo tokios informacijos sąmoningo ar atsitiktinio neteisėto atskleidimo arba praradimo, nustatyti tokius atvejus ir pašalinti jų padarinius.

II. ĮSLAPTINIMO ADMINISTRAVIMAS

Slaptumo ir kitos žymos

2. Informacija įslaptinama tuo atveju, jei dėl jos konfidencialumo reikia ją apsaugoti.
3. ESĮI rengėjas atsako už slaptumo žymos lygio nustatymą pagal atitinkamas įslaptinimo gaires ir už informacijos platinimą.
4. ESĮI slaptumo žymos lygis nustatomas vadovaujantis A priedo 2 straipsnio 2 dalimi ir remiantis saugumo gairėmis, kurios turi būti tvirtinamos pagal A priedo 3 straipsnio 3 dalį.
5. Valstybių narių įslaptintai informacijai, kuria jos keičiasi su EIVT, suteikiamas toks pat apsaugos lygis, koks suteikiamas atitinkamo slaptumo lygio ESĮI. Atitikmenų lentelė pateikiama šio sprendimo B priedėlyje.
6. Slaptumo žyma ir, jei taikytina, data ar konkretus įvykis, po kurio informacijos slaptumo žymos laipsnis gali būti sumažintas arba ji gali būti išslaptinta, nurodoma aiškiai ir teisingai, neatsižvelgiant į tai, ar ESĮI yra pateikiama popieriuje, žodžiu, elektronine ar bet kuria kita forma.
7. Atskiroms dokumento dalims (t. y. puslapiams, dalims, skirsniams, priedams ir priedėliams) gali būti suteikiamos skirtingos slaptumo žymos ir jos atitinkamai pažymimos, taip pat tais atvejais, kai jos saugomos elektronine forma.
8. Kiek įmanoma, dokumentams, kurių dalys pažymėtos skirtingo lygio slaptumo žymomis, suteikiama tokia struktūra, kad skirtingo lygio slaptumo žymomis pažymėtas dalis būtų galima lengvai nustatyti ir prireikus atskirti.

9. Dokumento ar dokumentų bylos bendras slaptumo žymos lygis nustatomas pagal aukščiausią slaptumo žymos lygį turinčią jo dalį. Kai renkama informacija iš įvairių šaltinių, galutinis dokumentas peržiūrimas siekiant nustatyti jo bendrą slaptumo žymos lygį, nes gali prireikti jam suteikti aukštesnį slaptumo žymos lygį nei jo dalims.
10. Pridedamų dokumentų lydinčiųjų dokumentų slaptumo žymos lygis atitinka priedų aukščiausio lygio slaptumo žymas. Jei tokie dokumentai pateikiami atskirai nuo priedų, įslaptintos informacijos rengėjas aiškiai nurodo, koks slaptumo žymos lygis jiems suteikiamas, naudodamas atitinkamą žymą, pavyzdžiui:

    CONFIDENTIEL UE/EU CONFIDENTIAL
    Be priedo (-ų) RESTREINT UE/EU RESTRICTED

Ženklai

11. Be vienos iš slaptumo žymų, nurodytų A priedo 2 straipsnio 2 dalyje, ESĮI gali būti pažymėta papildomomis žymomis, pavyzdžiui:

    a) identifikatoriumi, kuriuo nurodomas įslaptintos informacijos rengėjas;

    b) bet kuriomis žymomis, kodiniais žodžiais ar santrumpomis, kuriais nurodoma veiklos sritis, su kuria dokumentas yra susijęs, jo specialus platinimas vadovaujantis principu „būtina žinoti“ arba naudojimo apribojimai;

    c) paskirstymo žymomis.
12. Priėmus sprendimą suteikti ESĮI trečiajai valstybei ar tarptautinei organizacijai, už saugumą atsakingas EIVT direktoratas perduoda atitinkamą įslaptintą informaciją, pažymėtą leidimo suteikti informaciją žyma, nurodančia trečiąją valstybę ar tarptautinę organizaciją, kuriai ji suteikiama.
13. Patvirtintų žymų sąrašą tvirtina EIVT saugumo institucija.

Žymų santrumpos

14. Nurodant atskirų teksto pastraipų slaptumo žymos lygį gali būti naudojamos standartinės slaptumo žymų santrumpos. Santrumpos nepakeičia visais žodžiais nurodytų slaptumo žymų.

15. ES įslaptintuose dokumentuose gali būti naudojamos šios standartinės santrumpos, kuriomis nurodomas skirsnių arba teksto dalių, užimančių mažiau nei vieną puslapį, slaptumo žymos lygis:
TRES SECRET UE/EU TOP SECRET – TS-UE/EU-TS;
SECRET UE/EU SECRET – S-UE/EU-S;
CONFIDENTIEL UE/EU CONFIDENTIAL – C-UE/EU-C;
RESTREINT UE/EU RESTRICTED – R-UE/EU-R.

ESĮI rengimas

16. Rengiant ES įslaptintą dokumentą:

a) kiekvienas puslapis aiškiai pažymimas slaptumo žyma;

b) kiekvienas puslapis numeruojamas;

c) dokumente nurodomas jo numeris ir dalykas, kurie nėra įslaptinta informacija, išskyrus tuo atveju, kai jie pažymėti kaip įslaptinta informacija;

d) dokumente nurodoma data;

e) jei platinamos kelios dokumentų, pažymėtų CONFIDENTIEL UE/EU CONFIDENTIAL ar aukštesnio lygio slaptumo žyma, kopijos, kiekvienos iš jų kiekviename puslapyje nurodomas kopijos numeris.

17. Kai rengiant ESĮI neįmanoma taikyti 16 dalyje išdėstytų reikalavimų, taikomos kitos atitinkamos priemonės vadovaujantis saugumo gairėmis, parengtomis pagal šį sprendimą.

ESĮI slaptumo mažinimas ir ESĮI išslaptinimas

18. Įslaptintos informacijos rengėjas, kai įmanoma, rengdamas ESĮI, ypač RESTREINT UE/EU RESTRICTED slaptumo žyma pažymėtą informaciją, nurodo, ar tam tikrą dieną arba po tam tikro įvykio galima sumažinti ESĮI slaptumo žymos laipsnį arba ją išslaptinti.
19. EIVT reguliariai peržiūri jo turimą ESĮI, siekdama įsitikinti, ar slaptumo žymos lygis vis dar taikomas. EIVT sukuria sistemą, skirtą peržiūrėti registruotos ESĮI, kurią ji parengė, slaptumo žymos lygį ne rečiau kaip kas penkerius metus. Tokia peržiūra nėra reikalinga, jeigu įslaptintos informacijos rengėjas iš pat pradžių nurodo konkretų laiką, kada informacijos slaptumo žymos laipsnis bus sumažintas arba informacija bus išslaptinta automatiškai; informacija yra atitinkamai pažymėta.

III. ESĮI REGISTRAVIMAS SAUGUMO TIKSLAIS

20. Būstinėje įsteigiama centrinė registratūra. Kiekviename EIVT organizaciniame vienete, kuriame tvarkoma ESĮI, steigiamos atsakingos registratūros, pavaldžios centrinei registratūrai, siekiant užtikrinti, kad ESĮI būtų administruojama pagal šį sprendimą. Registratūros steigiamos kaip A priede apibrėžtos saugumo zonos.
    Kiekviena Europos Sąjungos delegacija įsteigia savo ESĮI registratūrą.
    Šioms registratūroms administruoti EIVT paskiria vyriausiąjį registratūros pareigūną.
21. Šiame sprendime registravimas saugumo tikslais (toliau – registravimas) – procedūrų, kuriomis užregistruojamas informacijos gyvavimo ciklas, įskaitant jo platinimą ir sunaikinimą, taikymas. RIS atveju registravimo procedūros gali būti atliekamos vykdant procesus pačioje RIS.
22. Kai organizacinis vienetas, įskaitant Europos Sąjungos delegacijas, gauna CONFIDENTIEL UE/EU CONFIDENTIAL ir aukštesnio lygio slaptumo žyma pažymėtą medžiagą ir kai ją išsiunčia, visa ši medžiaga registruojama. Slaptumo žyma TRES SECRET UE/ES TOP SECRET pažymėta informacija registruojama tam skirtose registratūrose.
23. EIVT būstinėje centrinė registratūra yra pagrindinis įslaptintos informacijos, kuria keičiamasi su trečiosiomis valstybėmis ir tarptautinėmis organizacijomis, gavimo ir išsiuntimo punktas. Ji registruoja visus šiuos keitimosi informacija atvejus.
24. EIVT saugumo institucija saugumo tikslais patvirtina ESĮI registravimo saugumo gaires pagal šio sprendimo 14 straipsnį.

TRES SECRET UE/EU TOP SECRET registratūros

25. EIVT būstinėje įsteigiama centrinė registratūra, kuri veikia kaip centrinė slaptumo žyma TRES SECRET UE/EU TOP SECRET pažymėtą informaciją gaunanti ir siunčianti institucija. Prireikus gali būti paskirtos antrinės registratūros, kurios tvarko tokią informaciją jos registravimo tikslais.

26. Tokios antrinės registratūros negali perduoti slaptumo žyma TRES SECRET UE/ES TOP SECRET pažymėtų dokumentų tiesiogiai kitoms tos pačios centrinės TRES SECRET UE/ES TOP SECRET registratūros antrinėms registratūroms arba į išorę be aiškaus rašytinio tos registratūros leidimo.

IV. ES ĮSLAPTINTŲ DOKUMENTŲ KOPIJAVIMAS IR VERTIMAS

27. Slaptumo žyma TRES SECRET UE/ES TOP SECRET pažymėti dokumentai kopijuojami arba verčiami tik gavus išankstinį rašytinį įslaptintos informacijos rengėjo sutikimą.
28. Jeigu SECRET UE/EU SECRET arba žemesnio laipsnio slaptumo žyma pažymėtų dokumentų įslaptintos informacijos rengėjas nenustatė apribojimų dėl jų kopijavimo ar vertimo, dokumento turėtojo nurodymu tokius dokumentus galima kopijuoti arba versti.
29. Dokumento kopijoms ir vertimams taikomos tokios pat saugumo priemonės kaip ir dokumento originalui. Dokumentų, pažymėtų CONFIDENTIEL UE/EU CONFIDENTIAL ar aukštesnio lygio slaptumo žyma, kopijas daro tik atitinkama (sub)registratūra, naudodama apsaugotą kopijavimo aparatą. Kopijos turi būti registruojamos.

V. ESĮI GABENIMAS

30. Gabenant ESĮI taikomos 32–42 dalyse išdėstytos apsaugos priemonės. Tais atvejais, kai ESĮI gabenama elektroninėje laikmenoje, ir nepaisant A priedo 7 straipsnio 4 dalies, toliau išvardytas apsaugos priemones gali papildyti EIVT saugumo institucijos nurodytos atitinkamos techninės kontrpriemonės, kad būtų sumažinta rizika, jog informacija bus prarasta ar neteisėtai atskleista.
31. EIVT saugumo institucija parengia ESĮI gabenimo instrukcijas pagal šį sprendimą.

Pastate arba uždaroje pastatų grupėje

32. Pastate arba uždaroje pastatų grupėje gabenama informacija turi būti uždengta, kad nebūtų galima stebėti jos turinio.

33. Slaptumo žyma TRES SECRET UE/EU TOP SECRET pažymėta informacija pastate arba uždaroje pastatų grupėje turi būti gabenama apsaugotame voke, ant kurio nurodytas tik gavėjo vardas ir pavardė; ją gabena asmenys, kurių patikimumas tinkamai patikrintas.

Europos Sąjungoje

34. ESĮI, gabenama iš vieno pastato ar patalpos į kitą Europos Sąjungoje, turi būti supakuota taip, kad ji būtų apsaugota nuo neteisėto atskleidimo.
35. SECRET UE/EU SECRET ir žemesnio laipsnio slaptumo žyma pažymėtą informaciją Europos Sąjungoje gabena:

    a) atitinkamai karinis, vyriausybinis ar diplomatinis kurjeris;

    b) kurjeris su sąlyga, kad:

    i) ESĮI nepaliekama be ją gabenančio asmens priežiūros, išskyrus tuo atveju, kai ji saugoma laikantis A II priede nustatytų reikalavimų;

    ii) paketas su ESĮI neatidaromas gabenimo metu arba ESĮI neskaitoma viešose vietose;

    iii) asmenų patikimumas patikrintas atitinkamu lygiu ir jie informuoti apie jų pareigas saugumo srityje;

    iv) prireikus asmenims suteikiamas kurjerio pažymėjimas;

    c) pašto tarnybos arba komercinės kurjerių pašto tarnybos su sąlyga, kad:

    i) jos yra patvirtintos atitinkamos NSI vadovaujantis nacionaliniais įstatymais ir kitais teisės aktais;

    ii) jos taiko atitinkamas apsaugos priemones, laikydamosi būtiniausių reikalavimų, kurie turi būti nustatyti saugumo gairėse pagal šio sprendimo 21 straipsnio 1 dalį.

    Gabenimo iš vienos valstybės narės į kitą atveju c punkto nuostatos taikomos tik gabenant informaciją, pažymėtą slaptumo žyma iki CONFIDENTIEL UE/EU CONFIDENTIAL.
36. CONFIDENTIEL UE/EU CONFIDENTIAL ir SECRET UE/EU SECRET slaptumo žyma pažymėtą medžiagą (pavyzdžiui, įrangą ar įrenginius), kurios negalima gabenti 34 dalyje nurodytomis priemonėmis, kaip krovinį, pagal A V priedą gabena komercinės vežėjų bendrovės.

37. TRES SECRET UE/EU TOP SECRET slaptumo žyma pažymėtą informaciją iš vieno pastato ar patalpos į kitą Europos Sąjungoje gabena atitinkamai karinis, vyriausybinis ar diplomatinis kurjeris.

Iš ES į trečiosios valstybės teritoriją arba tarp ES subjektų trečiosiose valstybėse

38. ESĮI, gabenama iš ES į trečiosios valstybės teritoriją arba tarp ES subjektų trečiosiose valstybėse, turi būti supakuota taip, kad ji būtų apsaugota nuo neteisėto atskleidimo.
39. CONFIDENTIEL UE/EU CONFIDENTIAL ir SECRET UE/EU SECRET slaptumo žyma pažymėtą informaciją iš ES į trečiosios valstybės teritoriją ir SECRET UE/EU SECRET slaptumo žyma pažymėtą informaciją tarp ES subjektų trečiosiose valstybėse gabena:

    a) karinis ar diplomatinis kurjeris;

    b) kurjeris jei:

    i) ant paketo yra oficialus spaudas arba ESĮI supakuota aiškiai nurodant, kad tai yra oficiali siunta ir jai neturėtų būti taikomas muitinės ar saugumo patikrinimas;

    ii) asmenys turi kurjerio pažymėjimą, kuriame nurodytas paketas ir kuris suteikia jiems teisę gabenti paketą;

    iii) ESĮI nepaliekama be ją gabenančio asmens priežiūros, išskyrus tuo atveju, kai ji saugoma laikantis A II priede nustatytų reikalavimų;

    iv) paketas su ESĮI neatidaromas gabenimo metu arba ESĮI neskaitoma viešose vietose;

    v) asmenų patikimumas patikrintas atitinkamu lygiu ir jie informuoti apie jų pareigas saugumo srityje.
40. Gabenant ES parengtą trečiajai valstybei ar tarptautinei organizacijai skirtą slaptumo žyma CONFIDENTIEL UE/EU CONFIDENTIAL ir SECRET UE/EU SECRET pažymėtą informaciją laikomasi atitinkamų nuostatų, numatytų susitarime dėl informacijos saugumo arba administraciniame susitarime pagal A priedo 10 straipsnio 2 dalį.
41. Slaptumo žyma RESTREINT UE/EU RESTRICTED pažymėtą informaciją iš ES į trečiosios valstybės teritoriją taip pat gali gabenti pašto tarnybos ar komercinės kurjerių pašto tarnybos.

42. Slaptumo žyma TRES SECRET UE/EU TOP SECRET pažymėtą informaciją iš ES į trečiosios valstybės teritoriją arba tarp ES subjektų trečiosiose valstybėse gabena karinis ar diplomatinis kurjeris.

VI. ESĮI NAIKINIMAS

43. Nebereikalingi ES įslaptinti dokumentai gali būti sunaikinti nepažeidžiant atitinkamų taisyklių ir nuostatų dėl archyvavimo.
44. Dokumentus, kurie turi būti registruojami pagal A priedo 7 straipsnio 2 dalį, turėtojo arba kompetentingos institucijos nurodymu sunaikina atsakinga registratūra. Registracijos knygos ir kita registravimo informacija atitinkamai atnaujinama.
45. Dokumentai, pažymėti SECRET UE/EU SECRET arba TRES SECRET UE/EU TOP SECRET slaptumo žyma, naikinami dalyvaujant liudytojui, kuris turi leidimą susipažinti su ne žemesnio už naikinamo dokumento slaptumo žymos laipsnio įslaptinta informacija.
46. Atsakingas registratūros darbuotojas ir liudytojas, kai pastarojo dalyvavimas privalomas, pasirašo sunaikinimo aktą, kuris registruojamas atitinkamame registre. Slaptumo žyma TRES SECRET UE/EU TOP SECRET pažymėtų dokumentų sunaikinimo aktai registre saugomi bent dešimt metų, o CONFIDENTIEL UE/EU CONFIDENTIAL ir SECRET UE/EU SECRET slaptumo žyma pažymėtų dokumentų – bent penkerius metus.
47. Įslaptinti dokumentai, įskaitant pažymėtus slaptumo žyma RESTREINT UE/EU RESTRICTED, sunaikinami tokiais būdais, kurie atitinka atitinkamus ES arba lygiaverčius standartus arba kuriuos valstybės narės patvirtino laikydamosi nacionalinių techninių standartų, kad jų nebūtų galima visiškai ar iš dalies atkurti.
48. Kompiuterinių duomenų saugojimo laikmenos, naudotos ESĮI, sunaikinamos taikant EIVT saugumo institucijos patvirtintas procedūras.

VII. SAUGUMO PATIKRINIMAI

EIVT saugumo patikrinimai

49. Pagal šio sprendimo 16 straipsnį EIVT saugumo patikrinimai yra:

a) bendrieji saugumo patikrinimai, kurių tikslas – nustatyti EIVT būstinės, Europos Sąjungos delegacijų ir visų EIVT priklausančių ir su EIVT susijusių patalpų bendrą saugumo lygį, visų pirma siekiant įvertinti EIVT saugumo interesų apsaugos priemonių efektyvumą;

b) EIVT saugumo patikrinimai, kurių tikslas – akreditacijos požiūriu įvertinti EIVT būstinėje ir Europos Sąjungos delegacijose įgyvendintų ESĮI apsaugos priemonių efektyvumą.

Tokie patikrinimai atliekami, *inter alia*, siekiant:

i) užtikrinti, kad būtų laikomasi šiame sprendime nustatytų būtiniausių ESĮI apsaugos standartų;

ii) tikrinamuose subjektuose pabrėžti saugumo ir veiksmingo rizikos valdymo svarbą;

iii) rekomenduoti atsakomąsias priemones konkrečiam įslaptintos informacijos konfidencialumo praradimo, jos vientisumo ar prieinamumo netekimo poveikiui sušvelninti;

iv) sustiprinti saugumo institucijų vykdomas švietimo saugumo klausimais ir sąmoningumo ugdymo programas.

EIVT saugumo patikrinimų vykdymas ir jų ataskaitų teikimas

50. EIVT saugumo patikrinimus vykdo už saugumą atsakingo EIVT direktorato patikrinimo grupė, jei reikia, padedant kitų ES institucijų ar valstybių narių saugumo ekspertams.
Patikrinimo grupei leidžiama patekti į visas vietas, kuriose tvarkoma ESĮI, visų pirma registratūras ir RIS įrengimo vietas.
51. Jei reikia, EIVT saugumo patikrinimus Europos Sąjungos delegacijose gali padėti vykdyti trečiosiose šalyse esančių valstybių narių ambasadų saugumo pareigūnai.
52. Iki kiekvienų kalendorinių metų pabaigos EIVT saugumo institucija patvirtina kitų metų EIVT tikrinimo programą.
53. Jei reikia, EIVT saugumo institucija gali vykdyti pirmiau nurodytoje programoje nenumatytus saugumo patikrinimus.

54. Pabaigus saugumo patikrinimą, tikrinamam subjektui pateikiamos pagrindinės išvados ir rekomendacijos. Po to patikrinimo grupė parengia patikrinimo ataskaitą. Jei buvo pasiūlyti taisomieji veiksmai ir pateiktos rekomendacijos, ataskaitoje padarytos išvados turėtų būti pakankamai išsamiai pagrįstos. Ataskaita pateikiama EIVT saugumo institucijai ir patikrinto subjekto vadovui. Už saugumą atsakingas EIVT direktoratas rengia reguliarią ataskaitą, skirtą nurodytu laikotarpiu atliktų patikrinimų metu įgytai ir EIVT saugumo komiteto išnagrinėtai patirčiai pabrėžti.

Saugumo patikrinimų vykdymas pagal ES sutarties V antraštinės dalies 2 skyrių įsteigtose ES agentūrose ir įstaigose ir šių patikrinimų ataskaitų teikimas

55. Jei reikia, už saugumą atsakingas EIVT direktoratas gali paskirti papildomus ekspertus, kurie dalyvautų jungtinėse ES patikrinimo grupėse, kurios vykdo saugumo patikrinimus ES agentūrose ir įstaigose, kurios įsteigtos pagal ES sutarties V antraštinės dalies 2 skyrių.

EIVT saugumo patikrinimų kontrolinis sąrašas

56. Už saugumą atsakingas EIVT direktoratas parengia ir atnaujina aspektų, kurie tikrintini vykdant EIVT saugumo patikrinimus, kontrolinį sąrašą. Šis kontrolinis sąrašas pateikiamas EIVT saugumo komitetui.
57. Kontroliniam sąrašui užpildyti būtina informacija gaunama visų pirma patikrinimo metu iš tikrinamo subjekto saugumo valdymo tarnybų. Į kontrolinį sąrašą įrašius išsamius atsakymus, susitarus su tikrinamu subjektu, sąrašas įslaptinamas. Jis negali būti patikrinimo ataskaitos sudedamoji dalis.

A IV PRIEDAS

RIS TVARKOMOS ESĮI APSAUGA

I. ĮVADAS

1. Šiame priede pateiktos A priedo 8 straipsnio įgyvendinimo nuostatos.
2. Toliau išdėstytos informacijos saugumo užtikrinimo (ISU) savybės ir sąvokos yra būtinos saugumui ir tinkamam ryšių ir informacijos sistemų (RIS) operacijų vykdymui užtikrinti:

   Autentiškumas – užtikrinimas, kad informacija yra tikra ir gauta iš *bona fide* šaltinių;

   Prieinamumas – galimybė leidimą turinčiam subjektui pateikus prašymą gauti informaciją ir ja naudotis;

   Konfidencialumas – savybė, kuri reiškia, kad informacija nėra atskleidžiama neturintiems leidimo asmenims, subjektams ar procesams;

   Vientisumas – savybė, kuri reiškia, kad apsaugomas informacijos tikslumas ir išsamumas bei turtas;

   Atsakomybės už veiksmus prisiėmimas – galimybė įrodyti, kad veiksmas buvo atliktas ar įvykis įvyko, kad šio įvykio ar veiksmo po to negalima būtų išsižadėti.

II. INFORMACIJOS SAUGUMO UŽTIKRINIMO PRINCIPAI

3. Toliau išdėstytos nuostatos yra RIS, kurioje tvarkoma ESĮI, saugumo užtikrinimo pagrindas. Išsamūs šių nuostatų įgyvendinimo reikalavimai nustatyti ISU saugumo gairėse.

Saugumo rizikos valdymas

4. Saugumo rizikos valdymas yra neatsiejama RIS apibrėžties, kūrimo, veikimo ir priežiūros dalis. Rizikos valdymą (įvertinimą, traktavimą, pripažinimą ir informavimą), kaip kartotinį procesą, kartu vykdo sistemos savininkų, projekto institucijų, vykdančiųjų institucijų ir saugumo patvirtinimo institucijų atstovai, taikydami patvirtintą, skaidrų ir visiškai suprantamą rizikos įvertinimo procesą. RIS ir jos turinio taikymo sritis aiškiai apibrėžiama rizikos valdymo proceso pradžioje.

5. EIVT kompetentingos institucijos peržiūri pavojus, kurie gali kilti RIS, ir nuolat vykdo naujausiais duomenimis grindžiamus ir tikslius pavojų įvertinimus, kurie atspindi esamą sistemos operacinę aplinką. Jos nuolat atnaujina savo žinias pažeidžiamumo klausimais ir reguliariai peržiūri pažeidžiamumo įvertinimą, neatsilikdamos nuo informacinių technologijų (IT) aplinkos pokyčių.
6. Tvarkant saugumo riziką siekiama taikyti apsaugos priemonių rinkinį, kuris užtikrina tinkamą vartotojų reikalavimų ir su saugumu susijusios likutinės rizikos pusiausvyrą.
7. RIS akreditavimui taikomi konkretūs reikalavimai, reikalavimai dėl informacijos apimties ir išsamumo, kuriuos nustato atitinkama saugumo akreditavimo institucija (SAI), turi atitikti įvertintą riziką, atsižvelgiant į visus svarbius veiksnius, įskaitant ESĮI, kuri tvarkoma RIS, slaptumo žymos lygį. Akreditavimas apima atsakingos institucijos oficialų pareiškimą dėl likutinės rizikos ir likutinės rizikos pripažinimą.

Saugumas viso RIS gyvavimo ciklo metu

8. Saugumas turi būti užtikrintas viso RIS gyvavimo ciklo metu – nuo pradžios iki naudojimosi pabaigos.
9. Kiekvienu gyvavimo ciklo etapu nustatomas kiekvieno RIS dalyvio ir jo sąveikos su kitais dalyviais vaidmuo saugumo požiūriu.
10. RIS, įskaitant technines ir netechnines saugumo priemones, bandomos saugumo požiūriu akreditavimo proceso metu siekiant užtikrinti tinkamą įgyvendintų saugumo priemonių lygį ir patikrinti, ar jos teisingai įgyvendintos, integruotos ir sukonfigūruotos.
11. Saugumo įvertinimai, patikrinimai ir peržiūros atliekami reguliariai RIS veikimo ir techninės priežiūros metu bei susidarius išskirtinėms aplinkybėms.
12. RIS saugumo dokumentų atnaujinimas viso jos gyvavimo ciklo metu vykdomas kaip neatsiejama pakeitimų atlikimo ir konfigūracijos tvarkymo proceso dalis.

Geriausia praktika

13. EIVT bendradarbiauja su TGS, Komisija ir valstybėmis narėmis, kad nustatytų geriausią praktiką RIS tvarkomos ESĮI apsaugos srityje. Geriausios praktikos gairėse išdėstomos RIS skirtos techninės, fizinės, organizacinės ir procedūrinės saugumo priemonės, kurių veiksmingumas apsisaugant nuo konkrečių grėsmių ir pažeidžiamumo buvo įrodytas.
14. RIS tvarkomos ESĮI apsauga grindžiama ir ES, ir už jos ribų ISU srityje dirbančių subjektų įgyta patirtimi.
15. Geriausios praktikos pavyzdžių platinimu ir jų įgyvendinimu prisidedama prie siekio užtikrinti lygiavertį įvairių EIVT naudojamų RIS, kuriose tvarkoma ESĮI, saugumo užtikrinimo lygį.

Nuodugni apsauga

16. Siekiant sušvelninti pavojų RIS, įgyvendinama daug techninių ir netechninių saugumo priemonių, kurios grupuojamos kaip kelios gynybinės linijos. Jos apima:

    a) ***atgrasymą*** – saugumo priemones, skirtas įtikinti nerengti priešiškų planų pulti RIS;

    b) ***prevenciją*** – saugumo priemones, skirtas apsunkinti RIS puolimą arba jam sutrukdyti;

    c) ***aptikimą*** – saugumo priemones, skirtas aptikti RIS puolimo atvejį;

    d) ***atsparumą*** – saugumo priemones, skirtas apriboti puolimo poveikį iki mažiausio informacijos rinkinio ar RIS dalių grupės bei užkirsti kelią tolesnei žalai;

    e) ***atstatymą*** **–** saugumo priemones, skirtas RIS saugiai padėčiai atkurti.

    Tokių saugumo priemonių griežtumo ir taikymo lygis nustatomas atsižvelgiant į rizikos įvertinimą.
17. EIVT kompetentingos institucijos užtikrina savo gebėjimus reaguoti į incidentus, kurie gali apimti kelias organizacijas ar valstybes, kad galėtų derinti reagavimo veiksmus ir dalytis informacija apie šiuos incidentus bei susijusią riziką (kompiuterinių incidentų tyrimo gebėjimai).

Minimalumo ir mažiausių privilegijų principas

18. Siekiant išvengti nereikalingos rizikos, įdiegiamos tik tos funkcijos, prietaisai ir paslaugos, kurie atitinka operacinius reikalavimus.
19. RIS naudotojams ir automatizuotiems procesams suteikiama tik tokia prieiga, privilegijos ar leidimai, kokios jiems reikia savo užduotims atlikti, siekiant apriboti žalą, kuri padaroma dėl avarijų, klaidų ar RIS išteklių naudojimo be leidimo.
20. RIS atliekamos registravimo procedūros prireikus patikrinamos akreditavimo proceso metu.

Informuotumas informacijos saugumo užtikrinimo srityje

21. Informuotumas apie riziką ir turimas saugumo priemones yra pirmoji RIS saugumo gynybos linija. Visų pirma visi personalo nariai, susiję su RIS gyvavimo ciklu, įskaitant naudotojus, suvokia:

    a) kad saugumo spragos gali labai pakenkti RIS ir visai organizacijai;

    b) galimą žalą kitiems, kuri gali kilti dėl tarpusavio sujungimo ir tarpusavio priklausomybės;

    c) savo asmeninę atsakomybę ir atskaitomybę už RIS saugumą atsižvelgdami į savo vaidmenį naudojant sistemas ir procesus.
22. Siekiant užtikrinti, kad būtų suvokiama atsakomybė už saugumą, visam dalyvaujančiam personalui, įskaitant aukštesniąją vadovybę ir RIS naudotojus, yra privalomi ISU švietimo ir informuotumo mokymai.

IT saugumo priemonių vertinimas ir patvirtinimas

23. Reikiamas saugumo priemonių patikimumo lygis apibrėžiamas kaip saugumo užtikrinimo lygis, nustatomas remiantis rizikos valdymo proceso rezultatais ir laikantis atitinkamos saugumo politikos bei saugumo gairių.
24. Saugumo užtikrinimo lygis patikrinamas naudojant tarptautiniu arba nacionaliniu lygiu patvirtintus procesus ir metodus. Tai apima pirminį įvertinimą, kontrolę ir auditą.
25. ESĮI apsaugai skirtas šifravimo priemones įvertina ir patvirtina valstybės narės nacionalinė kriptografijos patvirtinimo institucija (KPI).

26. Prieš rekomenduojant, kad pagal šio sprendimo 8 straipsnio 5 dalį jas patvirtintų EIVT KPI, tokias šifravimo priemones turi būti įvertinusi antra šalis, t. y. valstybės narės Tinkamos kvalifikacijos institucija (TKI), kuri nesusijusi su įrangos projektavimu arba gamyba. Reikalaujamas antros šalies įvertinimo išsamumo lygis priklauso nuo numatomo didžiausio ESĮI, kuri bus apsaugoma šiomis priemonėmis, slaptumo žymos laipsnio.
27. EIVT KPI, remdamasi Tarybos saugumo komiteto rekomendacija, gali netaikyti 25 arba 26 dalyse nustatytų reikalavimų ir tam tikram laikotarpiui suteikti laikiną patvirtinimą pagal šio sprendimo 8 straipsnio 5 dalyje nustatytą tvarką, kai tai pateisinama dėl konkrečių su veikla susijusių priežasčių.
28. TKI yra valstybės narės KPI, kuri buvo akredituota remiantis Tarybos nustatytais kriterijais antram ESĮI apsaugai skirtų šifravimo priemonių įvertinimui atlikti.
29. Vyriausiasis įgaliotinis patvirtina ne šifravimo IT saugumo priemonių reikalavimų atitikimo ir patvirtinimo saugumo politiką.

Perdavimas saugumo zonose

30. Nepaisant šio sprendimo nuostatų, kai ESĮI perdavimas vykdomas saugumo zonose arba administracinėse zonose, remiantis rizikos valdymo proceso rezultatais ir SAI pritarus gali būti naudojamas nešifruotas perdavimas arba šifravimas žemesniu lygiu.

Saugus RIS tarpusavio sujungimas

31. Šiame sprendime sistemų tarpusavio sujungimas reiškia tiesioginį dviejų ar daugiau IT sistemų sujungimą siekiant dalytis duomenimis ir kitais informacijos šaltiniais (pavyzdžiui, ryšiais) vienakrypčiu arba daugiakrypčiu būdu.
32. RIS kiekviena tarpusavyje sujungta IT sistema pirmiausia yra traktuojama kaip nepatikima ir sistemoje įdiegiamos apsaugos priemonės keitimuisi įslaptinta informacija kontroliuoti.

33. Bet kokio RIS ir kitos IT sistemos tarpusavio sujungimo atveju laikomasi toliau išdėstytų pagrindinių reikalavimų:

    a) tokiems tarpusavio sujungimams taikomus veiklos arba operacinius reikalavimus nurodo ir patvirtina atsakingos institucijos;

    b) tarpusavio sujungimui taikomas rizikos valdymas ir akreditavimo procesas bei yra reikalingas kompetentingų SAI patvirtinimas;

    c) ribų apsaugos priemonės (RAP) įdiegiamos visų RIS perimetre.
34. Akredituota RIS ir neapsaugotas arba viešas tinklas negali būti tarpusavyje sujungiami, išskyrus atvejus, kai tarp RIS ir neapsaugoto arba viešojo tinklo yra šiuo tikslu įdiegtos patvirtintos ribų apsaugos priemonės. Tokiems tarpusavio sujungimams taikytinas saugumo priemones peržiūri kompetentinga informacijos saugumo užtikrinimo institucija (ISUI) ir patvirtina kompetentinga SAI.

    Kai duomenys, perduodami neapsaugotu arba viešuoju tinklu, yra užšifruojami pagal šio sprendimo 8 straipsnio 5 dalį patvirtinta šifravimo priemone, toks sujungimas nelaikomas tarpusavio sujungimu.
35. Draudžiamas tiesioginis arba pakopinis RIS, akredituotos tvarkyti slaptumo žyma TRES SECFRET UE/EU TOP SECRET pažymėtą informaciją, ir neapsaugoto arba viešo tinklo tarpusavio sujungimas.

Kompiuterinių duomenų saugojimo laikmenos

36. Kompiuterinių duomenų saugojimo laikmenos sunaikinamos laikantis EIVT saugumo institucijos patvirtintų procedūrų.
37. Kompiuterinių duomenų saugojimo laikmenos gali būti naudojamos pakartotinai, gali būti sumažintas jų slaptumo žymos laipsnis arba jos gali būti išslaptinamos laikantis saugumo gairių, kurios turi būti nustatytos pagal šio sprendimo 8 straipsnio 2 dalį.

Nepaprastosios padėties sąlygos

38. Nepaisant šio sprendimo nuostatų, toliau apibūdintos specialios procedūros gali būti ribotą laiką taikomos esant nepaprastajai padėčiai, pavyzdžiui, gresiant ar esant krizei, konfliktui ar karinei padėčiai arba susidarius išskirtinėms su eksploatavimu susijusioms sąlygoms.
39. ESĮI gali būti perduodama naudojant šifravimo priemones, kurios buvo patvirtintos žemesnio įslaptinimo lygio informacijai, arba nešifruota kompetentingai institucijai pritarus, jei vėlavimas padarytų aiškiai didesnę žalą nei įslaptintos medžiagos atskleidimas ir jei:

    a) siuntėjas ir gavėjas neturi reikiamos šifravimo įrangos arba jokios šifravimo įrangos;

    b) įslaptinta medžiaga negali būti laiku perduota kitomis priemonėmis.
40. 39 dalyje išdėstytomis aplinkybėmis perduodama įslaptinta informacija nėra pažymėta jokiomis žymomis arba nuorodomis, kurios sudarytų sąlygas ją atskirti nuo neįslaptintos informacijos arba kurią galima apsaugoti naudojant turimas šifravimo priemones. Gavėjams kitomis priemonėmis nedelsiant pranešama apie informacijos slaptumo laipsnį.
41. Jeigu taikoma 39 dalis, EVIT saugumo direktoratui, o per jį – EIVT saugumo komitetui vėliau pateikiama ataskaita. Šioje ataskaitoje nurodomas kiekvieno ESĮI elemento siuntėjas, gavėjas ir rengėjas.

III. SU INFORMACIJOS SAUGUMO UŽTIKRINIMU SUSIJUSIOS FUNKCIJOS IR INSTITUCIJOS

42. EIVT nustatomos toliau išdėstytos su informacijos saugumo užtikrinimu susijusios funkcijos. Šioms funkcijoms nereikalingas vienas bendras organizacinis subjektas. Joms suteikiami atskiri įgaliojimai. Tačiau šios funkcijos ir su jomis susijusi atsakomybė gali būti sujungtos arba integruotos viename organizaciniame vienete arba padalytos skirtingiems organizaciniams vienetams, jei išvengiama vidaus interesų arba užduočių konfliktų.

Informacijos saugumo užtikrinimo institucija (ISUI)

43. ISUI atsako už šias sritis:

a) ISU srities saugumo gairių rengimą bei jų veiksmingumo ir reikšmingumo stebėjimą;

b) su šifravimo priemonėmis susijusios techninės informacijos apsaugą ir administravimą;

c) užtikrinimą, kad ESĮI apsaugai parinktos ISU priemonės atitiktų atitinkamas jų tinkamumo nustatymo ir atrankos gaires;
d) užtikrinimą, kad šifravimo priemonės būtų pasirenkamos laikantis jų tinkamumo nustatymo ir atrankos gairių;

e) mokymo ir informuotumo ISU srityje derinimą;

f) konsultavimąsi su sistemos tiekėju, saugumo srities subjektais ir vartotojų atstovais ISU saugumo gairių klausimais;

g) užtikrinimą, kad EIVT saugumo komiteto ISU klausimais ekspertų pogrupis turėtų atitinkamų žinių.

Institucija TEMPEST

44. TEI užtikrina, kad RIS atitiktų TEMPEST politiką ir gaires. Ji patvirtina TEMPEST kontrpriemones, skirtas įrenginiams ir priemonėms, siekiant apsaugoti ESĮI iki nustatyto slaptumo žymos laipsnio operacinėje aplinkoje.

Kriptografijos patvirtinimo institucija (KPI)

45. KPI institucija užtikrina šifravimo priemonių atitiktį atitinkamoms šifravimo gairėms. Ji patvirtina šifravimo priemonę, siekdama apsaugoti ESĮI iki nustatyto slaptumo žymos lygio jos operacinėje aplinkoje.

Kriptografijos platinimo institucija (KPLI)

46. KPLI atsako už šias sritis:

a) ES šifravimo medžiagos valdymą ir apskaitą;

b) užtikrinimą, kad visos ES šifravimo medžiagos apskaitai, saugiam tvarkymui, saugojimui ir platinimui būtų taikomos tinkamos procedūros ir nustatyti tinkami kanalai;

c) ES šifravimo medžiagos perdavimo ją naudojantiems asmenims ir tarnyboms arba priėmimo iš jų užtikrinimą.

Saugumo akreditavimo institucija (SAI)

47. Kiekvienai sistemai skirta SAI atsako už šias sritis:

a) užtikrinimą, kad RIS atitiktų atitinkamas saugumo gaires, pareiškimo dėl RIS patvirtinimo, leidžiant jas naudoti tvarkant ESĮI iki nustatyto slaptumo žymos laipsnio operacinėje aplinkoje, pateikimą, nurodant akreditavimo reikalavimus ir sąlygas bei kriterijus, kuriais remiantis sprendžiama, kad reikia iš naujo patvirtinti arba akredituoti RIS;

b) saugumo akreditavimo proceso nustatymą, vadovaujantis atitinkamomis gairėmis, aiškiai nurodant patvirtinimo sąlygas, nustatytas jos priežiūrai pavestoms RIS;

c) saugumo akreditavimo strategijos, kurioje išdėstytas akreditavimo proceso išsamumo lygis, atitinkantis reikiamą saugumo užtikrinimo lygį, nustatymą;

d) su saugumu susijusių dokumentų, įskaitant pareiškimus dėl rizikos valdymo ir likutinės rizikos, sistemos saugumo reikmių aktus (toliau – SSRA), saugumo įgyvendinimo patikrinimo dokumentus ir saugios eksploatacijos taisykles (toliau – SecOPs), nagrinėjimą ir patvirtinimą bei užtikrinimą, kad jie atitiktų EIVT saugumo taisykles ir gaires;

e) su RIS susijusių saugumo priemonių įgyvendinimo patikrinimą vykdant saugumo įvertinimus, patikrinimus ar peržiūras arba juos finansuojant;

f) saugumo reikalavimų (pavyzdžiui, susijusių su asmens patikimumo lygiais), taikomų svarbiausioms, susijusioms su RIS apsauga pareigoms, nustatymą;

g) patvirtintų šifravimo ir TEMPEST priemonių, naudojamų siekiant užtikrinti RIS saugumą, parinkimo patvirtinimą;

h) RIS tarpusavio sujungimo su kitomis RIS patvirtinimą arba prireikus dalyvavimą bendrame patvirtinime;

i) sistemos tiekėjo, saugumo srities subjektų ir vartotojų atstovų konsultavimą saugumo rizikos valdymo, visų pirma likutinės rizikos, ir pareiškimo dėl patvirtinimo reikalavimų ir sąlygų klausimais.

48. EIVT SAI atsako už visų į EIVT kompetencijos sritį patenkančių RIS akreditavimą.

Saugumo akreditavimo valdyba (SAV)

49. Jungtinė SAV atsakinga ir už EIVT SAI žinioje, ir už valstybių narių SAI žinioje esančių RIS akreditavimą. Ją sudaro po vieną kiekvienos valstybės narės SAI atstovą, o jos posėdžiuose dalyvauja TGS ir Komisijos atstovai SAI klausimais. Kiti subjektai, turintys prijungimo prie RIS mazgus, kviečiami dalyvauti posėdžiuose, kai svarstomi su ta sistema susiję klausimai.

    SAV pirmininkauja EIVT SAI atstovas. Ji sprendimus priima institucijų, valstybių narių ir kitų subjektų, turinčių prijungimo prie RIS mazgus, SAI atstovų sutarimu. SAV reguliariai teikia savo veiklos ataskaitas EIVT saugumo komitetui ir jam praneša apie visus pareiškimus dėl akreditavimo.

Informacijos saugumo užtikrinimo operacinė institucija

50. Kiekvienai sistemai skirta ISU operacinė institucija atsako už šias sritis:

    a) saugumo dokumentų, atitinkančių saugumo gaires, rengimą, visų pirma sistemos saugumo reikmių aktus (**SSRA**), įskaitant pareiškimą dėl likutinės rizikos, saugios eksploatacijos taisykles (**SecOPs**) ir šifravimo planą vykdant RIS akreditavimo procesą, rengimą;

    b) dalyvavimą atrenkant ir bandant konkrečioms sistemoms skirtas techninio saugumo priemones, prietaisus ir programinę įrangą, jų įgyvendinimo priežiūrą ir užtikrinimą, kad jie būtų saugiai įdiegti, sukonfigūruoti bei eksploatuojami pagal atitinkamus saugumo dokumentus;

    c) dalyvavimą parenkant TEMPEST saugumo priemones ir prietaisus, jei reikia pagal SSRA, ir užtikrinimą, kad jie būtų saugiai įdiegti ir eksploatuojami bendradarbiaujant su TEI;

    d) SecOPs įgyvendinimo ir taikymo stebėseną; prireikus atsakomybę už eksploatavimo saugumą deleguojant sistemos savininkui;

    e) šifravimo priemonių valdymą ir tvarkymą užtikrinant šifravimo ir kontroliuojamų objektų saugojimą ir prireikus užtikrinant šifravimo kintamųjų generavimą;

    f) saugumo analizės peržiūros ir bandymų atlikimą, visų pirma siekiant parengti atitinkamas rizikos ataskaitas, kurių reikalauja SAI;

    g) mokymo konkrečioms RIS skirto ISU klausimais rengimą;

    h) konkrečioms RIS skirtų apsaugos priemonių įgyvendinimą ir vykdymą.

A V PRIEDAS

PRAMONINIS SAUGUMAS

I. ĮVADAS

1. Šiame priede pateiktos A priedo 9 straipsnio įgyvendinimo nuostatos. Jame išdėstytos bendros saugumo nuostatos, taikomos pramonės ar kitiems subjektams derybų dėl sutarčių sudarymo metu arba visą EIVT sudarytų įslaptintų sutarčių gyvavimo ciklą.
2. EIVT saugumo institucija patvirtina pramoninio saugumo gaires, kuriose visų pirma apibrėžiami išsamūs reikalavimai, susiję su Įmonės patikimumą patvirtinančiu pažymėjimu (ĮPPP), saugumo aspektų paaiškinimais (SAP), vizitais, ESĮI perdavimu ir gabenimu.

II. SAUGUMO ASPEKTAI ĮSLAPTINTOSE SUTARTYSE

Slaptumo žymų vadovas (SŽV)

3. Prieš paskelbdama kvietimą teikti pasiūlymus įslaptintai sutarčiai sudaryti arba prieš sudarydama įslaptintą sutartį, EIVT, kaip perkančioji institucija, nustato visos informacijos, kuri turi būti suteikta konkurso dalyviams ir rangovams, slaptumo žymą, taip pat visos informacijos, kurią turi parengti rangovas, slaptumo žymą. Šiuo tikslu EIVT parengia SŽV, kuris turi būti naudojamas vykdant sutartį.
4. Siekiant nustatyti skirtingų įslaptintos sutarties dalių slaptumo žymą, taikomi toliau nurodyti principai:

   a) rengdama SŽV, EIVT atsižvelgia į visus svarbius saugumo aspektus, įskaitant slaptumo žymą, kurią informacijai priskyrė jos įslaptintos informacijos rengėjas ir kurią jis patvirtino kaip naudotiną tai sutarčiai;

   b) bendras sutarties slaptumo žymos laipsnis negali būti žemesnis nei aukščiausia bet kurio jos elemento slaptumo žyma;

   c) atitinkamais atvejais, jei daromi pakeitimai, susiję su slaptumo žymų suteikimu informacijai, parengtai rangovų ar jiems suteiktai vykdant sutartį, ir jei daromi vėlesni SŽV pakeitimai, EIVT palaiko ryšius su valstybių narių NSI/PSI ar kitomis atitinkamomis kompetentingomis saugumo institucijomis.

Saugumo aspektų paaiškinimas (SAP)

5. Konkrečioms sutartims skirti saugumo reikalavimai aprašomi SAP. Prireikus į SAP įtraukiamas SŽV; SAP yra neatsiejama įslaptintos sutarties ar subrangos sutarties dalis.
6. SAP nustatomos nuostatos, pagal kurias reikalaujama, kad rangovas ir (arba) subrangovas laikytųsi būtiniausių šiame sprendime nustatytų standartų. Šių būtiniausių standartų nesilaikymas gali būti pakankamas pagrindas sutarčiai nutraukti.

Programos / projekto saugumo instrukcijos (PRSI)

7. Atsižvelgiant į programų ar projektų, kuriuos vykdant reikia susipažinti su ESĮI arba ją tvarkyti ar saugoti, apimtį, programą ar projektą valdyti paskirta perkančioji institucija gali parengti konkrečios programos / projekto saugumo instrukcijas (PSI). PSI turi patvirtinti valstybių narių NSI/PSI ar kita programoje / projekte dalyvaujanti kompetentinga saugumo institucija; jose gali būti nustatyti papildomi saugumo reikalavimai.

III. ĮMONĖS PATIKIMUMĄ PATVIRTINANTIS PAŽYMĖJIMAS (ĮPPP)

8. Už saugumą atsakingas EIVT direktoratas prašo atitinkamos valstybės narės NSI, PSI ar kitos kompetentingos saugumo institucijos pagal nacionalinius įstatymus ir kitus teisės aktus suteikti ĮPPP, pažymintį, kad pramonės arba kitas subjektas savo patalpose gali apsaugoti atitinkamo slaptumo žymos (CONFIDENTIEL UE/EU CONFIDENTIAL arba SECRET UE/EU SECRET) lygio ESĮI. Rangovui ar subrangovui arba potencialiam rangovui ar subrangovui ESĮI arba galimybė susipažinti su ESĮI suteikiama tik tada, kai EIVT pateikiamas ĮPPP turėjimo įrodymas.
9. Atitinkamais atvejais EIVT, kaip perkančioji institucija, praneša atitinkamai NSI/PSI ar kitai kompetentingai saugumo institucijai, kad prieš sudarant sutartį arba sutarties vykdymui reikalingas ĮPPP. ĮPPP arba APP reikalaujama prieš sudarant sutartį, tais atvejais, kai ESĮI, pažymėta CONFIDENTIEL UE/EU CONFIDENTIAL arba SECRET UE/EU SECRET slaptumo žyma, turi būti suteikta paraiškų teikimo proceso metu.

10. EIVT, kaip perkančioji institucija, nesudaro įslaptintos sutarties su pasirinktu dalyviu prieš tai negavusi valstybės narės, kurioje yra registruotas atitinkamas rangovas ar subrangovas, NSI/PSI ar kitos kompetentingos saugumo institucijos patvirtinimo, kad reikiamais atvejais yra išduotas tinkamas ĮPPP.
11. EIVT, kaip perkančioji institucija, prašo NSI/PSI ar kitos ĮPPP išdavusios kompetentingos saugumo institucijos pranešti visą neigiamą informaciją, galinčią turėti įtakos ĮPPP. Subrangos sutarties atveju atitinkamai informuojama NSI/PSI ar kita kompetentinga saugumo institucija.
12. Jeigu atitinkama NSI/PSI ar kita kompetentinga saugumo institucija panaikina ĮPPP, tai yra pakankamas pagrindas EIVT, kaip perkančiajai institucijai, nutraukti įslaptintą sutartį arba pašalinti dalyvį iš konkurso.

IV. RANGOVO DARBUOTOJAMS IŠDUODAMI ASMENS PATIKIMUMO PAŽYMĖJIMAI (APP)

13. Visų subrangovo darbuotojų, kuriems reikia susipažinti su CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio lygio slaptumo žyma pažymėta ESĮI, patikimumas tinkamai patikrinamas ir jie atitinka principą „būtina žinoti“, kurio reikia norint susipažinti su informacija. Nors, norint susipažinti su informacija, pažymėta slaptumo žyma RESTREINT UE/EU RESTRICTED, APP nereikia, vis tiek reikia atitikti principą „būtina žinoti“.
14. Prašymai rangovo darbuotojams išduoti APP teikiami už atitinkamą subjektą atsakingai NSI/PSI.
15. Rangovams, norintiems įdarbinti trečiosios valstybės pilietį, kuris užimtų pareigas, kurias einant reikia susipažinti su ESĮI, EIVT praneša, kad už sprendimą, ar asmeniui suteikti teisę susipažinti su šia informacija pagal šį sprendimą, ir patvirtinimą, kad prieš suteikiant tokią teisę gautas informacijos rengėjo sutikimas, atsakinga valstybės narės, kurioje samdomasis subjektas yra įsikūręs ir įregistruotas, NSI/PSI.

V. ĮSLAPTINTOS SUTARTYS IR SUBRANGOS SUTARTYS

16. Tais atvejais, kai ESĮI suteikiama dalyviui prieš sudarant sutartį, kvietime teikti paraiškas numatoma nuostata, kuria paraiškos nepateikęs dalyvis arba dalyvis, kuris nebuvo atrinktas, įpareigojamas per nurodytą laiką grąžinti visus įslaptintus dokumentus.
17. Sudarius įslaptintą sutartį ar subrangos sutartį, EIVT, kaip perkančioji institucija, praneša rangovo ar subrangovo NSI/PSI ar kitai kompetentingai saugumo institucijai tos įslaptintos sutarties saugumo nuostatas.
18. Nutraukus tokią sutartį ar jai pasibaigus, EIVT, kaip perkančioji institucija (ir (arba) atitinkamai NSI/PSI ar kita kompetentinga saugumo institucija subrangos sutarties atveju) skubiai apie tai praneša valstybės narės, kurioje registruotas rangovas arba subrangovas, NSI/PSI ar kitai kompetentingai saugumo institucijai.
19. Paprastai reikalaujama, kad nutraukus įslaptintą sutartį ar subrangos sutartį ar jai pasibaigus rangovas arba subrangovas perkančiajai institucijai grąžintų visą turimą ESĮI.
20. Konkrečios nuostatos dėl ESĮI sunaikinimo vykdant sutartį, ją nutraukus arba jai pasibaigus nustatomos SAP.
21. Tais atvejais, kai rangovui arba subrangovui duotas leidimas nutraukus sutartį arba jai pasibaigus pasilikti ESĮI, rangovas ir subrangovas toliau laikosi šiame sprendime nustatytų būtiniausių standartų bei užtikrina ESĮI konfidencialumą.
22. Sąlygos, kuriomis rangovas gali sudaryti subrangos sutartis, nurodomos kvietime teikti paraiškas ir sutartyje.
23. Prieš sudarydamas subrangos sutartis dėl įslaptintos sutarties dalių, rangovas turi gauti EIVT, kaip perkančiosios institucijos, leidimą. Su pramonės arba kitais subjektais, registruotais valstybėje, kuri nėra ES valstybė narė ir nėra sudariusi susitarimo dėl informacijos saugumo su ES, subrangos sutartys negali būti sudaromos.
24. Rangovas atsako už tai, kad visa subrangos veikla būtų vykdoma laikantis šiame sprendime nustatytų būtiniausių standartų, ir negali suteikti subrangovui ESĮI be išankstinio rašytinio perkančiosios institucijos sutikimo.
25. ESĮI, kurią parengė ar tvarko rangovas arba subrangovas, atžvilgiu įslaptintos informacijos rengėjo teisėmis naudojasi perkančioji institucija.

VI. SU ĮSLAPTINTOMIS SUTARTIMIS SUSIJĘ VIZITAI

26. Jei EIVT, rangovams ar subrangovams vykdant įslaptintą sutartį jiems priklausančiose patalpose reikia susipažinti su CONFIDENTIEL UE/EU CONFIDENTIAL arba SECRET UE/EU SECRET slaptumo žyma pažymėta informacija, dėl jų vizitų susitariama palaikant ryšius su NSI/PSI arba kita susijusia kompetentinga saugumo institucija. Tai nepažeidžia NSI/PSI prerogatyvos konkrečių projektų atveju susitarti dėl tvarkos, pagal kurią dėl tokių vizitų gali būti susitariama tiesiogiai.
27. Tam, kad būtų leista susipažinti su ESĮI, susijusia su EIVT sutartimi, visi lankytojai turi turėti atitinkamą APP ir turi būti vadovaujamasi principu „būtina žinoti“.
28. Lankytojams leidžiama susipažinti tik su ta ESĮI, kuri yra susijusi su vizito tikslu.

VII. ESĮI PERDAVIMAS IR GABENIMAS

29. Perduodant ESĮI elektroninėmis priemonėmis taikomos atitinkamos A priedo 8 straipsnio ir A IV priedo nuostatos.
30. Gabenant ESĮI taikomos atitinkamos A III priedo nuostatos, laikantis nacionalinių įstatymų ir kitų teisės aktų.
31. Nustatant įslaptintos medžiagos kaip krovinio gabenimui taikomą saugumo tvarką taikomi toliau nurodyti principai:

    a) saugumas užtikrinamas visuose gabenimo etapuose nuo išgabenimo vietos iki galutinės paskirties vietos;

    b) siuntai suteikiamas apsaugos lygis nustatomas pagal joje esančios medžiagos aukščiausią slaptumo žymos lygį;

    c) gabenimą užtikrinančios bendrovės turi gauti atitinkamos slaptumo žymos ĮPPP, jei gabenant įslaptinta informacija saugoma rangovo patalpose. Bet kuriuo atveju siuntą gabenančio personalo patikimumas turi būti patikrintas pagal A I priedą;

d) prieš gabenant per valstybių sienas medžiagą, pažymėtą CONFIDENTIEL UE/EU CONFIDENTIAL arba SECRET UE/EU SECRET slaptumo žyma, siuntėjas parengia, o EIVT, jei reikia, bendradarbiaudama su siuntėjo ir gavėjo valstybių NSI/DSI ar kitomis atitinkamomis kompetentingomis saugumo institucijomis, patvirtina gabenimo planą;

e) stengiamasi, kad kelionės vyktų be sustojimo ir būtų užbaigtos kuo greičiau, atsižvelgiant į aplinkybes;

f) kai galima, turėtų būti pasirenkami maršrutai tik per valstybių narių teritorijas. Maršrutais per valstybes, kurios nėra valstybės narės, turėtų būti gabenama tik gavus EIVT arba siuntėjo ir gavėjo valstybių kompetentingų saugumo institucijų leidimą.

VIII. ESĮI PERDAVIMAS TREČIOSIOSE VALSTYBĖSE ĮSIKŪRUSIEMS RANGOVAMS

32. ESĮI trečiosiose valstybėse, kurios su ES yra sudariusios galiojantį saugumo susitarimą, įsikūrusiems rangovams ir subrangovams perduodama laikantis saugumo priemonių, dėl kurių susitarė EIVT, kaip perkančioji institucija, ir atitinkamos trečiosios valstybės, kurioje registruotas rangovas, NSI/PSI.

IX. RESTREINT UE/EU RESTRICTED SLAPTUMO ŽYMA PAŽYMĖTOS INFORMACIJOS TVARKYMAS IR SAUGOJIMAS

33. Palaikydama ryšius su valstybės narės NSI/PSI EIVT, kaip perkančioji institucija, prireikus turi teisę remiantis sutarties nuostatomis rengti vizitus į rangovo / subrangovo patalpas, kad patikrintų, ar įgyvendintos pagal sutartį reikalaujamos tinkamos saugumo priemonės, skirtos apsaugoti RESTREINT UE/EU RESTRICTED lygio slaptumo žyma pažymėtą ESĮI.
34. Kiek būtina pagal nacionalinius įstatymus ir kitus teisės aktus, NSI/PSI ar kitoms kompetentingoms saugumo institucijoms EIVT, kaip perkančioji institucija, praneša apie sutartis arba subrangos sutartis, kuriose yra RESTREINT UE/EU RESTRICTED slaptumo žyma pažymėtos informacijos.

35. EIVT sudarytų sutarčių, kuriose yra RESTREINT UE/EU RESTRICTED slaptumo žyma pažymėtos informacijos, atveju rangovai ar subrangovai ir jų personalas neprivalo turėti ĮPPP ar APP.
36. EIVT, kaip perkančioji institucija, išnagrinėja atsakymus į kvietimus dalyvauti konkurse dėl sutarčių, pagal kurias turi būti suteikta galimybė susipažinti su RESTREINT UE/EU RESTRICTED slaptumo žyma pažymėta informacija, neatsižvelgdama į reikalavimus, susijusius su ĮPPP ar APP, kurie gali būti numatyti nacionaliniuose įstatymuose ir kituose teisės aktuose.
37. Sąlygos, kuriomis rangovas gali sudaryti subrangos sutartis, turi atitikti 22–24 punktų reikalavimus.
38. Kai pagal sutartį numatytas informacijos, pažymėtos RESTREINT UE/EU RESTRICTED slaptumo žyma, tvarkymas rangovo naudojamoje RIS, EIVT, kaip perkančioji institucija, užtikrina, kad sutartyje arba subrangos sutartyje būtų nustatyti su RIS akreditavimu susiję būtini techniniai ir administraciniai reikalavimai, kurie atitiktų įvertintą riziką, atsižvelgiant į visus svarbius veiksnius. Perkančioji institucija ir atitinkama NSI/PSI susitaria dėl tokio RIS akreditavimo masto.

A VI PRIEDAS

KEITIMASIS ĮSLAPTINTA INFORMACIJA SU TREČIOSIOMIS ŠALIMIS IR TARPTAUTINĖMIS ORGANIZACIJOMIS

I. ĮVADAS

1. Šiame priede pateiktos A priedo 10 straipsnio įgyvendinimo nuostatos.

II. TVARKA, REGLAMENTUOJANTI KEITIMĄSI ĮSLAPTINTA INFORMACIJA

2. EIVT gali keistis ESĮI su trečiosiomis valstybėmis ar tarptautinėmis organizacijomis pagal A priedo 10 straipsnio 1 dalį.
Siekiant padėti vyriausiajam įgaliotiniui vykdyti SESV 218 straipsnyje nurodytas aplinkybes:

a) atitinkamas EIVT geografinis ar teminis departamentas, konsultuodamasis su už saugumą atsakingu EIVT direktoratu, reikiamais atvejais nustato ilgalaikio keitimosi ESĮI su atitinkama trečiąja valstybe ar tarptautine organizacija poreikį;

b) už saugumą atsakingas EIVT direktoratas, konsultuodamasis su atitinkamu EIVT geografiniu departamentu, reikiamais atvejais vyriausiajam įgaliotiniui teikia projektų tekstus, kuriuos ketinama pasiūlyti Tarybai pagal SESV 218 straipsnio 3, 5 ir 6 dalis;

c) už saugumą atsakingas EIVT direktoratas vyriausiajam įgaliotiniui padeda vykdyti derybas, savo veiksmus koordinuodamas su atitinkamomis Komisijos ir Tarybos generalinio sekretoriato tarnybomis;

d) susitarimų ar administracinių susitarimų su trečiosiomis valstybėmis dėl jų dalyvavimo BSGP krizių valdymo operacijose pagal A priedo 10 straipsnio 1 dalies c punktą atveju EIVT krizių valdymo ir planavimo direktoratas, konsultuodamasis su atitinkamomis EIVT tarnybomis, reikiamais atvejais vyriausiajam įgaliotiniui teikia projektų tekstus, kuriuos ketinama pasiūlyti Tarybai pagal SESV 218 straipsnio 3, 5 ir 6 dalis, ir vyriausiajam įgaliotiniui padeda vykdyti derybas, savo veiksmus koordinuodamas su atitinkamomis EIVT ir Tarybos generalinio sekretoriato tarnybomis.

3. Jei susitarimuose dėl informacijos saugumo numatytos techninio įgyvendinimo nuostatos, dėl kurių už saugumą atsakingas EIVT direktoratas, savo veiksmus koordinuodamas su Komisijos Žmogiškųjų išteklių ir saugumo generalinio direktorato Saugumo direktoratu ir Tarybos generalinio sekretoriato Saugumo tarnyba, susitaria su atitinkamos trečiosios valstybės ar tarptautinės organizacijos kompetentinga saugumo institucija, tokiose nuostatose atsižvelgiama į esamais teisės aktais, struktūromis ir procedūromis atitinkamoje trečiojoje valstybėje ar tarptautinėje organizacijoje užtikrinamą apsaugos lygį.
4. Esant ilgalaikiam poreikiui su trečiąja valstybe ar tarptautine organizacija keistis įslaptinta informacija, kurios slaptumo žymos lygis nėra aukštesnis nei RESTREINT UE/EU RESTRICTED, ir nustačius, kad atitinkama šalis neturi pakankamai išplėtotos tokiai informacijai skirtos saugumo sistemos, kad ta šalis galėtų sudaryti susitarimą dėl informacijos saugumo, vyriausiasis įgaliotinis gali, vieningai pritarus EIVT saugumo komitetui pagal šio sprendimo 15 straipsnio 5 dalį, sudaryti administracinį susitarimą su atitinkamos trečiosios valstybės ar tarptautinės organizacijos kompetentingomis saugumo institucijomis.
5. Keistis ESĮI su trečiąja valstybe ar tarptautine organizacija elektroninėmis priemonėmis neleidžiama, jei tai nėra aiškiai numatyta susitarime dėl informacijos saugumo arba administraciniame susitarime.
6. Pagal administracinį susitarimą dėl keitimosi įslaptinta informacija EIVT ir trečioji valstybė ar tarptautinė organizacija įsteigia savo registratūras, kurios yra pagrindiniai įslaptintos informacijos, kuria keičiamasi, gavimo ir išsiuntimo punktai. EIVT atveju tai EIVT centrinė registratūra.
7. Administraciniai susitarimai paprastai sudaromi pasikeičiant laiškais.

III. ĮVERTINIMO VIZITAI

8. Šio sprendimo 17 straipsnyje nurodyti įvertinimo vizitai vykdomi sudarius dvišalį susitarimą su atitinkama trečiąja valstybe ar tarptautine organizacija; jų metu vertinami šie aspektai:

   a) įslaptintai informacijai apsaugoti taikoma reglamentavimo sistema;

   b) bet kokie trečiosios valstybės ar tarptautinės organizacijos saugumo įstatymų, taisyklių, strategijų ar procedūrų ypatumai, kurie galėtų daryti poveikį įslaptintos informacijos, kuria gali būti keičiamasi, didžiausiam slaptumo žymos lygiui;

c) esamos saugumo priemonės ir procedūros, skirtos įslaptintai informacijai apsaugoti;

d) patikimumo patikrinimo procedūros, susijusios su numatomos suteikti ESĮI slaptumo žymos lygiu.

9. Kol neįvykdytas įvertinimo vizitas ir nenustatytas lygis, kuriuo šalys gali keistis įslaptinta informacija (remiantis jai suteikto apsaugos lygio lygiavertiškumo principu), ESĮI keistis negalima.

Jei prieš tokį įvertinimą vyriausiajam įgaliotiniui pranešama apie kokias nors išskirtines ar ypač svarbias priežastis keistis įslaptinta informacija, EIVT vykdo šiuos veiksmus:

a) visų pirma siekia gauti informacijos rengėjo rašytinį sutikimą, kad įsitikintų, kad nėra jokių prieštaravimų suteikti šią informaciją;

b) remiasi EIVT saugumo institucija, kuri gali nuspręsti suteikti informaciją, jei tam vieningai pritaria valstybės narės, atstovaujamos EIVT saugumo komitete.

Jei EIVT negali nustatyti atitinkamos informacijos rengėjo, EIVT saugumo institucija, gavusi vieningą EIVT saugumo komiteto narių pritarimą, perima rengėjo atsakomybę.

IV. LEIDIMAS SUTEIKTI ESĮI TREČIOSIOMS VALSTYBĖMS ARBA TARPTAUTINĖMS ORGANIZACIJOMS

10. Jei nustatyta keitimosi įslaptinta informacija su trečiąja valstybe ar tarptautine organizacija sistema pagal A priedo 10 straipsnio 1 dalį, sprendimą, kuriuo EIVT trečiajai valstybei ar tarptautinei organizacijai suteikia ESĮI, priima EIVT saugumo institucija, kuri tokio leidimo suteikimą gali deleguoti aukštesnio rango EIVT pareigūnams ar kitiems jos vadovaujamiems darbuotojams.
11. Jei EIVT nėra įslaptintos informacijos, kurią ketinama suteikti, rengėja, įskaitant pradinės medžiagos, kuri gali būti įtraukta į tą informaciją, rengėjus, EIVT pirmiausia prašo šios informacijos rengėjo pateikti rašytinį sutikimą suteikti šią informaciją, kad įsitikintų, kad nėra jokių prieštaravimų suteikti šią informaciją. Jei EIVT negali nustatyti atitinkamos informacijos rengėjo, EIVT saugumo institucija, gavusi vieningą valstybių narių, atstovaujamų EIVT saugumo komitete, pritarimą, perima rengėjo atsakomybę.

V. ESĮI AD HOC SUTEIKIMAS IŠIMTINE TVARKA

12. Jei nėra vienos iš A priedo 10 straipsnio 1 dalyje nurodytų sistemų ir jei ES arba vienai ar daugiau jos valstybių narių dėl politinių, operacinių ar labai svarbių priežasčių būtina suteikti ESĮI, ESĮI gali būti išimties tvarka suteikta trečiajai valstybei ar tarptautinei organizacijai, jei įvykdyti toliau nurodyti veiksmai.

    Už saugumą atsakingas EIVT direktoratas, įsitikinęs, kad pirmiau pateiktoje 11 dalyje nurodytos sąlygos įvykdytos:

    a) kiek įmanoma, patikrina atitinkamas trečiosios valstybės ar tarptautinės organizacijos saugumo institucijas, ar jų saugumo teisės aktai, struktūros bei procedūros yra pakankami, kad užtikrintų, jog joms suteikta ESĮI būtų apsaugota pagal ne mažiau griežtus standartus, nei yra nustatyti šiame sprendime;

    b) prašo EIVT saugumo komiteto remiantis turima informacija pateikti nuomonę, kiek galima pasitikėti atitinkamos trečiosios valstybės ar tarptautinės organizacijos, kuriai bus suteikta ESĮI, saugumo teisės aktais, struktūromis ir procedūromis;

    c) remiasi EIVT saugumo institucija, kuri gali nuspręsti suteikti informaciją, jei tam vieningai pritaria valstybės narės, atstovaujamos EIVT saugumo komitete.

13. Jei nėra vienos iš A priedo 10 straipsnio 1 dalyje nurodytų sistemų, atitinkama trečioji šalis raštu prašo tinkamai apsaugoti ESĮI.

A priedėlis

Apibrėžtys

Šiame sprendime vartojamų terminų apibrėžtys:

akreditavimas – procesas, po kurio Saugumo akreditavimo institucija (SAI) pateikia oficialų pareiškimą, patvirtinantį, kad sistemai yra leista veikti taikant nustatytą slaptumo žymos laipsnį konkrečiu slaptumo režimu jos operacinėje aplinkoje ir priimtinu rizikos lygiu, laikantis prielaidos, kad įgyvendintas patvirtintas techninių, fizinių, organizacinių ir procedūrinių saugumo priemonių rinkinys;

turtas – viskas, kas turi tam tikrą vertę organizacijai, jos veiklos operacijoms bei jų tęstinumui, įskaitant informacijos išteklius, padedančius vykdyti organizacijos misiją;

leidimas susipažinti su ESĮI – EIVT saugumo institucijos leidimas, kuris suteikiamas pagal šį sprendimą po to, kai valstybės narės kompetentingos institucijos suteikia APP, ir kuriuo pažymima, kad atitinkamam asmeniui, nustačius, kad jis atitinka principą „būtina žinoti“, suteikiamas leidimas iki nurodytos datos susipažinti su atitinkamo lygio slaptumo žyma (CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio lygio slaptumo žyma) pažymėta ESĮI (žr. A I priedo 2 straipsnį);

pažeidimas – šiame sprendime nustatytoms saugumo taisyklėms ir (arba) saugumo strategijoms ar gairėms, kuriose nustatytos šių taisyklių įgyvendinimo priemonės, priešingas asmens veiksmas arba neveikimas;

RIS gyvavimo ciklas – visa RIS egzistavimo trukmė, įskaitant inicijavimą, koncepciją, planavimą, reikalavimų analizę, projektavimą, sukūrimą, bandymą, įdiegimą, veikimą ir priežiūrą bei naudojimo nutraukimą;

įslaptinta sutartis – EIVT ir rangovo sudaryta prekių tiekimo, darbų vykdymo arba paslaugų teikimo sutartis, kurią vykdant reikia susipažinti su ESĮI ar ją rengti arba suteikiama galimybė su ja susipažinti ar ją rengti;

įslaptinta subrangos sutartis – EIVT rangovo ir kito rangovo (t. y. subrangovo) sudaryta prekių tiekimo, darbų vykdymo arba paslaugų teikimo sutartis, kurią vykdant reikia susipažinti su ESĮI ar ją rengti arba suteikiama galimybė su ja susipažinti ar ją rengti;

ryšių ir informacinė sistema (RIS) – sistema, sudaranti sąlygas tvarkyti informaciją elektroniniu būdu. Ryšių ir informacinė sistema ap-

ima visas sistemos dalis, kurių reikia jos veikimui, įskaitant infrastruktūrą, organizavimą, personalą ir informacijos išteklius, – žr. A priedo 8 straipsnio 2 dalį;

ESĮI neteisėtas atskleidimas – visiškas ar dalinis ESĮI atskleidimas leidimo neturintiems asmenims ar subjektams (žr. 9 straipsnio 2 dalį);

rangovas – fizinis arba juridinis asmuo, turintis teisnumą ir veiksnumą sudaryti sutartis;

šifravimo priemonės – šifravimo algoritmai, šifravimo techninės ir programinės įrangos moduliai, priemonės, apimančios vykdymo informaciją bei susijusius dokumentus ir raktų duomenis;

BSGP operacija – karinio ar civilinio krizių valdymo operacija vadovaujantis ES sutarties V antraštinės dalies 2 skyriumi;

išslaptinimas – bet kokios slaptumo žymos panaikinimas;

nuodugni apsauga – saugumo priemonių, kurios grupuojamos į kelis apsaugos lygius, taikymas;

paskirtoji saugumo institucija (PSI) – valstybės narės nacionalinei saugumo institucijai (NSI) atsakinga institucija, kuri atsako už pramonės ar kitų subjektų informavimą apie nacionalinę politiką visais pramoninio saugumo klausimais ir duoda nurodymus bei padeda ją įgyvendinti. PSI funkciją gali vykdyti NSI arba kita kompetentinga institucija;

dokumentas – fiksuota informacija, neatsižvelgiant į jos fizinę formą ar charakteristikas;

slaptumo žymos laipsnio sumažinimas – slaptumo žymos lygio sumažinimas;

ES įslaptinta informacija (ESĮI) – bet kuri informacija arba medžiaga, kurią neteisėtai atskleidus galėtų būti padaryta tam tikro dydžio žala Europos Sąjungos arba vienos ar kelių valstybių narių interesams ir kuriai suteikta ES slaptumo žyma – žr. 2 straipsnio f punktą);

įmonės patikimumą patvirtinantis pažymėjimas (ĮPPP) – NSI ar PSI administracinis patvirtinimas, kad saugumo požiūriu patalpose gali būti užtikrinta nurodyto slaptumo žymos lygio ESĮI tinkama apsauga ir kad buvo tinkamai patikrintas jose dirbančio personalo narių, kuriems reikia susipažinti su ESĮI, patikimumas bei jie buvo informuoti apie atitinkamus saugumo reikalavimus, būtinus norint susipažinti su ESĮI ir ją apsaugoti;

ESĮI administravimas – visi galimi veiksmai, kurie gali būti atliekami su ESĮI per visą jos gyvavimo ciklą. Tai apima ESĮI parengimą, ap-

dorojimą, gabenimą, slaptumo žymos laipsnio sumažinimą, išslaptinimą ir sunaikinimą. RIS atžvilgiu tai taip pat apima ESĮI rinkimą, skelbimą, perdavimą ir saugojimą;

turėtojas – tinkamą leidimą turintis asmuo, kuris atitinka principą „būtina žinoti“ ir turi ESĮI dalį bei yra atitinkamai atsakingas už jos apsaugą;

pramonės arba kitas subjektas – subjektas, tiekiantis prekes, vykdantis darbus arba teikiantis paslaugas; tai gali būti pramonės, prekybos, paslaugų, mokslo, mokslinių tyrimų, švietimo ar vystymo subjektas arba savarankiškai dirbantis asmuo;

pramoninis saugumas – priemonių, kurias rangovai arba subrangovai taiko derybų dėl sutarčių sudarymo metu ir visą įslaptintų sutarčių gyvavimo ciklą siekdami užtikrinti ESĮI apsaugą, taikymas – žr. A priedo 9 straipsnio 1 dalį;

informacijos saugumo užtikrinimas (ISU) ryšių ir informacinių sistemų srityje – užtikrinimas, kad tokiose sistemose tvarkoma informacija bus apsaugota ir kad, valdant teisėtiems naudotojams, jos veiks taip, kaip turi veikti, ir tada, kada turi veikti. Veiksmingas ISU užtikrina tinkamą konfidencialumo, vientisumo, prieinamumo, atsakomybės už veiksmus prisiėmimo ir autentiškumo lygį. ISU grindžiamas rizikos valdymo procesu – žr. A priedo 8 straipsnio 1 dalį;

šiame sprendime sistemų tarpusavio sujungimas – tiesioginis dviejų ar daugiau IT sistemų sujungimas siekiant dalytis duomenimis ir kitais informacijos šaltiniais (pavyzdžiui, ryšiais) vienakrypčiu arba daugiakrypčiu būdu – žr. A IV priedo 31 dalį;

įslaptintos informacijos administravimas – administracinių ESĮI kontrolės visą jos gyvavimo ciklą priemonių taikymas siekiant papildyti 5, 6 ir 8 straipsniuose numatytas priemones ir tokiu būdu atgrasyti nuo tokios informacijos sąmoningo ar atsitiktinio atskleidimo arba praradimo, nustatyti tokius atvejus ir pašalinti jų padarinius. Tokios priemonės visų pirma yra susijusios su ESĮI rengimu, registravimu, kopijavimu, vertimu, gabenimu, tvarkymu, saugojimu ir naikinimu – žr. A priedo 7 straipsnio 1 dalį;

medžiaga – dokumentas arba bet kokie pagaminti ar gaminami įrenginiai ar įranga;

rengėjas – ES institucija, agentūra ar įstaiga, valstybė narė, trečioji valstybė ar tarptautinė organizacija, kurios atsakomybe įslaptinta infor-

macija buvo parengta ir (arba) pateikta naudoti ES struktūrose;

personalo patikimumas – priemonių taikymas, siekiant užtikrinti, kad galimybė susipažinti su ESĮI būtų suteikta tik asmenims:

– kuriems „būtina žinoti“,
– kurių patikimumas patikrintas atitinkamu lygiu ir suteikta teisė prieiti prie informacijos, pažymėtos CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio lygio saugumo žyma, arba kiti tinkami leidimai pagal nacionalinius įstatymus ir kitus teisės aktus;
– kurie yra informuoti apie savo pareigas – žr. A priedo 5 straipsnio 1 dalį;

asmens patikimumo pažymėjimas (APP), kuriuo suteikiama teisė susipažinti su ESĮI – valstybės narės kompetentingos institucijos patvirtinimas, kuris pateikiamas valstybės narės kompetentingoms institucijoms baigus patikimumo tyrimą ir kuriuo pažymima, kad atitinkamam asmeniui, nustačius, kad jis atitinka principą „būtina žinoti“, suteikiamas leidimas iki nurodytos datos susipažinti su atitinkamo lygio slaptumo žyma (CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio lygio slaptumo žyma) pažymėta ESĮI; laikoma, kad asmens, kuriam taikoma ši apibrėžtis, patikimumas patikrintas;

asmens patikimumo pažymėjimą patvirtinanti pažyma (APPP) – kompetentingos institucijos išduota pažyma, kurioje nurodoma, kad asmens patikimumas yra patikrintas ir jis turi galiojantį APP arba už saugumą atsakingo direktorato vadovo leidimą susipažinti su ESĮI, ir nurodomas ESĮI, su kuria tam asmeniui gali būti leista susipažinti, slaptumo žymos lygis (CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma), atitinkamo APP galiojimo laikas ir pačios pažymos galiojimo laikas;

fizinis saugumas – fizinių ir techninių apsaugos priemonių taikymas siekiant užkirsti kelią leidimo neturintiems asmenims susipažinti su ESĮI – žr. A priedo 6 straipsnį;

programos / projekto saugumo instrukcijos – (PRSI) saugumo procedūrų, kurios yra taikomos konkrečiai programai / projektui, siekiant standartizuoti saugumo procedūras, sąrašas. Jos gali būti tikslinamos įgyvendinant programą / projektą;

registravimas – procedūrų, kuriomis užregistruojamas informacijos gyvavimo ciklas, įskaitant jo platinimą ir sunaikinimą, taikymas – žr. A III priedo 21 dalį);

likutinė rizika – rizika, kuri lieka po to, kai buvo įgyvendintos saugumo priemonės, atsižvelgiant į tai, kad ne nuo visų grėsmių apsisaugoma ir ne visi pažeidžiamumo aspektai gali būti pašalinti;

rizika – galimybė, kad tam tikros grėsmės atveju bus pasinaudota organizacijos ar sistemų vidiniu ir išoriniu pažeidžiamumu ir taip bus padaryta žala organizacijai ir jos materialiajam ar nematerialiajam turtui. Ji įvertinama atsižvelgiant į kylančios grėsmės tikimybę ir į jos poveikį;

rizikos pripažinimas – sprendimas atlikus rizikos tvarkymą pripažinti, kad vis dar yra likutinė rizika;

rizikos įvertinimas – grėsmių ir pažeidžiamų sričių nustatymas bei susijusios rizikos analizės, t. y. galimumo ir poveikio analizės, atlikimas;

informavimas apie riziką – RIS vartotojų bendruomenės informuotumo apie riziką didinimas, patvirtinimo institucijų informavimas apie tokią riziką ir pranešimų vykdančiosioms institucijoms teikimas;

saugumo rizikos valdymo procesas – visas nebūtinai galinčių įvykti atvejų, kurie gali paveikti organizacijos arba jos naudojamų sistemų saugumą, nustatymo, kontrolės ir mažinimo procesas. Jis apima visą su rizika susijusią veiklą, įskaitant jos įvertinimą, valdymą, pripažinimą ir informavimą apie ją;

rizikos valdymas – rizikos silpninimas, šalinimas, mažinimas (taikant tinkamas technines, fizines, organizacines arba procedūrines priemones), perkėlimas arba stebėjimas;

saugumo aspektų paaiškinimas (SAP) – specialių sutartinių sąlygų rinkinys, kurį parengia perkančioji institucija ir kuris yra įslaptintos sutarties, pagal kurią gali būti susipažįstama su ESĮI arba tokia informacija gali būti rengiama, sudėtinė dalis – jame nurodomi saugumo reikalavimai arba sutarties dalys, kurių saugumą būtina užtikrinti – žr. A V priedo II skyrių;

slaptumo žymų vadovas – (SŽV) dokumentas, kuriame aprašomos programos arba sutarties įslaptintos dalys, nurodant taikomus slaptumo žymų laipsnius. SŽV gali būti papildomas programos arba sutarties vykdymo laikotarpiu, o informacijos dalims gali būti suteiktos naujos slaptumo žymos arba jų slaptumo žymos laipsnis gali būti sumažintas; tais atvejais, kai yra parengtas SŽV, jis yra SAP dalis – žr. A V priedo II skyrių;

patikimumo tyrimas – tyrimo procedūros, kurias, vadovaudamasi valstybėje narėje galiojančiais įstatymais ir kitais teisės aktais, atlieka kompetentinga institucija, siekdama gauti užtikrinimą, kad nėra jo-

kios nepalankios informacijos, kuri neleistų asmeniui išduoti nacionalinio arba ES asmens patikimumo pažymėjimo, suteikiančio galimybę susipažinti su tam tikro lygio ESĮI (CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio lygio slaptumo žyma pažymėta informacija);

saugios eksploatacijos taisyklės (SecOPs) – saugumo politikos įgyvendinimo, kurį ketinama patvirtinti, eksploatacijos taisyklių, kurių reikia laikytis, ir personalo atsakomybės aprašas;

neskelbtina neįslaptinta informacija – informacija arba medžiaga, kurią EIVT privalo apsaugoti dėl Sutartyse ir priimtuose jų įgyvendinimo aktuose nustatytų teisinių prievolių ir (arba) dėl jos neskelbtinumo. Neskelbtina neįslaptinta informacija apima (bet neapsiriboja) informaciją ar medžiagą, kuriai taikoma tarnybinės paslapties saugojimo prievolė, kaip nurodyta SESV 339 straipsnyje, informaciją, kuri susijusi su interesais, saugomais Europos Parlamento ir Tarybos reglamento (EB) Nr. 1049/2001 ([1]) 4 straipsniu kartu su atitinkama Europos Sąjungos Teisingumo Teismo praktika, arba asmens duomenis, patenkančius į Reglamento (EB) Nr. 45/2001 taikymo sritį;

sistemos saugumo reikmių aktas (SSRA) – saugumo principų, kurių reikia laikytis, ir išsamių saugumo reikalavimų, kuriuos reikia įgyvendinti, rinkinys, kuris yra RIS sertifikavimo ir akreditavimo pagrindas;

TEMPEST – elektromagnetinio spinduliavimo, dėl kurio neteisėtai atskleidžiama informacija, tikrinimas, tyrimas bei kontrolė ir jo šalinimo priemonės;

grėsmė – galimas nepageidaujamas atvejis, dėl kurio gali būti padaryta žala organizacijai ar jos naudojamoms sistemoms; tokios grėsmės gali būti atsitiktinės arba tyčinės (piktybinės); jas apibūdina pavojingi elementai, galimi taikiniai ir puolimo būdai;

pažeidžiamumas – bet kokio pobūdžio silpnumas, kuriuo gali būti naudojamasi vienos ar daugiau grėsmių atveju. Pažeidžiamumas gali atsirasti dėl neveikimo arba gali būti susijęs su kontrolės stiprumo, išsamumo ar nuoseklumo trūkumu ir gali būti techninio, procedūrinio, fizinio, organizacinio ar veiklos pobūdžio.

([1]) 2001 m. gegužės 30 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 1049/2001 dėl galimybės visuomenei susipažinti su Europos Parlamento, Tarybos ir Komisijos dokumentais (OL L 145, 2001 5 31, p. 43).

B priedas

Saugumo klasifikacijų atitikmenys

EU	TRES SECRET UE/ EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
EURATOMAS	EURA TOP SECRET	EURA SECRET	EURA CONFIDENTIAL	EURA RESTRICTED
Belgija	Très Secret (Loi 11.12.1998) Zeer Geheim (Wet 11.12.1998)	Secret (Loi 11.12.1998) Geheim (Wet 11.12.1998)	Confidentiel (Loi 11.12.1998) Vertrouwelijk (Wet 11.12.1998)	Pastaba ([1])
Bulgarija	Строго секретно	Секретно	Поверително	За служебно ползване
Čekija	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Danija	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Vokietija	STRENG GEHEIM	GEHEIM	VS ([2]) – VERTRAULICH	VS – NUR FÜR DEN DIENSTGEBRAUCH
Estija	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Airija	Top Secret	Secret	Confidential	Restricted
Graikija	Άκρως Απόρρητο Santrumpa: ΑΑΠ	Απόρρητο Santrumpa: (ΑΠ)	Εμπιστευτικό Santrumpa: (ΕΜ)	Περιορισμένης Χρήσης Santrumpa: (ΠΧ)
Ispanija	SECRETO	RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
Prancūzija	Très Secret Défense	Secret Défense	Confidentiel Défense	Pastaba ([3])
Kroatija	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Italija	Segretissimo	Segreto	Riservatissimo	Riservato
Kipras	Άκρως Απόρρητο Santrumpa: (ΑΑΠ)	Απόρρητο Santrumpa: (ΑΠ)	Εμπιστευτικό Santrumpa: (ΕΜ)	Περιορισμένης Χρήσης Santrumpa: (ΠΧ)
Latvija	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Lietuva	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Liuksemburgas	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Vengrija	„Szigorúan titkos!“	„Titkos!“	„Bizalmas!“	„Korlátozott terjesztésű!“
Malta	L-Ogħla Segretezza	Sigriet	Kunfidenzjali	Ristrett
Nyderlandai	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK

Austrija	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Lenkija	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugalija	Muito Secreto	Suomija	Confidencial	Reservado
Rumunija	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu
Slovėnija	Strogo tajno	Tajno	Zaupno	Interno
Slovakija	Prísne tajné	Tajné	Dôverné	Vyhradené
Suomija	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Švedija ([4])	HEMLIG/TOP SECRET	HEMLIG/SECRET	HEMLIG/CONFIDENTIAL	HEMLIG/RESTRICTED
	HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG	HEMLIG	HEMLIG
Jungtinė Karalystė	UK TOP SECRET	UK SECRET	Ekvivalento nėra ([5])	UK OFFICIAL - SENSITIVE

([1]) Diffusion Restreinte/Beperkte Verspreiding nėra slaptumo žyma Belgijoje. Žyma RESTREINT UE/EU RESTRICTED pažymėtą informaciją Belgija tvarko ir saugo taip pat griežtai, kaip taikant nustatytus Europos Sąjungos Tarybos saugumo taisyklėse aprašytus standartus ir procedūras.

([2]) Vokietijoje: VS = Verschlusssache.

([3]) Prancūzijos nacionalinėje sistemoje slaptumo žyma RESTREINT nenaudojama. Žyma RESTREINT UE/EU RESTRICTED pažymėtą informaciją Prancūzija tvarko ir saugo taip pat griežtai, kaip taikant nustatytus Europos Sąjungos Tarybos saugumo taisyklėse aprašytus standartus ir procedūras.

([4]) Švedija: viršutinėje eilutėje nurodytas saugumo klasifikacijos žymas naudoja gynybos institucijos, o nurodytas apatinėje eilutėje – kitos institucijos.

([5]) Žyma CONFIDENTIEL UE/ES CONFIDENTIAL pažymėtą ESĮI Jungtinė Karalystė tvarko ir saugo laikydamasi žyma UK SECRET pažymėtai informacijai taikomų saugumo reikalavimų.

2.16. DECISION OF THE HIGH REPRESENTATIVE OF THE UNION FOR FOREIGN AFFAIRS AND SECURITY POLICY OF 19 SEPTEMBER 2017 ON THE SECURITY RULES FOR THE EUROPEAN EXTERNAL ACTION SERVICE ADMIN(2017) 10

Decision of the High Representative of the Union for Foreign Affairs and Security Policy of 19 September 2017 on the security rules for the European External Action Service

ADMIN(2017) 10

(2018/C 126/01)

THE HIGH REPRESENTATIVE OF THE UNION FOR FOREIGN AFFAIRS AND SECURITY POLICY,

Having regard to Council Decision 2010/427/EU of 26 July 2010 establishing the organisation and functioning of the European External Action Service ([1]) ('EEAS'),

Having regard to the opinion of the Committee referred to in Article 9(6) of the Decision of the High Representative of 15 June 2011 on the security rules for the European External Action Service ([2]),

Whereas:

(1) The EEAS, as a functionally autonomous body of the European Union (EU), should have security rules as referred to in Article 10(1) of the Council Decision 2010/427/EU;

(2) The High Representative of the Union for Foreign Affairs and Security Policy (hereinafter 'High Representative' or 'HR') should decide on security rules for the EEAS covering all aspects of security regarding the functioning of the EEAS, so that it can manage effectively the risks to staff placed under its responsibility, to its physical assets, information, and visitors, and fulfil its duty of care responsibilities in this regard;

(3) In particular, a level of protection should be afforded to staff placed under the responsibility of the EEAS, to EEAS physical assets, including communication and information systems, information, and visitors, which is in line with the best practice in the Council, the Commission, the Member States and, as appropriate, in international organisations;

(4) The security rules for the EEAS should help achieve a more coherent comprehensive general framework within the EU for protecting EU Classified Information (hereinafter referred to as 'EUCI'), building on, and maintaining as much coherence as possible with, the Council of the European Union (hereinafter referred to as 'the Council') security rules and the European Commission security provisions;

(5) The EEAS, the Council and the Commission are committed to applying equivalent security standards for protecting EUCI;

(6) This Decision is taken without prejudice to Articles 15 and 16 of the Treaty on the Functioning of the European Union (TFEU) and to instruments implementing them;

(7) It is necessary to establish the organisation of security in the EEAS and the allocation of security tasks within the EEAS structures;

(8) The High Representative should draw on relevant expertise in the Member States, in the General Secretariat of the Council and in the Commission as necessary;

(9) The High Representative should take all appropriate measures necessary to implement these rules with the support of the Member States, the General Secretariat of the Council and the Commission;

(10) The Secretary-General of the EEAS is the Security Authority of the EEAS, and Article 1 of Decision ADMIN (2015)34 of 14 September 2015 of the Secretary General of the European External Action Service provides that the security functions of the Security Authority, as provided for in the EEAS security rules, shall be exercised by the Director-General for budget and administration,

HAS ADOPTED THIS DECISION:

Article 1

Purpose and scope

This Decision lays down the security rules for the European External Action Service (hereinafter 'EEAS security rules').

Pursuant to Article 10(1) of Council Decision 2010/427/EU of 26 July 2010 establishing the organisation and functioning of the European External Action Service, it shall apply to all EEAS staff and all staff in Union Delegations, regardless of their administrative status or origin, and it shall establish the general regulatory framework for managing effectively the risks to staff placed under the responsibility of the EEAS as referred to in Article 2, to EEAS premises, physical assets, information, and visitors.

Article 2

Definitions

For the purpose of this decision, the following definitions shall apply:

(a) 'EEAS staff' means EEAS officials and other servants, including personnel from the diplomatic services of the Member States appointed as temporary agents, and seconded national experts, as defined in Article 6 of Council Decision 2010/427/EU of 26 July 2010 establishing the organisation and functioning of the European External Action Service.

(b) 'Staff placed under the responsibility of the EEAS' means the EEAS staff at Headquarters and in Union Delegations and all other staff in Union Delegations, regardless of their administrative status or origin, as well as, in the context of this decision, the High Representative and, as appropriate, other staff resident in EEAS Headquarters premises.

(c) 'Dependants' means the members of the family of the staff member placed under the responsibility of the EEAS in Union Delegations forming part of their respective household as notified to the Ministry for Foreign Affairs of the receiving State.

(d) 'EEAS premises' means all EEAS establishments, including buildings, offices, rooms and other areas, as well as areas housing communication and information systems (including those handling EUCI), where the EEAS conducts permanent or temporary activities.

(e) 'EEAS security interests' means the Staff placed under the responsibility of the EEAS, EEAS premises, dependants, physical assets, including communication and information systems, information, and visitors.

(f) 'EUCI' means any information or material designated by an EU security classification, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States.

(g) 'Union Delegation' means delegations to third countries and international organisations as referred to in Article 1(4) of Council Decision 2010/427/EU of 26 July 2010 establishing the organisation and functioning of the European External Action Service.

Other definitions are listed in the relevant Annexes and in Appendix A.

Article 3

Duty of care

1. The EEAS security rules shall aim at fulfilling the duty of care responsibilities of the EEAS.

2. The EEAS duty of care comprises due diligence in taking all reasonable steps to implement security measures to prevent reasonably foreseeable harm to EEAS security interests.

It encompasses both security and safety components, including those resulting from emergency situations or crises, whatever their nature.

3. Taking into account the duty of care responsibility of Member States, EU institutions or bodies and other parties with staff in Union Delegations and/or in Union Delegation premises, or such responsibility

incumbent upon the EEAS when Union Delegations are hosted in above mentioned other parties' premises, the EEAS shall enter into administrative arrangements with each of the above entities that shall address the respective roles and responsibilities, tasks and cooperation mechanisms.

Article 4

Physical and infrastructure security

1. The EEAS shall put in place all appropriate physical security measures (whether permanent or temporary), including access control arrangements, in all EEAS premises, for the protection of EEAS security interests. Such measures shall be taken into account in the design and the planning of new premises or before leasing existing premises.

2. Special obligations or restrictions can be imposed on staff placed under the responsibility of the EEAS and on dependants, for security reasons, for a specific period and in specific areas.

3. The measures referred to in paragraphs 1 and 2 shall be commensurate with the assessed risk.

Article 5

Alert states and management of crisis situations

1. The EEAS Security Authority as defined in Article 13(1), Section I, shall be responsible for putting in place appropriate alert state measures in anticipation of or in response to threats and incidents affecting security at the EEAS, and for measures required for managing crisis situations.

2. The alert state measures referred to in paragraph 1 shall be commensurate with the level of threat to security. The alert state levels shall be defined in close cooperation with the competent services of other Union institutions, agencies and bodies, and of the Member State or Member States hosting EEAS premises.

3. The EEAS Security Authority shall be the contact point for alert states and management of crisis situations.

Article 6

The protection of classified information

1. The protection of EUCI shall be governed by the requirements laid down in this decision, and in particular in Annex A. The holder of any item of EUCI shall be responsible for protecting it accordingly.

2. The EEAS shall ensure that access to classified information is only granted to individuals who meet the conditions set out in Article 5 of Annex A.

3. The conditions under which local agents may have access to EUCI shall also be laid down by the High Representative, in accordance with the rules for protecting EUCI laid down in Annex A to this decision.

4. The EEAS Directorate responsible for Security manages a database on the security clearance status of all staff placed under the responsibility of the EEAS and of EEAS contractors.

5. Where Member States introduce classified information bearing a national security classification marking into the structures or networks of the EEAS, the EEAS shall protect that information in accordance with the requirements applicable to EUCI at the equivalent level, as set out in the table of equivalence of security classifications contained in Appendix B to this decision.

6. Areas in the EEAS, in which information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above, or classified at an equivalent level, is stored, shall be established as Secured Areas in accordance with the rules pursuant to Annex AII to this decision, and shall be approved by the EEAS Security Authority.

7. Procedures for performing High Representative responsibilities in the framework of agreements or administrative arrangements for the exchange of EUCI with third States or international organisations are described in Annexes A and AVI of this Decision.

8. The Secretary General shall determine the conditions under which the EEAS may share EUCI held by it with other Union institutions, bodies, offices or agencies. An appropriate framework will be put in place to that effect, including by entering into interinstitutional agreements or other arrangements where necessary for that purpose.

9. Any such framework shall ensure that EUCI is given protection

appropriate to its classification level and according to basic principles and minimum standards which shall be equivalent to those laid down in this Decision.

Article 7

Security incidents and emergencies

1. In order to ensure a timely and effective response to security incidents, the EEAS shall establish a process for reporting such incidents and emergencies, which shall be operational twenty-four hours a day, seven days a week and cover any kind of security incidents or threats to the EEAS security interests (e.g. accidents, conflict, malicious acts, criminal acts, kidnap and hostage situations, medical emergencies, communication and information systems incidents, cyber-attacks, etc.).

2. Emergency liaison channels shall be established between the EEAS Headquarters, the Union Delegations, the Council, the Commission, the EU Special Representatives and Member States, to support them in managing security incidents involving personnel and their consequences, including contingency planning.

3. This security incident management shall include, inter alia:

– procedures for effectively supporting the decision-making process in relation to a security incident involving personnel, including decisions relating to the extraction or the suspension of a mission, and
– a policy and procedures for personnel recovery – e.g. in the case of missing personnel or kidnap and hostage situations – taking into account the particular responsibilities of the Member States, of the EU Institutions and of the EEAS in this regard. The need for specific capabilities, within the management of such operations in this regard, shall be considered taking into account the resources that could be provided by the Member States.

4. The EEAS shall put in place appropriate administrative arrangements for reporting security incidents in Union Delegations. When appropriate, the Member States, the Commission, any other relevant authority, as well as the relevant Security Committees shall be informed.

5. The incident management processes should be regularly exercised and reviewed.

Article 8

Security of communication and information systems

1. The EEAS shall protect information handled in communication and information systems ('CIS') against threats to confidentiality, integrity, availability, authenticity and non-repudiation.

2. Rules, security Guidelines and a security programme for protecting all CIS owned or operated by EEAS shall be approved by the EEAS Security Authority.

3. The rules, the policy and the programme shall be in conformity and their implementation closely coordinated with those of the Council and the Commission, and, where appropriate, with the security policies applied by the Member States.

4. All CIS handling classified information shall undergo an accreditation process. The EEAS shall apply a system for managing security accreditation in consultation with the General Secretariat of the Council and the Commission.

5. Where the protection of EUCI handled by the EEAS is provided by cryptographic products, such products shall be approved by the EEAS Crypto Approval Authority on a recommendation by the Council Security Committee.

6. The EEAS Security Authority shall, to the extent necessary, establish the following information assurance functions:

(a) an information assurance authority;

(b) a TEMPEST authority;

(c) a crypto approval authority;

(d) a crypto distribution authority.

7. For each system, the EEAS Security Authority shall establish the following functions:

(a) a security accreditation authority;

(b) an information assurance operational authority.

8. Provisions for implementing this Article as regards the protection of EUCI are set out in Annex A and A IV.

Article 9

Security breaches and compromise of classified information

1. A breach of security occurs as the result of an act or omission which is contrary to the security rules laid down in this Decision and/or to the security policies or guidelines setting out any measures necessary for its implementation, as approved in accordance with Article 21(1).

2. A compromise of classified information occurs when it has wholly or in part been disclosed to unauthorised persons or entities.

3. Any breach or suspected breach of security, and any compromise or suspected compromise of classified information shall be reported immediately to the EEAS Directorate responsible for security, which shall take appropriate measures as set out in Annex A, Article 11.

4. Any individual who is responsible for a breach of the security rules laid down in this Decision, or for compromising classified information, may be liable to disciplinary and/or legal action, in accordance with the applicable laws, rules and regulations, as set out in Article 11(3) of Annex A.

Article 10

Investigation of security incidents, breaches and/or compromises and corrective actions

1. Without prejudice to Article 86 (disciplinary measures) and Annex IX of the Staff Regulations ([3]), security investigations may be conducted by the EEAS Directorate responsible for security:

(a) in case of potential leakage, mishandling or compromise of EUCI, Euratom Classified Information or sensitive non-classified information;

(b) to counter hostile intelligence service attacks against the EEAS and its staff;

(c) to counter terrorist attacks against the EEAS and its staff;

(d) in case of cyber-incidents;

(e) in case of other incidents that affect or may affect general security at the EEAS, including suspected criminal offences;

2. The EEAS Directorate responsible for security assisted by experts

from Member States and/or from other EU institutions as appropriate, and upon authorisation from the EEAS Security Authority as necessary, shall implement any necessary corrective actions resulting from investigations, when and as appropriate.

Only staff authorised on the basis of a nominative mandate conferred on them by the EEAS Security Authority, given their current duties, may be entrusted with the power to conduct and coordinate security investigations in the EEAS.

3. Investigators shall have access to all information necessary for the conduct of such investigations and shall receive the full support of all EEAS services and staff in this regard.

Investigators may take appropriate actions to safeguard the trail of evidence in a manner that is proportionate to the seriousness of the matter under investigation.

4. Where access to information relates to personal data, including those contained in communication and information systems, such access shall be in accordance with Regulation (EC) 45/2001 ([4]).

5. Where it is necessary to establish an investigative database that will contain personal data, the European Data Protection Supervisor (EDPS) shall be notified in accordance with the aforementioned regulation.

Article 11

Security risk management

1. In order to determine its protective security needs, the EEAS shall develop, in close cooperation with the Security Directorate of the Commission and, where appropriate, with the Security Office of the General Secretariat of the Council, a comprehensive security risk assessment methodology.

2. Risks to EEAS security interests shall be managed as a process. This process shall be aimed at determining known security risks, at defining security measures to reduce such risks to an acceptable level and at applying measures in line with the concept of defence in depth. The effectiveness of such measures, and the level of risk, shall be continuously evaluated.

3. The roles, responsibilities and tasks laid down in this Decision are

without prejudice to the responsibility of each member of staff placed under the responsibility of the EEAS; in particular EU staff on mission in third countries must exercise common sense and good judgement with regard to their own safety and security, and comply with all applicable security rules, regulations, procedures and instructions.

4. In order to prevent and control risks to security, mandated staff may carry out background checks of persons falling under the scope of this Decision, so as to determine whether giving such persons access to EEAS premises or information presents a threat to security. For that purpose, and in compliance with Regulation (EC) No 45/2001, the mandated staff concerned may: (a) use any source of information available to the EEAS, taking into account the reliability of the source of information; (b) access the personnel file or data the EEAS holds with regard to individuals it employs or intends to employ, or for contractors' staff when duly justified.

5. The EEAS shall take all reasonable measures to ensure its security interests are protected, and to prevent reasonably foreseeable damage thereto.

6. Security measures in the EEAS for protecting EUCI throughout its life cycle shall be commensurate in particular with its security classification level, with the form and volume of the information or material, with the location and construction of facilities housing EUCI and with the threat, including the locally assessed threat, of malicious and/or criminal activities, including espionage, sabotage and terrorism.

Article 12

Security awareness and training

1. The EEAS Security Authority shall ensure that appropriate security awareness and training programmes are drawn up and implemented, and that Staff placed under the responsibility of the EEAS as well as, where appropriate, their dependants, receive the necessary awareness briefings and training commensurate with the risks in their place of work or residence.

2. Before being granted access to EUCI and at regular intervals thereafter, staff shall be briefed on and acknowledge their responsibilities to protect EUCI in accordance with the rules pursuant to Article 6.

Article 13

Organisation of security in the EEAS

1. The Secretary General shall be the Security Authority of the EEAS. In that capacity, the Secretary General shall ensure that:

(a) security measures are coordinated as necessary with the competent authorities of the Member States, the General Secretariat of the Council and the Commission, and, as appropriate, of third States or international organisations, on all security matters relevant for the EEAS' activities, including on the nature of risks to the EEAS security interests and the means of protection against them;

(b) security aspects are fully taken into account from the outset for all EEAS activities;

(c) access to classified information is only granted to individuals who meet the conditions set out in Article 5 of Annex A;

(d) a registry system is established which shall ensure that information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above is handled in accordance with this Decision within EEAS, and when released to EU Member States, EU Institutions, bodies or agencies or other authorised recipients. A separate record shall be kept of all EUCI released by the EEAS to third States or international organisations, and of all classified information received from third States or international organisations;

(e) security inspections referred to in Article 16 are undertaken;

(f) investigations are conducted into any actual or suspected breach of security, as well as into any actual or suspected compromise or loss of classified information held by or originated in the EEAS, and that the relevant security authorities are requested to assist in such investigations;

(g) appropriate incident and consequence management plans and mechanisms are established, in order to provide a timely and effective response to security incidents;

(h) appropriate measures are taken in the event of failure by individuals to comply with this Decision;

(i) appropriate physical and organisational measures are in place for the protection of the EEAS security interests.
In this regard, the EEAS Security Authority:
– sets the security category of the Union Delegations, in consultation with the Commission,
– decides, after consulting the HR, where appropriate, when Union Delegation staff should be evacuated if the security situation requires it,
– decides on the measures to be applied for the protection of dependants, when appropriate, taking into account arrangements with EU institutions as referred to in article 3(3);
– approves the crypto communication policy, in particular the programme of installation of cryptographic products and mechanism.

2. The EEAS Security Authority shall be assisted in this task by the DGBA, by the EEAS Director responsible for security, and, as appropriate, by the Deputy Secretary-General for CSDP and Crisis Response.

3. The Secretary-General as EEAS Security Authority may delegate tasks in this regard, as appropriate.

4. Each Head of department/division shall be responsible for implementing rules on protecting EUCI within his department/division.

Whilst remaining responsible as mentioned above, each Head of department/division shall designate staff for a Departmental Security Coordinator function, whose resources shall be proportionate to the amount of EUCI handled by that department/division.

Departmental Security Coordinators shall, when and as appropriate, assist and support their Head of department/division in performing tasks related to security, such as:

(a) developing any additional security requirements appropriate to the specific needs of the department/division;
(b) giving periodic security briefings to the members of their department/division;
(c) ensuring the need-to-know principle is respected in their department/division;
(d) maintaining up-to-date a list of safe codes and keys;

(e) maintaining security procedures and security measures;

(f) reporting any breaches of security and/or compromise of EUCI both to their Director and to the Directorate responsible for security;

(g) debriefing staff who cease to be employed by the EEAS;

(h) providing regular reports through their hierarchy on department/division's security matters;

(i) liaising with the EEAS Directorate responsible for security on security issues.

Any activity or issue that might have an impact on security shall be notified to the EEAS Directorate responsible for security in a timely manner.

5. Each Head of Delegation shall be responsible for implementing all measures relating to the security of the Union Delegation.

1. The EEAS shall have a Directorate responsible for security. It shall:

(a) manage, coordinate, supervise and/or implement all security measures in all premises under the responsibility of the EEAS, at Headquarters, within the EU and in third States;

(b) ensure coherence and consistency with this decision and with implementing provisions of any activity which may have an impact on protecting EEAS security interests;

(c) be the principal adviser of the HR, of the EEAS Security Authority and of the Deputy Secretary-General on all matters related to security;

(d) be assisted by the competent services of the Member States, in accordance with Article 10(3) of Council Decision 2010/427/EU establishing the organisation and functioning of the EEAS.

(e) support the activities of the EEAS Security Accreditation Authority by carrying out physical security assessments of the General Security Environment (GSE) / Local Security Environment (LSE) of communication and information systems handling EUCI, and of premises to be authorised for handling and storing EUCI.

2. The EEAS Director responsible for security shall be responsible for:

(a) ensuring the overall protection of the EEAS security interests;

(b) drafting, reviewing and updating of the security rules, as well as co-ordinating security measures with the competent authorities of the Member States and, as appropriate, the competent authorities of third States and international organisations linked to the EU by security agreements and/or arrangements;

(c) supporting the EEAS Security Committee proceedings, as set out in Article 15(1) of this Decision;

(d) liaising with any partners or authorities other than those under (b) above on security matters, where appropriate;

(e) prioritising and making proposals for the management of the budget for security in Headquarters and in Union Delegations.

3. The Head of the EEAS Directorate responsible for security shall:

(a) ensure that security breaches and compromises are recorded and investigations are launched and undertaken where and when necessary;

(b) meet regularly, and whenever necessary, to discuss areas of common interest with the Director of Security of the General Secretariat of the Council and the Director of the Security Directorate of the Commission.

4. The EEAS Directorate responsible for security shall establish contact and maintain close cooperation with:

– the departments in charge of security in the Ministries of Foreign Affairs of the Member States;

– the National Security Authorities (NSAs) and/or the other competent security authorities of Member States, to elicit their assistance in regard to the information it needs to assess such dangers and threats as may face the EEAS, its staff, its activities, its assets and resources and its classified information at its usual place of business;

– the competent security authorities of the Member States or Host States on the territory of which the EEAS may exercise its activity, regarding any matter relating to the protection of its staff, its activity, its assets and resources, and its classified information while on their territory;

– the Security Office of the General Secretariat of the Council and the Security Directorate of the Directorate General for Human Resources and Security of the Commission, and, where appropriate the security departments of the other EU institutions, bodies and agencies;

– the security departments of third States or international organisations, with a view to any useful co-ordination; and

– the Member States' NSAs, regarding any matter relating to the protection of EUCI.

1. Each Head of Delegation shall be responsible for locally implementing and managing all measures relating to the protection of

EEAS security interests within the Union Delegations' premises and competence.

In consultation with the competent authorities of the Host State when necessary, he will take all reasonably practicable measures to ensure that appropriate physical and organisational measures are in place to achieve this aim.

The Head of Delegation shall draw up security procedures for the protection of the dependants as defined in Article 2(c), when appropriate, taking into account any administrative arrangement, as referred to in Article 3(3). The Head of Delegation shall report on all security related issues within his remit to the Head of the EEAS Directorate responsible for security.

He shall be assisted, in these tasks, by the EEAS Directorate responsible for security, by the Union Delegation's Security Management Team which is composed of staff exercising security tasks and functions, and by security staff posted where necessary.

The Union Delegation shall establish regular contacts and maintain close cooperation in security matters with Member States' diplomatic missions.

2. In addition, the Head of Delegation will:

– establish detailed Union Delegation security and contingency plans, on the basis of generic standard operating procedures;
– operate an effective 24/7 system for managing security incidents and emergencies within the Union Delegation scope of operation;
– ensure that all staff deployed in the Union Delegation are covered by insurance as required by the conditions in the area;
– ensure that security is part of the Union Delegation induction training to be given to all staff deployed in the Union Delegation upon arriving in the Union Delegation; and
– ensure that any recommendations made following security assessments are implemented, and provide written reports at regular intervals on their implementation and on other security issues to the EEAS Security Authority.

3. Whilst remaining both responsible and accountable for safeguarding the security management as well as for ensuring corporate resilience, the Head of Delegation may delegate the execution of his or her security tasks to the Delegation Security Coordinator ('DSC'), being the Deputy Head of Delegation or, where none is appointed, an appropriate alternative.

In particular, the following responsibilities may be entrusted to the DSC:

– to coordinate security functions in the Union Delegation;
– to liaise on security issues with competent authorities of the host State and the appropriate counterparts in the Member States embassies and diplomatic missions;
– to implement appropriate security management procedures related to the EEAS Security interests, including the protection of EUCI;
– to ensure compliance with security rules and instructions;
– to brief staff about the security rules that are applicable to them, and on the particular risks in the host State;
– to submit requests to the EEAS Directorate responsible for security clearances regarding those positions which require a Personnel Security Clearance (PSC); and
– to keep the Head of Delegation, the Regional Security Officer (RSO) and the EEAS Directorate responsible for security continuously informed with regard to incidents or developments in the area which have a bearing on the protection of EEAS security interests.

4. The Head of Delegation may delegate security tasks of an administrative or technical character to the Head of Administration and other members of the Union Delegation's staff.

5. The Union Delegation shall be assisted by an RSO. The RSOs shall undertake the roles defined below in the Union Delegations within each of their respective geographical areas of responsibility.

In certain circumstances, where the prevailing security situation dictates, a dedicated RSO may be assigned to a specific Union Delegation as full time resident.

An RSO may be required to relocate to an area outside his present area of responsibility, including the Headquarters, or even take up a residential post according to the relevant security situation in any country, and as required by the EEAS Directorate responsible for security.

6. The RSOs shall be under the direct operational control of the EEAS Headquarters service in charge of Field Security, but under the shared administrative control of the Head of Delegation of their place of employment and the Headquarters service in charge of Field Security. They shall advise and assist the Head of Delegation and the Union Delegation's staff in arranging and implementing all physical, organisational and procedural measures related to the security of the

Union Delegation.

7. RSOs provide the Head of Delegation and Union Delegation staff with advice and support. Where appropriate, in particular where an RSO is a full time resident, he or she should assist a Union Delegation in security management and implementation, including the preparation of security contracts, the management of accreditations and clearances.

Article 14

CSDP Operations and EU Special Representatives

The EEAS Directorate responsible for security advises the Director of the Crisis Management and Planning Directorate (CMPD), the Director General of the EU Military Staff (EUMS), the Civilian Operations Commander heading the Civilian Planning and Conduct Capacity (CPCC), and the EU Military Operations Commanders on security aspects of CSDP operations, and the EU Special Representatives on security aspects of their mandate, complementary to the specific provisions existing in this regard in the relevant policies adopted by the Council.

Article 15

The EEAS Security Committee

1. An EEAS Security Committee is hereby established.

It shall be chaired by the EEAS Security Authority or a designated delegate, and shall meet as instructed by the Chair or at the request of any of its members. The EEAS Directorate responsible for security shall support the Chair in this function and provide administrative assistance, as necessary, to the Committee proceedings.

2. The EEAS Security Committee shall be composed of representatives of:

– each Member State;
– the Security Office of the General Secretariat of the Council;
– the Security Directorate of the Directorate General for Human Resources and Security of the Commission.

A Member State delegation to the EEAS Security Committee may consist of members of:

– the National Security Authority and/or the Designated Security Authority,
– the departments in charge of security in the Ministries of Foreign Affairs.

3. The Committee's representatives may be accompanied and advised by experts as they deem necessary. Representatives of other EU Institutions, agencies or bodies may be invited to attend when issues relevant to their security are discussed.

4. Without prejudice to paragraph 5 below, the EEAS Security Committee shall assist the EEAS, by means of consultation, on all security issues relevant to EEAS activities, to Headquarters and Union Delegations.

In particular, without prejudice to paragraph 5 below, the EEAS Security Committee:

(a) shall be consulted on:
  – security policies, guidelines, concepts or other methodology documents related to security, in particular as regards the protection of classified information and the measures to be taken in the event of a failure by EEAS staff to comply with the security rules;
  – technical security aspects which may influence the HR decision to submit a recommendation to the Council for the opening of negotiations for security of information agreements referred to in Article 10,1(a) of Annex A;
  – any amendments to this decision.

(b) may be consulted or informed, as appropriate, on issues relating to the security of staff and assets within EEAS Headquarters and Union Delegations, without prejudice to Article 3(3);

(c) shall be informed of any compromises or losses of EUCI occurred within the EEAS.

5. Any change to the rules relating to the protection of EUCI contained in this decision and its Annex A shall require the unanimous favourable opinion of the Member States as represented in the EEAS Security Committee. Such unanimous favourable opinion shall also be required before:

– entering into negotiations of administrative arrangements as referred to in Article 10(1)(b) of Annex A;

– releasing classified information in the exceptional circumstances referred to in Paragraphs 9, 11 and 12 of Annex A VI;
– assuming the information originator's responsibility in the circumstances referred to in Article 10(6), last sentence, of Annex A.

When a unanimous favourable opinion is requested, this condition will be met when no objections are expressed by Member States delegations during the Committee proceedings.

6. The EEAS Security Committee shall take full account of security policies and guidelines in force in the Council and the Commission.

7. The EEAS Security Committee receives the list of annual EEAS inspections, and the inspection reports, once finalised.

8. Organisation of the meetings:
– The EEAS Security Committee shall meet at least twice a year. Additional meetings, either in its fully fledged configuration or in NSA/DSA or in MFA security format, can be arranged by the Chair or requested by the members of the Committee.
– The EEAS Security Committee shall organise its activities in such a way that it can make recommendations on specific areas of security. It may establish other expert sub-areas as necessary. It shall draw up terms of reference for such expert sub-areas and receive reports from them on their activities.
– The EEAS Directorate responsible for security shall be responsible for preparing items for discussion. The Chair shall draw up the provisional agenda for each meeting. The members of the Committee may propose additional items for discussion.

Article 16

Security inspections

1. The EEAS Security Authority shall ensure that security inspections are undertaken, on a regular basis, within the EEAS Headquarters and within Union Delegations in order to assess the adequacy of security measures and to verify their compliance with this Decision. The EEAS Directorate responsible for security may, where appropriate, designate contributing experts to participate in security inspections to EU agencies and bodies established under title V, Chapter 2 of the TEU.

2. EEAS security inspections are conducted under the authority of the EEAS Directorate responsible for security and, when appropriate,

with the support of security experts representing other EU Institutions or Member States, in particular in the context of the arrangements referred to in Article 3(3).

3. The EEAS may draw, as necessary, on expertise in the Member States, in the General Secretariat of the Council and in the Commission.

Where necessary, relevant security experts based in Member State Missions in the third States and/or representatives of the diplomatic security departments of the Member States may be invited to participate in the security inspection of the Union Delegation.

4. Provisions for implementing this Article as regards the protection of EUCI are set out in Annex A III.

Article 17

Assessment visits

Assessment visits shall be arranged to ascertain the effectiveness of the security measures in place in a third State or international organisation for protecting EUCI exchanged under an administrative arrangement as referred to in Article 10(1)(b) of Annex A.

The EEAS Directorate responsible for security may designate contributing experts to participate in assessment visits to third States or international organisations with which the EU has concluded a Security of Information Agreement as referred to in Article 10(1)(a) of Annex A.

Article 18

Business continuity planning

The EEAS Directorate responsible for security shall assist the EEAS Security Authority in managing the security-related aspects of EEAS business continuity processes as part of the overall Business Continuity Planning of the EEAS.

Article 19

Travel advice for missions outside the EU

The EEAS Directorate responsible for security shall ensure the

availability of travel advice regarding missions of staff placed under the responsibility of the EEAS outside the EU, drawing upon the resources of all relevant services of the EEAS – in particular the SITROOM, the INTCEN, the geographical departments and the Union Delegations.

The EEAS Directorate responsible for security provides, on request, and drawing upon aforementioned resources, specific travel advice regarding missions by staff placed under the responsibility of the EEAS to third States presenting a high risk or an increased risk level.

Article 20

Health and safety

The EEAS security rules complement the EEAS rules for the protection of health and safety, as adopted by the High Representative.

Article 21

Implementation and review

1. The EEAS Security Authority shall, after consultation with the EEAS Security Committee as appropriate, approve security Guidelines setting out any measures necessary to implement these rules in the EEAS, and shall build up the necessary capacity covering all aspects of security, in close cooperation with the Member States' competent security authorities and with the support of the relevant services of the EU Institutions.

2. In accordance with article 4(5) of Council Decision 2010/427/EU of 26 July 2010 establishing the organisation and functioning of the European External Action Service, transitional arrangements may be used, as necessary, through service-level agreements with the relevant services of the General Secretariat of the Council and of the Commission.

3. The HR shall ensure overall consistency in the application of this Decision, and shall keep these security rules under review.

4. The EEAS security rules are to be implemented in close cooperation with the Member States' competent security authorities.

5. EEAS shall ensure that all aspects of the security process are taken into account within the EEAS crisis response system.

6. The Secretary General, as Security Authority, and the Head of the

EEAS Directorate responsible for security shall ensure implementation of this decision.

Article 22

Replacement of previous decisions

This decision shall repeal and replace the Decision of the High Representative of the Union for Foreign Affairs and Security Policy of 19 April 2013 on the security rules for the European External Action Service ([5]).

Article 23

Final provisions

This decision shall enter into force on the date of its signature.

It shall be published in the Official Journal of the European Union.

The competent authorities in the EEAS shall duly and timely inform all staff falling within the scope of this decision and its annexes, on the content, entry into force and any subsequent modifications thereof.

Done at Brussels, 19 September 2017.

Federica MOGHERINI

High Representative of the Union for Foreign Affairs and Security Policy

---

([1]) OJ L 201, 3.8.2010, p. 30.

([2]) OJ C 304, 15.10.2011, p. 7.

([3]) Staff regulations of Officials of the European Union and the Conditions of Employment of Other Servants of the European Union, laid down in Regulation (EEC, Euratom, ECSC) No 259/68 of the Council (OJ L 56, 4.3.1968, p. 1), hereinafter referred to as 'the Staff Regulations'.

([4]) Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).

([5]) OJ C 190, 29.6.2013, p. 1.

ANNEX A

PRINCIPLES AND STANDARDS FOR PROTECTING EUCI

Article 1

Purpose, scope and definitions

1. This Annex sets out the basic principles and minimum standards of security for protecting EUCI.

2. These basic principles and minimum standards shall apply to the EEAS and to Staff placed under the responsibility of the EEAS as referred to and defined respectively in Articles 1 and 2 of this Decision.

Article 2

Definition of EUCI, security classifications and markings

1. 'EU classified information' (EUCI) means any information or material designated by an EU security classification, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States.

2. EUCI shall be classified at one of the following levels:

(a) **TRES SECRET UE/EU TOP SECRET**: information and material the unauthorised disclosure of which could cause exceptionally grave prejudice to the essential interests of the European Union or of one or more of the Member States.

(b) **SECRET UE/EU SECRET**: information and material the unauthorised disclosure of which could seriously harm the essential interests of the European Union or of one or more of the Member States.

(c) **CONFIDENTIEL UE/EU CONFIDENTIAL**: information and material the unauthorised disclosure of which could harm the essential interests of the European Union or of one or more of the Member States.

(d) **RESTREINT UE/EU RESTRICTED**: information and material the unauthorised disclosure of which could be disadvantageous to the

interests of the European Union or of one or more of the Member States.

3. EUCI shall bear a security classification marking in accordance with paragraph 2. It may bear additional markings to designate the field of activity to which it relates, identify the originator, limit distribution, restrict use or indicate releasability.

Article 3

Classification management

1. The EEAS shall ensure that EUCI is appropriately classified, clearly identified as classified information and retains its classification level for only as long as necessary.

2. EUCI shall not be downgraded or declassified nor shall any of the markings referred to in Article 2(3) be modified or removed without the prior written consent of the originator.

3. The EEAS Security Authority shall approve, after consulting the EEAS Security Committee pursuant to Article 15(5) of this Decision, security Guidelines on creating EUCI which shall include a practical classification guide.

Article 4

Protection of classified information

1. EUCI shall be protected in accordance with this Decision.

2. The holder of any item of EUCI shall be responsible for protecting it in accordance with this Decision.

3. Where Member States introduce classified information bearing a national security classification marking into the structures or networks of the EEAS, the EEAS shall protect that information in accordance with the requirements applicable to EUCI at the equivalent level as set out in the table of equivalence of security classifications contained in Appendix B.

The EEAS shall establish appropriate procedures to maintain accurate records as to the originator of the

- classified information EEAS receives; and
- source material included in classified information originated by the EEAS.

The EEAS Security Committee shall be informed of these procedures.

4. Large quantities or a compilation of EUCI may warrant a level of protection corresponding to a higher classification than that of its components.

Article 5

Personnel security for handling EU classified information

1. Personnel security is the application of measures to ensure that access to EUCI is granted only to individuals who have:

– a need-to-know;
– for access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above, been security cleared to the relevant level, or are otherwise duly authorised by virtue of their functions in accordance with national laws and regulations; and
– been briefed on their responsibilities.

2. Personnel Security Clearance (PSC) procedures shall determine whether an individual, taking into account his loyalty, trustworthiness and reliability, may be authorised to access EUCI.

3. All individuals shall be briefed on and acknowledge in writing their responsibilities to protect EUCI in accordance with this Decision before being granted access to EUCI, and at regular intervals thereafter.

4. Provisions for implementing this Article are set out in Annex A I.

Article 6

Physical security of EU classified information

1. Physical security is the application of physical and technical protective measures to deter unauthorised access to EUCI.

2. Physical security measures shall be designed to deny surreptitious or forced entry by an intruder, to deter, impede and detect unauthorised actions and to allow for differentiation in personnel in their access to EUCI on a need-to-know basis. Such measures shall be determined based on a risk management process.

3. Physical security measures shall be put in place for all premises, buildings, offices, rooms and other areas in which EUCI is handled or stored, including areas housing communication and information systems

as defined in Article 8(2) of Annex A.

4. Areas in which EUCI classified CONFIDENTIEL UE/EU CONFIDENTIAL or above is stored shall be established as Secured Areas in accordance with Annex A II and approved by the EEAS Security Authority.

5. Only approved equipment or devices shall be used for protecting EUCI at the level CONFIDENTIEL UE/EU CONFIDENTIAL or above.

6. Provisions for implementing this Article are set out in Annex A II.

Article 7

Management of classified information

1. The management of classified information is the application of administrative measures for controlling EUCI throughout its life-cycle to supplement the measures provided for in Articles 5, 6 and 8 and thereby help deter, detect and recover from deliberate or accidental compromise or loss of such information. Such measures relate in particular to the creation, registration, copying, translation, carriage, handling, storage and destruction of EUCI.

2. Information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above shall be registered for security purposes prior to distribution and on receipt. The competent authorities in the EEAS shall establish a registry system for this purpose. Information classified TRES SECRET UE/EU TOP SECRET shall be registered in designated registries.

3. Services and premises where EUCI is handled or stored shall be subject to regular inspection by the EEAS Security Authority.

4. EUCI shall be conveyed between services and premises outside physically protected areas as follows:

(a) as a general rule, EUCI shall be transmitted by electronic means protected by cryptographic products approved in accordance with Article 7(5) of this Decision and according to clearly defined Security Operational Procedures (SecOPs);

(b) when the means referred to in point (a) are not used, EUCI shall be carried either:

(i) on electronic media (e.g. USB sticks, CDs, hard drives) protected by cryptographic products approved in accordance with Article 8(5) of this Decision; or

(ii) in all other cases, as prescribed by the EEAS Security Authority in accordance with the relevant protective measures laid down in Annex A III, Section V.

5. Provisions for implementing this Article are set out in Annex A III.

Article 8

Protection of EUCI handled in communication and information systems

1. Information Assurance (IA) in the field of communication and information systems is the confidence that such systems will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users. Effective IA shall ensure appropriate levels of confidentiality, integrity, availability, non-repudiation and authenticity. IA shall be based on a risk management process.

2. 'Communication and Information System' (CIS) means any system enabling the handling of information in electronic form. A communication and information system shall comprise the entire assets required for it to operate, including the infrastructure, organisation, personnel and information resources. This Annex shall apply to any EEAS CIS handling EUCI.

3. CIS shall handle EUCI in accordance with the concept of IA.

4. All CIS handling EUCI shall undergo an accreditation process. Accreditation shall aim at obtaining assurance that all appropriate security measures have been implemented and that a sufficient level of protection of the EUCI and of the CIS has been achieved in accordance with this Decision. The accreditation statement shall determine the maximum classification level of the information that may be handled in a CIS as well as the corresponding terms and conditions.

5. CIS handling information classified CONFIDENTIEL UE/EU CONFIDENTIAL and above shall be protected in such a way that the information cannot be compromised by unintentional electromagnetic

emanations ('TEMPEST security measures').

6. Where the protection of EUCI is provided by cryptographic products, such products shall be approved in accordance with Article 8(5) of this Decision.

7. During transmission of EUCI by electronic means, approved cryptographic products shall be used. Notwithstanding this requirement, specific procedures may be applied under emergency circumstances or specific technical configurations as specified in Annex A IV.

8. Pursuant to Article 8(6) of this Decision, the following IA functions will be established to the extent necessary:

(a) an IA Authority (IAA);

(b) a TEMPEST Authority (TA);

(c) a Crypto Approval Authority (CAA);

(d) a Crypto Distribution Authority (CDA).

9. Pursuant to Article 8(7) of this Decision, for each system shall be established:

(a) a Security Accreditation Authority (SAA);

(b) an IA Operational Authority.

10. Provisions for implementing this Article are set out in Annex A IV.

Article 9

Industrial security

1. Industrial security is the application of measures to ensure the protection of EUCI by contractors or subcontractors in pre-contract negotiations and throughout the life-cycle of classified contracts. As a general rule, such contracts shall not involve access to information classified TRES SECRET UE/EU TOP SECRET.

2. The EEAS may entrust by contract tasks involving or entailing access to or the handling or storage of EUCI by industrial or other entities registered in a Member State, or in a third State with which a security of information agreement or an administrative arrangement referred to in Article 10(1) of Annex A has been concluded.

3. The EEAS, as contracting authority, shall ensure that the minimum standards on industrial security set out in this Decision, and referred to in the contract, are complied with when awarding classified contracts to

industrial or other entities. It shall ensure compliance with such minimum standards through the relevant NSA/DSA.

4. Contractors or subcontractors registered in a Member State and participating in classified contracts or sub-contracts which are required to handle and store information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET within their facilities, either in the performance of such contracts or during the pre-contractual stage, shall hold a Facility Security Clearance (FSC) at the relevant classification level, granted by the NSA, DSA or any other competent security authority of the said Member State.

5. Contractor or subcontractor personnel who, for the performance of a classified contract, require access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET shall hold a PSC granted by the respective National Security Authority (NSA), Designated Security Authority (DSA) or any other competent security authority in accordance with national laws and regulations and the minimum standards laid down in Annex A I.

6. Provisions for implementing this Article are set out in Annex A V.

Article 10

Exchange of classified information with third States and International Organisations

1. The EEAS can only exchange EUCI with a third State or international organisation where:

(a) a security of information agreement between the EU and that third State or international organisation, concluded in accordance with Article 37 TEU and Article 218 TFEU, is in force; or

(b) an administrative arrangement between the HR and the competent security authorities of that third State or international organisation, for the exchange of information classified, in principle, no higher than RESTREINT UE/EU RESTRICTED, concluded in accordance with the procedure set out in Article 15(5) of this Decision, has taken effect; or

(c) a framework or ad-hoc participation agreement between the EU and that third State in the context of a CSDP crisis management operation, concluded in accordance with Article 37 TEU and Article 218 TFEU, is applicable,

and the conditions set out in that instrument have been met.

Exceptions to the general rule above are set out in Annex A VI, Section V.

2. Administrative arrangements referred to in paragraph 1(b) shall contain provisions to ensure that when third States or international organisations receive EUCI, such information is given protection appropriate to its classification level and according to minimum standards which are no less stringent than those laid down in this Decision.

Information exchanged on the basis of agreements referred to in paragraph 1(c) shall be limited to information concerning CSDP operations in which the third state in question participates on the basis of these agreements and in accordance with their provisions.

3. If a security of information agreement is subsequently concluded between the Union and a contributing third State or international organisation, the security of information agreement shall supersede the provision on exchange of classified information laid down in any framework participation agreement, ad hoc participation agreement or ad hoc administrative arrangement as far as the exchange and handling of EUCI is concerned.

4. EUCI generated for the purpose of a CSDP operation may be disclosed to personnel seconded to that operation by third States or international organisations in accordance with paragraphs 1-3 and Annex AVI. When authorising access to EUCI in premises or in CIS of a CSDP operation by such personnel, measures shall be applied (including recording of EUCI disclosed) to mitigate the risk of loss or compromise. Such measures shall be defined in relevant planning or mission documents.

5. Assessment visits to third States or international organisations, as referred to in Article 17 of this Decision shall be arranged to ascertain the effectiveness of the security measures in place for protecting any EUCI exchanged.

6. The decision to release EUCI held by the EEAS to a third State or international organisation shall be taken on a case-by-case basis,

according to the nature and content of such information, the recipient's need-to-know and the measure of advantage to the EU.

The EEAS shall seek the written consent of any entity which has provided classified information as source material for EUCI which the EEAS has originated, to establish that there are no objections to release.

If the originator of the classified information for which release is desired is not the EEAS, the EEAS shall first seek the originator's written consent to release.

If, however, the EEAS cannot establish the originator, the EEAS security authority shall assume the originator's responsibility after having obtained the unanimous favourable opinion of the Member States as represented in the EEAS Security Committee.

7. Provisions for implementing this Article are set out in Annex A VI.

Article 11

Breaches of security and compromise of classified information

1. Any breach or suspected breach of security, and any compromise or suspected compromise of classified information shall be reported immediately to the EEAS Directorate responsible for security, which shall inform, as appropriate, the Member State(s) concerned, or any other entity concerned.

2. Where it is known or where there are reasonable grounds to suspect that classified information has been compromised or lost, the EEAS Directorate responsible for security shall inform the NSA of the Member State(s) concerned and shall take all appropriate measures in accordance with the relevant laws and regulations to:

(a) safeguard evidence;

(b) ensure that the case is investigated by personnel not immediately concerned with the breach or compromise in order to establish the facts;

(c) immediately inform the originator or any other entity concerned;

(d) take appropriate measures to prevent a recurrence;

(e) assess the potential damage caused to the interests of the EU or of the Member States; and

(f) notify the appropriate authorities of the effects of the actual or suspected compromise and of the action taken.

3. Any member of staff under the responsibility of the EEAS who is responsible for a breach of the security rules laid down in this Decision may be liable to disciplinary action in accordance with the applicable rules and regulations.

Any individual who is responsible for the compromise or loss of classified information shall be liable to disciplinary and/or legal action in accordance with the applicable laws, rules and regulations.

4. Whilst an investigation into the breach and/or compromise is ongoing, the Head of the EEAS Directorate responsible for security may suspend the individual's access to EUCI and to EEAS premises. The Security Directorate of the Directorate General for Human Resources and Security of the Commission, the Security Office of the General Secretariat of the Council or the NSA of the Member State(s) or other entity concerned shall be immediately informed of this decision.

ANNEX A I

PERSONNEL SECURITY

I. INTRODUCTION

1. This Annex sets out provisions for implementing Article 5 of Annex A. It lays down in particular the criteria that the EEAS shall apply for determining whether an individual, taking into account his loyalty, trustworthiness and reliability, may be authorised to have access to EUCI, and the investigative and administrative procedures to be followed to that effect.
2. The 'Personnel Security Clearance' (PSC) for access to EUCI is a statement by a competent authority of a Member State which is made following completion of a security investigation conducted by the competent authorities of a Member State and which certifies that an individual may, provided his 'need-to-know' has been determined, be granted access to EUCI up to a specified level (CONFIDENTIEL UE/EU CONFIDENTIAL or above) until a specified date; the individual thus described is said to be 'security cleared'.

3. The 'Personnel Security Clearance Certificate' (PSCC) is a certificate issued by the EEAS Security authority establishing that an individual is security cleared, and which shows the level of EUCI to which that individual may be granted access, the date of validity of the relevant PSC and the date of the expiry of the certificate itself.
4. The 'Authorisation to access EUCI' is an authorisation by the EEAS Security Authority which is taken in accordance with this Decision after a PSC has been issued by the competent authorities of a Member State, and which certifies that an individual may, provided his 'need-to-know' has been determined, be granted access to EUCI up to a specified level (CONFIDENTIEL UE/EU CONFIDENTIAL or above) until a specified date; the individual thus described is said to be 'security cleared'.

II. AUTHORISING ACCESS TO EUCI

5. Access to information classified RESTREINT UE/EU RESTRICTED does not require a security clearance and is granted after:
   (a) the individual's statutory or contractual link to the EEAS has been established,
   (b) the individual's need-to-know has been determined,
   (c) he has been briefed on the security rules and procedures for protecting EUCI and has acknowledged in writing his responsibilities to protect EUCI in accordance with this Decision.
6. An individual shall only be authorised to access information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above after:
   (a) the individual's statutory or contractual link to the EEAS has been established;
   (b) his need-to-know has been determined;
   (c) he has been granted a PSC to the relevant level or is otherwise duly authorised by virtue of his functions in accordance with national laws and regulations; and
   (d) he has been briefed on the security rules and procedures for protecting EUCI and has acknowledged in writing his responsibilities with regard to protecting such information.
7. EEAS shall identify the positions in its structures which require access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above and therefore require a PSC to the relevant level, as referred to in paragraph 4 above.

8. EEAS Staff shall declare whether they hold the citizenship of more than one country.

PSC request procedures in the EEAS

9. For EEAS Staff, the EEAS Security Authority shall forward the completed personnel security questionnaire to the NSA of the Member State of which the individual is a national requesting that a security investigation be undertaken for the level of EUCI to which the individual will require access.
10. Where an individual holds citizenship of more than one country, the vetting request will be addressed to the NSA of the country under whose nationality the person has been recruited.
11. Where information relevant for a security investigation becomes known to the EEAS concerning an individual who has applied for a PSC, the EEAS, acting in accordance with the relevant rules and regulations, shall notify the relevant NSA thereof.
12. Following completion of the security investigation, the relevant NSA shall notify the EEAS Directorate responsible for security of the outcome of such an investigation.
    (a) Where the security investigation results in an assurance that nothing adverse is known which would call into question the loyalty, trustworthiness and reliability of the individual, the EEAS Security Authority may grant the individual concerned an Authorisation to access EUCI up to the relevant level until a specified date;
    (b) The EEAS shall take all appropriate measures to ensure that conditions or restrictions imposed by the NSA are duly implemented. The NSA will be informed about the outcome.
    (c) Where the security investigation does not result in such an assurance, the EEAS Security Authority shall notify the individual concerned, who may ask to be heard by the EEAS Security Authority. The EEAS Security Authority may ask the competent NSA for any further clarification it can provide according to its national laws and regulations. If the outcome is confirmed, an Authorisation to access EUCI shall not be granted. In that case EEAS shall take all appropriate measures to ensure that the applicant will be denied any access to EUCI.

13. The security investigation together with the results obtained, on which the EEAS bases its decision on whether or not to grant an authorisation to access EUCI, shall be subject to the relevant laws and regulations in force in the Member State concerned, including those concerning appeals. Decisions by the EEAS Security Authority shall be subject to appeals in accordance with the Staff Regulations.
14. The assurance on which a PSC is based, provided it remains valid, shall cover any assignment by the individual concerned within the EEAS, the General Secretariat of the Council or the Commission.
15. The EEAS shall accept the authorisation for access to EUCI granted by any other European Union institution, body or agency provided it remains valid. Authorisations shall cover any assignment by the individual concerned within the EEAS. The European Union institution, body or agency in which the individual is taking up employment will notify the relevant NSA of the change of employer.
16. If an individual's period of service does not commence within 12 months of the notification of the outcome of the security investigation to the EEAS Security Authority, or if there is a break of 12 months or more in an individual's service, during which time he has not been employed in the EEAS, in other EU Institutions, agencies or bodies, or in a position with a national administration of a Member State, which requires access to classified information, this outcome shall be referred to the relevant NSA for confirmation that it remains valid and appropriate.
17. Where information becomes known to the EEAS concerning a security risk posed by an individual who holds a valid PSC, the EEAS, acting in accordance with the relevant rules and regulations, shall notify the relevant NSA thereof and may suspend access to EUCI or withdraw authorisation for access to EUCI. Where an NSA notifies the EEAS of withdrawal of an assurance given in accordance with paragraph 12(a) for an individual who holds a valid Authorisation to access EUCI, the EEAS Security Authority may ask for any clarification the NSA can provide according to its national laws and regulations. If the adverse information is confirmed, the aforementioned Authorisation shall be withdrawn and the individual shall be excluded from access to EUCI and from positions where such access is possible or where he might endanger security.

18. Any decision to withdraw an Authorisation to access EUCI from an EEAS staff member and, where appropriate, the reasons for doing so shall be notified to the individual concerned, who may ask to be heard by the EEAS Security Authority. Information provided by an NSA shall be subject to the relevant laws and regulations in force in the Member State concerned, including those concerning appeals. Decisions by the EEAS Security Authority shall be subject to appeals in accordance with the Staff Regulations.
19. National experts seconded to the EEAS for a position requiring access to classified information CONFIDENTIEL UE/EU CONFIDENTIAL or above shall present a valid PSC for access to EUCI to the relevant level to the EEAS Security Authority prior to taking up their assignment. The above process shall be managed by the sending Member State.

Records of PSCs

20. A database on the security clearance status of all staff placed under the responsibility of the EEAS and of EEAS contractors' personnel shall be maintained by the EEAS. These records shall include the level of EUCI to which the individual may be granted access (CONFIDENTIEL UE/EU CONFIDENTIAL or above), the date the PSC was granted and its period of validity.
21. Appropriate coordination procedures shall be put in place with Member States and other EU Institutions, agencies and bodies to ensure that the EEAS holds an accurate and comprehensive record of security clearance status of all Staff placed under the responsibility of the EEAS and of EEAS contractors' personnel.
22. The EEAS Security Authority may issue a Personnel Security Clearance Certificate (PSCC) showing the level of EUCI to which the individual may be granted access (CONFIDENTIEL UE/EU CONFIDENTIAL or above), the date of validity of the relevant PSC or Authorisation and the date of expiry of the certificate itself.

Exemptions from the PSC requirement

23. Individuals duly authorised to access EUCI by virtue of their functions in accordance with national laws and regulations shall be briefed, as appropriate, by the EEAS Directorate responsible for security on their security obligations in respect of protecting EUCI.

III. SECURITY EDUCATION AND AWARENESS

24. Prior to being authorised to access EUCI, all individuals shall acknowledge in writing that they have understood their obligations in respect of protecting EUCI and the consequences if EUCI is compromised. A record of such a written acknowledgement shall be kept by the EEAS.
25. All individuals who are authorised to have access to, or required to handle EUCI, shall initially be made aware of, and periodically briefed on the threats to security and must report immediately to the appropriate security authorities any approach or activity that they consider suspicious or unusual.
26. All individuals granted access to EUCI must be subject to ongoing personnel security measures (i.e. aftercare) for the duration that they handle EUCI. Ongoing personnel security is the responsibility of:
    (a) Individuals granted access to EUCI: Individuals are personally responsible for their own security conduct and must report immediately to the appropriate security authorities any approach or activity that they consider suspicious or unusual, and any changes in their personal circumstances that may have an impact on their PSC or Authorisation to access EUCI.
    (b) Line managers: They are responsible for ensuring that their staff are aware of the security measures and responsibilities to protect EUCI, for monitoring the security conduct of their staff and for either addressing any security matters of concern themselves, or reporting to the appropriate security authorities any adverse information that may have an impact on their staff's PSC or Authorisation to access EUCI.

(c) Security actors of the EEAS security organisation as referred to in Article 12 of this decision: They are responsible for providing security awareness briefings to ensure staff in their area are periodically briefed, for fostering a strong security culture in their area of responsibility, for putting in place measures to monitor the security conduct of staff, and for reporting to the appropriate security authorities any adverse information that may have an impact on any individual's PSC.

(d) EEAS and Member States: shall put in place the necessary channels to communicate information that may have an impact on any individual's PSC or Authorisation to access EUCI.

27. All individuals who cease to be employed on duties requiring access to EUCI shall be made aware of, and where appropriate acknowledge in writing, their obligations in respect of the continued protection of EUCI.

IV. EXCEPTIONAL CIRCUMSTANCES

28. For reasons of urgency, where duly justified in the interests of the EEAS and pending completion of a full security investigation, the EEAS Security Authority may, after consulting the NSA of the Member State of which the individual is a national and subject to the outcome of preliminary checks to verify that no adverse information is known, grant a temporary authorisation for EEAS officials and other servants to access EUCI for a specific function. A full security investigation should be completed as soon as possible. Such temporary authorisations will be valid for a period not exceeding six months and shall not permit access to information classified TRES SECRET UE/EU TOP SECRET. All individuals who have been granted a temporary authorisation shall acknowledge in writing that they have understood their obligations in respect of protecting EUCI and the consequences if EUCI is compromised. A record of such a written acknowledgement shall be kept by the EEAS.

29. When an individual is to be assigned to a position that requires a PSC at one level higher than that currently possessed by the individual, the assignment may be made on a provisional basis, provided that:
    (a) the compelling need for access to EUCI at a higher level shall be justified, in writing, by the individual's superior;
    (b) access shall be limited to specific items of EUCI in support of the assignment;
    (c) the individual holds a valid PSC;
    (d) action has been initiated to obtain authorisation for the level of access required for the position;
    (e) satisfactory checks have been made by the competent authority that the individual has not seriously or repeatedly infringed security regulations;
    (f) the assignment of the individual is approved by the competent EEAS authority;
    (g) the relevant NSA/DSA which issued the individual's PSC has been consulted and no objection has been received; and
    (h) a record of the exception, including a description of the information to which access was approved, is kept by the registry or subordinate registry responsible.
30. The above procedure shall be used for one-time access to EUCI at one level higher than that to which the individual has been security cleared. Recourse to this procedure shall not be made on a recurring basis.
31. In very exceptional circumstances, such as missions in hostile environments or during periods of mounting international tension when emergency measures require it, in particular for the purposes of saving lives, the HR, the EEAS Security Authority or the DGBA may grant, where possible in writing, access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET to individuals who do not possess the requisite PSC, provided that such permission is absolutely necessary. A record shall be kept of this permission describing the information to which access was approved.

32. In the case of information classified TRES SECRET UE/EU TOP SECRET, this emergency access shall be confined to EU nationals who have been authorised access to either the national equivalent of TRES SECRET UE/EU TOP SECRET or information classified SECRET UE/EU SECRET.
33. The EEAS Security Committee shall be informed of cases when recourse is made to the procedure set out in paragraphs 31 and 32.
34. The EEAS Security Committee shall receive an annual report on recourse to the procedures set out in this section.

V. ATTENDANCE AT MEETINGS IN THE EEAS HEADQUARTERS AND UNION DELEGATIONS

35. Individuals assigned to participate in meetings in the EEAS Headquarters and Union Delegations at which information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above is discussed may only do so upon confirmation of the individual's PSC status. For Member States' representatives, officials from the GSC and Commission, a PSCC or other proof of PSC shall be forwarded by the appropriate authorities to the EEAS Directorate responsible for security, the Union Delegation Security Coordinator, or exceptionally be presented by the person concerned. Where applicable, a consolidated list of names may be used, giving the relevant proof of PSC.
36. Where a PSC for access to EUCI is withdrawn from an individual whose duties require attendance at meetings in the EEAS Headquarters or Union Delegation at which information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above is discussed, the EEAS shall be informed by the competent authority thereof.

VI. POTENTIAL ACCESS TO EUCI

37. When individuals are to be employed in circumstances in which they may potentially have access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above, they shall be appropriately security cleared or escorted at all times.

38. Couriers, guards and escorts shall be security cleared to the relevant level or otherwise appropriately investigated in accordance with national laws and regulations, be briefed at regular intervals on security procedures for protecting EUCI and on their duties for protecting such information entrusted to them or to which they may inadvertently have access.

ANNEX A II

PHYSICAL SECURITY OF EU CLASSIFIED INFORMATION

I. INTRODUCTION

1. This Annex sets out provisions for implementing Article 6 of Annex A. It lays down minimum requirements for the physical protection of premises, buildings, offices, rooms and other areas where EUCI is handled and stored, including areas housing CIS.
2. Physical security measures shall be designed to prevent unauthorised access to EUCI by:
   (a) ensuring that EUCI is handled and stored in an appropriate manner;
   (b) allowing for segregation of personnel in terms of access to EUCI on the basis of their need-to-know and, where appropriate, their security clearance;
   (c) deterring, impeding and detecting unauthorised actions; and
   (d) denying or delaying surreptitious or forced entry by intruders.

II. PHYSICAL SECURITY REQUIREMENTS AND MEASURES

3. The EEAS shall apply a risk management process for protecting EUCI on their premises to ensure that a commensurate level of physical protection is afforded against the assessed risk. The risk management process shall take account of all relevant factors, in particular:
   (a) the classification level of EUCI;
   (b) the form and volume of EUCI, bearing in mind that large quantities or a compilation of EUCI may require more stringent protective measures to be applied;
   (c) the surrounding environment and structure of the buildings or areas housing EUCI;
   (d) the third country threat assessment as developed by INTCEN on the basis in particular of Union Delegation reports, and
   (e) the assessed threat from intelligence services which target the EU or Member States and from sabotage, terrorist, subversive or other criminal activities.
4. The EEAS Security Authority, applying the concept of defence in depth, shall determine the appropriate combination of physical security measures to be implemented. These can include one or more of the following:
   (a) a perimeter barrier: a physical barrier which defends the boundary of an area requiring protection;
   (b) intrusion detection systems (IDS): an IDS may be used to enhance the level of security offered by a perimeter barrier, or in rooms and buildings in place of, or to assist, security staff;
   (c) access control: access control may be exercised over a site, a building or buildings on a site or to areas or rooms within a building. Control may be exercised by electronic or electro-mechanical means, by security personnel and/or a receptionist, or by any other physical means;
   (d) security personnel: trained, supervised and, where necessary, appropriately security cleared security personnel may be employed, *inter alia*, in order to deter individuals planning covert intrusion;

(e) closed circuit television (CCTV): CCTV may be used by security personnel in order to verify incidents and IDS alarms on large sites or at perimeters;

(f) security lighting: security lighting may be used to deter a potential intruder, as well as to provide the illumination necessary for effective surveillance directly by security personnel or indirectly through a CCTV system; and

(g) any other appropriate physical measures designed to deter or detect unauthorised access or prevent loss of or damage to EUCI.

5. The EEAS Directorate responsible for security may conduct entry and exit searches to act as a deterrent to the unauthorised introduction of material or the unauthorised removal of EUCI from premises or buildings.
6. When EUCI is at risk from overlooking, even accidentally, appropriate measures shall be taken to counter this risk.
7. For new facilities, physical security requirements and their functional specifications shall be defined as part of the planning and design of the facilities. For existing facilities, physical security requirements shall be implemented to the maximum extent possible.

III. EQUIPMENT FOR THE PHYSICAL PROTECTION OF EUCI

8. When acquiring equipment (such as security containers, shredding machines, door locks, electronic access control systems, IDS, alarm systems) for the physical protection of EUCI, the EEAS security authority shall ensure that the equipment meets approved technical standards and minimum requirements.
9. The technical specifications of equipment to be used for the physical protection of EUCI shall be set out in security guidelines to be approved by the EEAS Security Committee.
10. Security systems shall be inspected at regular intervals and equipment shall be maintained regularly. Maintenance work shall take account of the outcome of inspections to ensure that equipment continues to operate at optimum performance.
11. The effectiveness of individual security measures and of the overall security system shall be re-evaluated during each inspection.

IV. PHYSICALLY PROTECTED AREAS

12. Two types of physically protected areas, or the national equivalents thereof, shall be established for the physical protection of EUCI:
    (a) Administrative Areas and
    (b) Secured Areas (including technically Secured Areas).
13. The EEAS Security Authority shall establish that an area meets the requirements to be designated as an Administrative Area, a Secured Area or a technically Secured Area.
14. For Administrative Areas:
    (a) a visibly defined perimeter shall be established which allows individuals and, where possible, vehicles to be checked;
    (b) unescorted access shall be granted only to individuals who are duly authorised by the EEAS Directorate responsible for Security; and
    (c) all other individuals shall be escorted at all times or be subject to equivalent controls.
15. For Secured Areas:
    (a) a visibly defined and protected perimeter shall be established through which all entry and exit are controlled by means of a pass or personal recognition system;
    (b) unescorted access shall be granted only to individuals who are security-cleared to the appropriate level and specifically authorised to enter the area on the basis of their need-to-know;
    (c) all other individuals shall be escorted at all times or be subject to equivalent controls.
16. Where entry into a Secured Area constitutes, for all practical purposes, direct access to the classified information contained in it, the following additional requirements shall apply:
    (a) the level of highest security classification of the information normally held in the area shall be clearly indicated;
    (b) all visitors shall require specific authorisation to enter the area, shall be escorted at all times and shall be appropriately security cleared unless steps are taken to ensure that no access to EUCI is possible;
    (c) electronic devices shall be left outside the area.

17. Secured Areas protected against eavesdropping shall be designated technically Secured Areas. The following additional requirements shall apply:
    (a) such areas shall be IDS equipped, be locked when not occupied and be guarded when occupied. Any keys shall be controlled in accordance with Section VI of this Annex;
    (b) all persons and material entering such areas shall be controlled;
    (c) such areas shall be regularly physically and/or technically inspected as required by the EEAS Security Authority. Such inspections shall also be conducted following any unauthorised entry or suspicion of such an entry; and
    (d) such areas shall be free of unauthorised communication lines, unauthorised telephones or other unauthorised communication devices and electrical or electronic equipment;
18. Notwithstanding point (d) of paragraph 17, before being used in areas where meetings are held or work is being performed involving information classified SECRET UE/EU SECRET and above, and where the threat to EUCI is assessed as high, any communications devices and electrical or electronic equipment shall first be examined by the EEAS Security Authority to ensure that no intelligible information can be inadvertently or illicitly transmitted by such equipment beyond the perimeter of the Secured Area.
19. Secured Areas which are not occupied by duty personnel on a 24-hour basis shall, where appropriate, be inspected at the end of normal working hours and at random intervals outside normal working hours, unless an IDS is in place.
20. Secured Areas and technically Secured Areas may be set up temporarily within an Administrative Area for a classified meeting or any other similar purpose.
21. Security operating procedures shall be drawn up for each Secured Area stipulating:
    (a) the level of EUCI which may be handled and stored in the area;
    (b) the surveillance and protective measures to be maintained;
    (c) the individuals authorised to have unescorted access to the area by virtue of their need-to-know and security clearance;
    (d) where appropriate, the procedures for escorts or for protecting EUCI when authorising any other individuals to access the area;
    (e) any other relevant measures and procedures.

22. Strong rooms shall be constructed within Secured Areas. The walls, floors, ceilings, windows and lockable doors shall be approved by the EEAS Security Authority and afford protection equivalent to a security container approved for the storage of EUCI of the same classification level.

V. PHYSICAL PROTECTIVE MEASURES FOR HANDLING AND STORING EUCI

23. EUCI which is classified RESTREINT UE/EU RESTRICTED may be handled:
    (a) in a Secured Area,
    (b) in an Administrative Area provided the EUCI is protected from access by unauthorised individuals, or
    (c) outside a Secured Area or an Administrative Area provided the holder carries the EUCI in accordance with paragraphs 30 to 42 of Annex A III and has undertaken to comply with compensatory measures laid down in security instructions issued by the EEAS Security Authority to ensure that EUCI is protected from access by unauthorised persons.
24. EUCI which is classified RESTREINT UE/EU RESTRICTED shall be stored in suitable locked office furniture in an Administrative Area or a Secured Area. It may temporarily be stored outside a Secured Area or an Administrative Area provided the holder has undertaken to comply with compensatory measures laid down in security instructions issued by the EEAS Security Authority.

25. EUCI which is classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET may be handled:
    (a) in a Secured Area;
    (b) in an Administrative Area provided the EUCI is protected from access by unauthorised individuals; or
    (c) outside a Secured Area or an Administrative Area provided the holder:
        (i) carries the EUCI in accordance with paragraphs 30 to 42 of Annex A III;
        (ii) has undertaken to comply with compensatory measures laid down in security instructions issued by the EEAS Security Authority to ensure that EUCI is protected from access by unauthorised persons;
        (iii) keeps the EUCI at all times under his personal control; and
        (iv) in the case of documents in paper form, has notified the relevant registry of the fact.

26. EUCI which is classified CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET shall be stored within a Secured Area, in a security container or strong room.
27. EUCI which is classified TRES SECRET UE/EU TOP SECRET shall be handled in a Secured Area.
28. EUCI which is classified TRES SECRET UE/EU TOP SECRET shall be stored in a Secured Area at the Headquarters under one of the following conditions:
    (a) in a security container that is in accordance with paragraph 8 with one or more of the following supplementary controls:
        (i) continuous protection or verification by cleared security staff or duty personnel;
        (ii) an approved IDS in combination with security response personnel;

    or
    (b) in an IDS-equipped strong room in combination with security response personnel.
29. Rules governing the carriage of EUCI outside physically protected areas are set out in Annex A III.

VI. CONTROL OF KEYS AND COMBINATIONS USED FOR PROTECTING EUCI

30. The EEAS Security Authority shall define procedures for managing keys and combination settings for offices, rooms, strong rooms and security containers. Such procedures shall protect against unauthorised access.
31. Combination settings shall be committed to memory by the smallest possible number of individuals needing to know them. Combination settings for security containers and strong rooms storing EUCI shall be changed:
    (a) on receipt of a new container;
    (b) whenever there is a change in personnel knowing the combination;
    (c) whenever a compromise has occurred or is suspected;
    (d) when a lock has undergone maintenance or repair; and
    (e) at least every 12 months.

ANNEX A III

MANAGEMENT OF CLASSIFIED INFORMATION

I. INTRODUCTION

1. This Annex sets out provisions for implementing Article 7 of Annex A. It lays down the administrative measures for controlling EUCI throughout its life-cycle in order to help deter, detect and recover from deliberate or accidental compromise or loss of such information.

II. CLASSIFICATION MANAGEMENT

Classifications and markings

2. Information shall be classified where it requires protection with regard to its confidentiality.

3. The originator of EUCI shall be responsible for determining the security classification level, in accordance with the relevant classification guidelines, and for the dissemination of the information.
4. The classification level of EUCI shall be determined in accordance with Article 2(2) of Annex A and by reference to the security Guidelines to be approved in accordance with Article 3(3) of Annex A.
5. Classified information of the Member States exchanged with the EEAS shall be afforded the same level of protection as EUCI bearing the equivalent classification. A table of equivalence can be found in Appendix B to this decision.
6. The security classification and, where applicable, the date or specific event after which it may be downgraded or declassified, shall be clearly and correctly indicated, regardless of whether the EUCI is in paper, oral, electronic or any other form.
7. Individual parts of a given document (i.e. pages, paragraphs, sections, annexes, appendices, attachments and enclosures) may require different classifications and shall be marked accordingly, including when stored in electronic form.
8. To the extent possible, documents containing parts with different classification levels shall be structured so that parts with a different classification level may be easily identified and detached if necessary.
9. The overall classification level of a document or file shall be at least as high as that of its most highly classified component. When information from various sources is collated, the final product shall be reviewed to determine its overall security classification level, since it may warrant a higher classification than its component parts.
10. The classification of a letter or note covering enclosures shall be as high as the highest classification of its enclosures. The originator shall indicate clearly at which level it is classified when detached from its enclosures by means of an appropriate marking, e.g.:

    CONFIDENTIEL UE/EU CONFIDENTIAL

    Without attachment(s) RESTREINT UE/EU RESTRICTED

Markings

11. In addition to one of the security classification markings set out in Article 2(2) of Annex A, EUCI may bear additional markings, such as:
    (a) an identifier to designate the originator;
    (b) any caveats, code words or acronyms specifying the field of activity to which the document relates, a particular distribution on a need-to-know basis or restrictions on use;
    (c) releasability markings.
12. Following a decision to release EUCI to a third State or International Organisation, the EEAS Directorate responsible for Security shall forward the classified information concerned, which shall bear a releasability marking indicating the third State or international organisation to which it is to be released.
13. A list of authorised markings will be adopted by the EEAS Security Authority.

Abbreviated classification markings

14. Standardised abbreviated classification markings may be used to indicate the classification level of individual paragraphs of a text. Abbreviations shall not replace the full classification markings.
15. The following standard abbreviations may be used within EU classified documents to indicate the classification level of sections or blocks of text of less than a single page:

TRES SECRET UE/EU TOP SECRET	TS-UE/EU-TS
SECRET UE/EU SECRET	S-UE/EU-S
CONFIDENTIEL UE/EU CONFIDENTIAL	C-UE/EU-C
RESTREINT UE/EU RESTRICTED	R-UE/EU-R

Creation of EUCI

16. When creating an EU classified document:
    (a) each page shall be marked clearly with the classification level;
    (b) each page shall be numbered;
    (c) the document shall bear a reference number and a subject, which is not itself classified information, unless it is marked as such;
    (d) the document shall be dated;
    (e) documents classified CONFIDENTIEL UE/EU CONFIDENTIAL or above shall bear a copy number on every page, if they are to be distributed in several copies.
17. Where it is not possible to apply paragraph 16 to EUCI, other appropriate measures shall be taken in accordance with security guidelines to be established pursuant to this Decision.

Downgrading and declassification of EUCI

18. At the time of its creation, the originator shall indicate, where possible, and in particular for information classified RESTREINT UE/EU RESTRICTED, whether EUCI can be downgraded or declassified on a given date or following a specific event.
19. The EEAS shall regularly review EUCI held by it to ascertain whether the classification level still applies. The EEAS shall establish a system to review the classification level of registered EUCI that it has originated no less frequently than every five years. Such a review shall not be necessary where the originator has indicated from the outset a specific time when the information will automatically be downgraded or declassified and the information has been marked accordingly.

III. REGISTRATION OF EUCI FOR SECURITY PURPOSES

20. A central registry shall be established in Headquarters. For every organisational entity within the EEAS in which EUCI is handled, a responsible registry shall be established, subordinated to the central registry, to ensure that EUCI is handled in accordance with this Decision. Registries shall be established as Secured Areas as defined in Annex A.
    Each Union Delegation establishes its own EUCI registry.
    The EEAS Security Authority shall designate a Chief Registry Officer for these registries.
21. For the purposes of this Decision, registration for security purposes (hereinafter referred to as 'registration') means the application of procedures that record the life-cycle of information, including its dissemination and destruction. In the case of a CIS, registration procedures may be performed by processes within the CIS itself.
22. All material classified CONFIDENTIEL UE/EU CONFIDENTIAL and above shall be registered when it arrives at or leaves an organisational entity including Union Delegations. Information classified TRES SECRET UE/EU TOP SECRET shall be registered in designated registries.
23. The Central Registry shall be, in EEAS Headquarters, the main point of entry and exit for classified information exchanges with third States and international organisations. It shall keep a record of all these exchanges.
24. The EEAS Security Authority shall approve security Guidelines on the registration of EUCI for security purposes, in accordance with article 14 of this Decision.

TRES SECRET UE/EU TOP SECRET registries

25. The Central Registry shall be designated in the EEAS Headquarters to act as the central receiving and dispatching authority for information classified TRES SECRET UE/EU TOP SECRET. Where necessary, subordinate registries may be designated to handle such information for registration purposes.

26. Such subordinate registries may not transmit TRES SECRET UE/EU TOP SECRET documents directly to other subordinate registries of the same central TRES SECRET UE/EU TOP SECRET registry or externally without the express written approval of the latter.

IV. COPYING AND TRANSLATING EU CLASSIFIED DOCUMENTS

27. TRES SECRET UE/EU TOP SECRET documents shall not be copied or translated without the prior written consent of the originator.
28. Where the originator of documents classified SECRET UE/EU SECRET and below has not imposed caveats on their copying or translation, such documents may be copied or translated on instruction from the holder.
29. The security measures applicable to the original document shall apply to copies and translations thereof. The copies of CONFIDENTIEL UE/EU CONFIDENTIAL or above shall be created only by a relevant (sub) registry with a secured copy-machine. The copies must be registered.

V. CARRIAGE OF EUCI

30. Carriage of EUCI shall be subject to the protective measures set out in paragraphs 32 to 42. When EUCI is carried on electronic media, and notwithstanding Article 7(4) of Annex A, the protective measures set out below may be supplemented by appropriate technical countermeasures prescribed by the EEAS Security Authority so as to minimise the risk of loss or compromise.
31. The EEAS Security Authority shall issue instructions on the carriage of EUCI in accordance with this Decision.

Within a building or self-contained group of buildings

32. EUCI carried within a building or self-contained group of buildings shall be covered in order to prevent observation of its contents.

33. Within a building or self-contained group of buildings, information classified TRES SECRET UE/EU TOP SECRET shall be carried by appropriately security cleared individuals, in a secured envelope bearing only the addressee's name.

Within the EU

34. EUCI carried between buildings or premises within the EU shall be packaged so that it is protected from unauthorised disclosure.
35. The carriage of information classified up to SECRET UE/EU SECRET within the EU shall be by one of the following means:
    (a) military, government or diplomatic courier, as appropriate;
    (b) hand carriage, provided that:
        (i) EUCI does not leave the possession of the bearer, unless it is stored in accordance with the requirements set out in Annex A II;
        (ii) EUCI is not opened *en route* or read in public places;
        (iii) individuals are security cleared to the appropriate level and briefed on their security responsibilities;
        (iv) individuals are provided with a courier certificate where necessary;
    (c) postal services or commercial courier services, provided that:
        (i) they are approved by the relevant NSA in accordance with national laws and regulations;
        (ii) they apply appropriate protective measures in accordance with minimum requirements to be laid down in security guidelines pursuant to Article 21(1) of this Decision.

    In the case of carriage from one Member State to another, the provisions of point (c) shall be limited to information classified up to CONFIDENTIEL UE/EU CONFIDENTIAL.
36. Material classified CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET (e.g. equipment or machinery) which cannot be carried by the means referred to in paragraph 34 shall be transported as freight by commercial carrier companies in accordance with Annex A V.

37. The carriage of information classified TRES SECRET UE/EU TOP SECRET between buildings or premises within the EU shall be by military, government or diplomatic courier, as appropriate.

From within the EU to the territory of a third State, or between EU entities in third States

38. EUCI carried from within the EU to the territory of a third State, or between EU entities in third States, shall be packaged in such a way that it is protected from unauthorised disclosure.

39. The carriage of information classified CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET from within the EU to the territory of a third State, and the carriage of any EUCI classified up to SECRET UE/EU SECRET between EU entities in third States, shall be by one of the following means:
    (a) military or diplomatic courier;
    (b) hand carriage, provided that:
        (i) the package bears an official seal, or is packaged so as to indicate that it is an official consignment and should not undergo customs or security scrutiny;
        (ii) individuals carry a courier certificate identifying the package and authorising them to carry the package;
        (iii) EUCI does not leave the possession of the bearer, unless it is stored in accordance with the requirements set out in Annex A II;
        (iv) EUCI is not opened *en route* or read in public places; and
        (v) individuals are security cleared to the appropriate level and briefed on their security responsibilities.

40. The carriage of information classified CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET released by the EU to a third State or international organisation shall comply with the relevant provisions under a security of information Agreement or an administrative arrangement in accordance with Article 10(2) of Annex A.

41. Information classified RESTREINT UE/EU RESTRICTED may also be carried from within the EU to the territory of a third State by postal services or commercial courier services.

42. The carriage of information classified TRES SECRET UE/EU TOP SECRET from within the EU to the territory of a third State, or between EU entities in third States, shall be by military or diplomatic courier.

VI. DESTRUCTION OF EUCI

43. EU classified documents that are no longer required may be destroyed, without prejudice to the relevant rules and regulations on archiving.

44. Documents subject to registration in accordance with Article 7(2) of Annex A shall be destroyed by the responsible registry on instruction from the holder or from a competent authority. The logbooks and other registration information shall be updated accordingly.

45. For documents classified SECRET UE/EU SECRET or TRES SECRET UE/EU TOP SECRET, destruction shall be performed in the presence of a witness who shall be cleared to at least the classification level of the document being destroyed.

46. The registrar and the witness, where the presence of the latter is required shall sign a destruction certificate, which shall be filed in the registry. The registry shall keep destruction certificates of TRES SECRET UE/EU TOP SECRET documents for a period of at least ten years and of documents CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET for a period of at least five years.

47. Classified documents, including those classified RESTREINT UE/EU RESTRICTED, shall be destroyed by methods which meet relevant EU or equivalent standards or which have been approved by Member States in accordance with national technical standards so as to prevent reconstruction in whole or in part.

48. The destruction of computer storage media used for EUCI shall be in accordance with procedures approved by the EEAS Security Authority.

VII. SECURITY INSPECTIONS

EEAS security inspections

49. In accordance with Article 16 of this Decision, the EEAS security inspections encompass:
    (a) general security inspections, whose aim shall be to assess the general security level of the EEAS Headquarters, Union Delegations and all dependent or related premises, especially in order to evaluate effectiveness of security measures implemented for protecting the EEAS security interests;
    (b) EUCI security inspections, whose aim shall be to evaluate, generally in view of an accreditation, the effectiveness of measures implemented for protecting EUCI in EEAS Headquarters and Union Delegations.
    In particular, such inspections shall be carried out, inter alia to:
        (i) ensure that the required minimum standards for protecting EUCI laid down in this Decision are respected;
        (ii) emphasise the importance of security and effective risk management within the entities inspected;
        (iii) recommend countermeasures to mitigate the specific impact of loss of confidentiality, integrity or availability of classified information; and
        (iv) reinforce security authorities' ongoing security education and awareness programmes.

Conduct of and reporting on EEAS security inspections

50. EEAS Security inspections shall be conducted by an inspection team of the EEAS Directorate responsible for Security and, when necessary, with the support of security experts of other EU Institutions or Member States.

    The inspection team shall have access to any location where EUCI is handled, in particular registries and CIS points of presence.

51. EEAS Security inspections in Union Delegations can be conducted, whenever necessary, with the support of the Security Officers of the Member States' embassies located in the third countries.

52. Before the end of each calendar year, the EEAS security authority shall adopt a security inspection programme for the EEAS for the following year.

53. Whenever necessary, security inspections that are not foreseen in the programme above can be arranged by the EEAS Security Authority.

54. At the end of the security inspection, the main conclusions and recommendations shall be presented to the inspected entity. Thereafter, a report on the inspection shall be drawn up by the inspection team. Where corrective actions and recommendations have been proposed, sufficient details shall be included in the report to support the conclusions reached. The report shall be forwarded to the EEAS Security Authority and to the head of the inspected entity.

    A regular report shall be prepared under the responsibility of the EEAS Directorate responsible for Security to highlight the lessons learned from the inspections conducted over a specified period and examined by the EEAS Security Committee.

Conduct of and reporting on security inspections in EU agencies and bodies established under Title V, Chapter 2 of the TEU

55. The EEAS Directorate responsible for security may, where appropriate, designate contributing experts to participate in joint EU inspection teams carrying out inspections in EU agencies and bodies established under Title V, Chapter 2 of the TEU.

EEAS security inspections checklist

56. The EEAS Directorate responsible for security shall draw up and update a security inspection checklist of items to be verified in the course of a EEAS security inspection. This checklist shall be forwarded to the EEAS Security Committee.

57. The information to complete the checklist shall be obtained in particular during the inspection from the security management of the entity being inspected. Once completed with the detailed responses, the checklist shall be classified by agreement with the inspected entity. It shall not form part of the inspection report.

ANNEX A IV

PROTECTION OF EUCI HANDLED IN CIS

I. INTRODUCTION

1. This Annex sets out provisions for implementing Article 8 of Annex A.
2. The following Information Assurance (IA) properties and concepts are essential for the security and correct functioning of operations on Communication and Information Systems (CIS):

Authenticity:	the guarantee that information is genuine and from *bona fide* sources;
Availability:	the property of being accessible and usable upon request by an authorised entity;
Confidentiality:	the property that information is not disclosed to unauthorised individuals, entities or processes;
Integrity:	the property of safeguarding the accuracy and completeness of information and assets;
Non-repudiation:	the ability to prove an action or event has taken place, so that this event or action cannot subsequently be denied.

II. INFORMATION ASSURANCE PRINCIPLES

3. The provisions set out below shall form the baseline for the security of any CIS handling EUCI. Detailed requirements for implementing these provisions shall be defined in IA security Guidelines.

Security risk management

4. Security risk management shall be an integral part of defining, developing, operating and maintaining CIS. Risk management (assessment, treatment, acceptance and communication) shall be conducted as an iterative process jointly by representatives of the system owners, project authorities, operating authorities and security approval authorities, using a proven, transparent and fully understandable risk assessment process. The scope of the CIS and its assets shall be clearly defined at the outset of the risk management process.

5. The EEAS competent authorities shall review the potential threats to CIS and shall maintain up-to-date and accurate threat assessments which reflect the current operational environment. They shall constantly update their knowledge of vulnerability issues and periodically review the vulnerability assessment to keep up with the changing information technology (IT) environment.

6. The aim of security risk management shall be to apply a set of security measures which results in a satisfactory balance between user requirements and residual security risk.

7. The specific requirements, scale and the degree of detail determined by the relevant Security Accreditation Authority (SAA) for accrediting a CIS shall be commensurate with the assessed risk, taking account of all relevant factors, including the classification level of the EUCI handled in the CIS. Accreditation shall include a formal residual risk statement and acceptance of the residual risk by a responsible authority.

Security throughout the CIS-life cycle

8. Ensuring security shall be a requirement throughout the entire CIS life-cycle from initiation to withdrawal from service.
9. The role and interaction of each actor involved in a CIS with regard to its security shall be identified for each phase of the life-cycle.
10. Any CIS, including its technical and non-technical security measures, shall be subject to security testing during the accreditation process to ensure that the appropriate level of assurance of the implemented security measures is obtained and to verify that they are correctly implemented, integrated and configured.

11. Security assessments, inspections and reviews shall be performed periodically during the operation and maintenance of a CIS and when exceptional circumstances arise.

12. Security documentation for a CIS shall evolve over its life-cycle as an integral part of the process of change and configuration management.

Best practice

13. The EEAS shall cooperate with GSC, Commission and Member States to develop best practice for protecting EUCI handled on CIS. Best practice guidelines shall set out technical, physical, organisational and procedural security measures for CIS with proven effectiveness in countering given threats and vulnerabilities.

14. The protection of EUCI handled on CIS shall draw on lessons learned by entities involved in IA within and outside the EU.

15. The dissemination and subsequent implementation of best practice shall help achieve an equivalent level of assurance for the various CIS operated by the EEAS which handle EUCI.

Defence in depth

16. To mitigate risk to CIS, a range of technical and non-technical security measures, organised as multiple layers of defence, shall be implemented. These layers shall include:

    (a) ***Deterrence***: security measures aimed at dissuading any adversary planning to attack the CIS;

    (b) ***Prevention***: security measures aimed at impeding or blocking an attack on the CIS;

    (c) ***Detection***: security measures aimed at discovering the occurrence of an attack on the CIS;

    (d) ***Resilience***: security measures aimed at limiting impact of an attack to a minimum set of information or CIS assets and preventing further damage; and

    (e) ***Recovery***: security measures aimed at regaining a secure situation for the CIS.

    The degree of stringency and applicability of such security measures shall be determined following a risk assessment.

17. The EEAS competent authorities shall ensure that they can respond to incidents which may transcend organisational and national boundaries to coordinate responses and share information about these incidents and the related risk (computer emergency response capabilities).

Principle of minimality and least privilege

18. Only the functionalities, devices and services to meet operational requirements shall be implemented in order to avoid unnecessary risk.
19. CIS users and automated processes shall be given only the access, privileges or authorisations they require to perform their tasks in order to limit any damage resulting from accidents, errors, or unauthorised use of CIS resources.
20. Registration procedures performed by a CIS, where required, shall be verified as part of the accreditation process.

Information Assurance awareness

21. Awareness of the risks and available security measures is the first line of defence for the security of CIS. In particular all personnel involved in the life-cycle of CIS, including users, shall understand:
    (a) that security failures may significantly harm the CIS and the whole organisation;
    (b) the potential harm to others which may arise from interconnectivity and interdependency; and
    (c) their individual responsibility and accountability for the security of CIS according to their roles within the systems and processes.
22. To ensure that security responsibilities are understood, IA education and awareness training shall be mandatory for all personnel involved, including senior management and CIS users.

Evaluation and approval of IT-security products

23. The required degree of confidence in the security measures, defined as a level of assurance, shall be determined following the outcome of the risk management process and in line with the relevant security policies and security guidelines.

24. The level of assurance shall be verified by using internationally recognised or nationally approved processes and methodologies. This includes primarily evaluation, controls and auditing.

25. Cryptographic products for protecting EUCI shall be evaluated and approved by a national Crypto Approval Authority (CAA) of a Member State.

26. Prior to being recommended for approval by the EEAS CAA in accordance with Article 8(5) of this Decision, such cryptographic products shall have undergone a successful second party evaluation by an Appropriately Qualified Authority (AQUA) of a Member State not involved in the design or manufacture of the equipment. The degree of detail required in a second party evaluation shall depend on the envisaged maximum classification level of EUCI to be protected by these products.

27. Where warranted on specific operational grounds, the EEAS CAA may, upon recommendation by the Council Security Committee, waive the requirements under paragraphs 25 or 26 and grant an interim approval for a specific period in accordance with Article 8(5) of this Decision.

28. An AQUA shall be a CAA of a Member State that has been accredited on the basis of criteria laid down by the Council to undertake the second evaluation of cryptographic products for protecting EUCI.

29. The High Representative shall approve a security policy on the qualifications and approval of non-cryptographic IT security products.

Transmission within Secured Areas

30. Notwithstanding the provisions of this Decision, when transmission of EUCI is confined within Secured Areas or Administrative Areas, unencrypted distribution or encryption at a lower level may be used based on the outcome of a risk management process and subject to the approval of the SAA.

Secure interconnection of CIS

31. For the purposes of this Decision, an interconnection shall mean the direct connection of two or more IT systems for the purpose of sharing data and other information resources (e.g. communication) in a unidirectional or multidirectional way.

32. A CIS shall treat any interconnected IT system as untrusted and shall implement protective measures to control the exchange of classified information.

33. For all interconnections of CIS with another IT system the following basic requirements shall be met:
    (a) business or operational requirements for such interconnections shall be stated and approved by the competent authorities;
    (b) the interconnection shall undergo a risk management and accreditation process and shall require the approval of the competent SAAs; and
    (c) Boundary Protection Services (BPS) shall be implemented at the perimeter of all CIS.

34. There shall be no interconnection between an accredited CIS and an unprotected or public network, except where the CIS has approved BPS installed for such a purpose between the CIS and the unprotected or public network. The security measures for such interconnections shall be reviewed by the competent Information Assurance Authority (IAA) and approved by the competent SAA.

    When the unprotected or public network is used solely as a carrier and the data is encrypted by a cryptographic product approved in accordance with Article 8(5) of this Decision, such a connection shall not be deemed to be an interconnection.

35. The direct or cascaded interconnection of a CIS accredited to handle TRES SECRET UE/EU TOP SECRET to an unprotected or public network shall be prohibited.

Computer storage media

36. Computer storage media shall be destroyed in accordance with procedures approved by the EEAS Security Authority.

37. Computer storage media shall be reused, downgraded or declassified in accordance with security Guidelines to be established pursuant to Article 8(2) of this Decision.

Emergency circumstances

38. Notwithstanding the provisions of this Decision, the specific procedures described below may be applied for a limited period of time in an emergency, such as during impending or actual crisis, conflict, war situations or in exceptional operational circumstances.

39. EUCI may be transmitted using cryptographic products which have been approved for a lower classification level or without encryption with the consent of the competent authority if any delay would cause harm clearly outweighing the harm entailed by any disclosure of the classified material and if:
    (a) the sender and recipient do not have the required encryption facility or have no encryption facility; and
    (b) the classified material cannot be conveyed in time by other means.

40. Classified information transmitted under the circumstances set out in paragraph 39 shall not bear any markings or indications distinguishing it from information which is unclassified or which can be protected by an available cryptographic product. Recipients shall be notified of the classification level, without delay, by other means.

41. Should recourse be made to paragraph 39, a subsequent report shall be made to the EEAS Security Directorate and, by it, to the EEAS Security Committee. This report will at least state the sender, the recipient and the originator of each piece of EUCI.

III. INFORMATION ASSURANCE FUNCTIONS AND AUTHORITIES

42. The following IA functions shall be established in the EEAS. These functions do not require single organisational entities. They shall have separate mandates. However, these functions, and their accompanying responsibilities, may be combined or integrated in the same organisational entity or split into different organisational entities, provided that internal conflicts of interests or tasks are avoided.

Information Assurance Authority (IAA)

43. The IAA shall be responsible for:
    (a) developing IA security Guidelines and monitoring their effectiveness and relevance;
    (b) safeguarding and administering technical information related to cryptographic products;
    (c) ensuring that IA measures selected for protecting EUCI comply with the relevant Guidelines governing their eligibility and selection;
    (d) ensuring that cryptographic products are selected in compliance with Guidelines governing their eligibility and selection;
    (e) coordinating training and awareness on IA;
    (f) consulting with the system provider, the security actors and representatives of users in respect of IA security guidelines; and
    (g) ensuring appropriate expertise is available in the expert sub-area of the EEAS Security Committee for IA issues.

TEMPEST Authority

44. The TEMPEST Authority (TA) shall be responsible for ensuring compliance of CIS with TEMPEST policies and guidelines. It shall approve TEMPEST countermeasures for installations and products to protect EUCI to a defined level of classification in its operational environment.

Crypto Approval Authority (CAA)

45. The CAA shall be responsible for ensuring that cryptographic products comply with respective cryptographic Guidelines. It shall approve a cryptographic product to protect EUCI to a defined level of classification in its operational environment.

Crypto Distribution Authority (CDA)

46. The CDA shall be responsible for:
    (a) managing and accounting for EU crypto material;
    (b) ensuring that appropriate procedures are enforced and channels established for accounting, secure handling, storage and distribution of all EU crypto material; and
    (c) ensuring the transfer of EU crypto material to or from individuals or services using it.

Security Accreditation Authority (SAA)

47. The SAA for each system shall be responsible for:
    (a) ensuring that CIS comply with the relevant security Guidelines, providing a statement of approval for CIS to handle EUCI to a defined level of classification in its operational environment, stating the terms and conditions of the accreditation, and criteria under which re-approval is required;
    (b) establishing a security accreditation process, in accordance with the relevant Guidelines, clearly stating the approval conditions for CIS under its authority;
    (c) defining a security accreditation strategy setting out the degree of detail for the accreditation process commensurate with the required level of assurance;
    (d) examining and approving security-related documentation, including risk management and residual risk statements, System-specific Security Requirement Statements (hereinafter referred to as 'SSRSs'), security implementation verification documentation and Security Operating Procedures (hereinafter referred to as 'SecOPs'), and ensuring that it complies with the EEAS's security rules and Guidelines;

47. The SAA for each system shall be responsible for:
    (a) ensuring that CIS comply with the relevant security Guidelines, providing a statement of approval for CIS to handle EUCI to a defined level of classification in its operational environment, stating the terms and conditions of the accreditation, and criteria under which re-approval is required;
    (b) establishing a security accreditation process, in accordance with the relevant Guidelines, clearly stating the approval conditions for CIS under its authority;
    (c) defining a security accreditation strategy setting out the degree of detail for the accreditation process commensurate with the required level of assurance;
    (d) examining and approving security-related documentation, including risk management and residual risk statements, System-specific Security Requirement Statements (hereinafter referred to as 'SSRSs'), security implementation verification documentation and Security Operating Procedures (hereinafter referred to as 'SecOPs'), and ensuring that it complies with the EEAS's security rules and Guidelines;
    (e) checking implementation of security measures in relation to the CIS by undertaking or sponsoring security assessments, inspections or reviews;
    (f) defining security requirements (e.g. personnel security clearance levels) for sensitive positions in relation to the CIS;
    (g) endorsing the selection of approved cryptographic and TEMPEST products used to provide security for a CIS;
    (h) approving, or where relevant, participating in the joint approval of the interconnection of a CIS to other CIS; and
    (i) consulting the system provider, the security actors and representatives of the users with respect to security risk management, in particular the residual risk, and the terms and conditions of the approval statement.
48. The EEAS SAA shall be responsible for accrediting all CIS operating within the remit of the EEAS.

Security Accreditation Board (SAB)

49. A joint SAB shall be responsible for accrediting CIS within the remit of both the EEAS SAA and Member States' SAAs. It shall be composed of an SAA representative from each Member State and be attended by an SAA representative of the GSC and Commission. Other entities with nodes on a CIS shall be invited to attend when that system is under discussion.

    The SAB shall be chaired by a representative of the EEAS SAA. It shall act by consensus of SAA representatives of institutions, Member States and other entities with nodes on the CIS. It shall make periodic reports on its activities to the EEAS Security Committee and shall notify it of all accreditation statements.

Information Assurance Operational Authority

50. The IA Operational Authority for each system shall be responsible for:
    (a) developing security documentation in line with security Guidelines, in particular the System-specific Security Requirement Statement (**SSRS**) including the residual risk statement, the Security Operating Procedures (**SecOPs**) and the crypto plan within the CIS accreditation process;
    (b) participating in selecting and testing the system-specific technical security measures, devices and software, to supervise their implementation and to ensure that they are securely installed, configured and maintained in accordance with the relevant security documentation;
    (c) participating in selecting TEMPEST security measures and devices if required in the SSRS and ensuring that they are securely installed and maintained in cooperation with the TA;
    (d) monitoring implementation and application of the SecOPs and, where appropriate, delegating operational security responsibilities to the system owner;
    (e) managing and handling cryptographic products, ensuring the custody of crypto and controlled items and, if so required, ensuring the generation of cryptographic variables;
    (f) conducting security analysis reviews and tests, in particular to produce the relevant risk reports, as required by the SAA;
    (g) providing CIS-specific IA training;
    (h) implementing and operating CIS-specific security measures.

ANNEX A V

INDUSTRIAL SECURITY

I. INTRODUCTION

1. This Annex sets out provisions for implementing Article 9 of Annex A. It lays down general security provisions applicable to industrial or other entities in pre-contract negotiations and throughout the life-cycle of classified contracts let by the EEAS.

2. The EEAS Security Authority shall approve Guidelines on industrial security outlining in particular detailed requirements regarding Facility Security Clearances (FSCs), Security Aspects Letters (SALs), visits, transmission and carriage of EUCI.

II. SECURITY ELEMENTS IN A CLASSIFIED CONTRACT

Security classification guide (SCG)

3. Prior to launching an invitation to tender or letting a classified contract, the EEAS, as the contracting authority, shall determine the security classification of any information to be provided to bidders and contractors, as well as the security classification of any information to be created by the contractor. For that purpose, the EEAS shall prepare a SCG to be used for the performance of the contract.

4. In order to determine the security classification of the various elements of a classified contract, the following principles shall apply:
   (a) in preparing an SCG, the EEAS shall take into account all relevant security aspects, including the security classification assigned to information provided and approved to be used for the contract by the originator of the information;
   (b) the overall level of classification of the contract may not be lower than the highest classification of any of its elements; and
   (c) where relevant, the EEAS shall liaise with the Member States' NSAs/DSAs or any other competent security authority concerned in the event of any changes regarding the classification of information created by or provided to contractors in the performance of a contract and when making any subsequent changes to the SCG.

Security aspects letter (SAL)

5. The contract-specific security requirements shall be described in an SAL. The SAL shall, where appropriate, contain the SCG and shall be an integral part of a classified contract or sub-contract.

6. The SAL shall contain provisions requiring the contractor and/or subcontractor to comply with the minimum standards laid down in this Decision. Non-compliance with these minimum standards may constitute sufficient grounds for the contract to be terminated.

Programme/project security instructions (PSI)

7. Depending on the scope of programmes or projects involving access to or handling or storage of EUCI, specific Programme/Project Security Instructions (PSI) may be prepared by the contracting authority designated to manage the programme or project. The PSI shall require the approval of the Member States' NSAs/DSAs or any other competent security authority participating in the programme/project and may contain additional security requirements.

III. FACILITY SECURITY CLEARANCE (FSC)

8. The EEAS Directorate responsible for security shall request the NSA or DSA or other competent security authority of the Member State concerned to grant an FSC to indicate, in accordance with national laws and regulations, that an industrial or other entity can protect EUCI at the appropriate classification level (CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET) within its facilities. A contractor, subcontractor, or potential contractor or subcontractor shall not be provided with or granted access to EUCI, until proof of FSC has been transmitted to the EEAS.

9. Where relevant, the EEAS, as the contracting authority, shall notify the appropriate NSA/DSA or any other competent security authority that an FSC is required in the pre-contractual stage or for performing the contract. An FSC or PSC shall be required in the pre-contractual stage where EUCI classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET has to be provided in the course of the bidding process.

10. The EEAS as contracting authority shall not award a classified contract with a preferred bidder before having received confirmation from the NSA/DSA or any other competent security authority of the Member State in which the contractor or subcontractor concerned is registered that, where required, an appropriate FSC has been issued.

11. The EEAS as contracting authority shall request the NSA/DSA or any other competent security authority which has issued an FSC to notify it of any adverse information affecting the FSC. In the case of a sub-contract, the NSA/DSA or any other competent security authority shall be informed accordingly.

12. Withdrawal of an FSC by the relevant NSA/DSA or any other competent security authority shall constitute sufficient grounds for the EEAS, as the contracting authority, to terminate a classified contract or exclude a bidder from the competition.

IV. PERSONNEL SECURITY CLEARANCES (PSCS) FOR CONTRACTORS' PERSONNEL

13. All personnel working for contractors requiring access to EUCI classified CONFIDENTIEL UE/EU CONFIDENTIAL or above shall have been appropriately security cleared and have a need-to-know to access the information. Although a PSC is not required for access to EUCI at the level of RESTREINT UE/EU RESTRICTED, the need-to-know for such access shall exist.

14. Applications for the PSCs for contractor personnel shall be made to the NSA/DSA responsible for the entity.

15. The EEAS shall point out to contractors wishing to employ a national of a third State in a position that requires access to EUCI, that it is the responsibility of the NSA/DSA of the Member State in which the hiring entity is located and incorporated to determine whether the individual can be granted access to such information, in accordance with this Decision, and to confirm that the originator's consent must have been provided before such access is given.

V. CLASSIFIED CONTRACTS AND SUB-CONTRACTS

16. Where EUCI is provided to a bidder at the pre-contractual stage, the invitation to tender shall contain a provision obliging a bidder which fails to submit a bid or which is not selected to return all classified documents within a specified period of time.

17. Once a classified contract or sub-contract has been awarded, the EEAS, as the contracting authority, shall notify the contractor's or subcontractor's NSA/DSA or any other competent security authority about the security provisions of the classified contract.

18. When such contracts are terminated or they end, the EEAS, as the contracting authority (and/or the NSA/DSA or any other competent security authority, as appropriate, in the case of a sub-contract) shall promptly notify the NSA/DSA or any other competent security authority of the Member State in which the contractor or subcontractor is registered.

19. As a general rule, the contractor or subcontractor shall be required to return to the contracting authority, upon termination or ending of the classified contract or sub-contract, any EUCI held by it.

20. Specific provisions for the disposal of EUCI during the performance of the contract or upon its termination or ending shall be laid down in the SAL.

21. Where the contractor or subcontractor is authorised to retain EUCI after termination or ending of a contract, the minimum standards contained in this Decision shall continue to be complied with and the confidentiality of EUCI shall be protected by the contractor or subcontractor.

22. The conditions under which the contractor may subcontract shall be defined in the invitation to tender and in the contract.

23. A contractor shall obtain permission from the EEAS, as the contracting authority, before sub-contracting any parts of a classified contract. No subcontract may be awarded to industrial or other entities registered in a non-EU Member State which has not concluded a security of information Agreement with the EU.

24. The contractor shall be responsible for ensuring that all sub-contracting activities are undertaken in accordance with the minimum standards laid down in this Decision and shall not provide EUCI to a subcontractor without the prior written consent of the contracting authority.

25. With regard to EUCI created or handled by the contractor or subcontractor, the rights incumbent on the originator shall be exercised by the contracting authority.

VI. VISITS IN CONNECTION WITH CLASSIFIED CONTRACTS

26. Where the EEAS, contractors or subcontractors require access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET in each other's premises for the performance of a classified contract, visits shall be arranged by liaison with the NSAs/DSAs or any other competent security authority concerned. This is without prejudice to the prerogative of the NSAs/DSAs, in the context of specific projects, to agree on a procedure whereby such visits can be arranged directly.

27. All visitors shall hold an appropriate PSC and have a 'need-to-know' for access to the EUCI related to the EEAS contract.

28. Visitors shall be given access only to EUCI related to the purpose of the visit.

VII. TRANSMISSION AND CARRIAGE OF EUCI

29. With regard to the transmission of EUCI by electronic means, the relevant provisions of Article 8 of Annex A, and of Annex A IV shall apply.

30. With regard to the carriage of EUCI, the relevant provisions of Annex A III shall apply, in accordance with national laws and regulations.

31. For the transport of classified material as freight, the following principles shall be applied when determining security arrangements:
    (a) security shall be assured at all stages during transportation from the point of origin to the final destination;
    (b) the degree of protection afforded to a consignment shall be determined by the highest classification level of material contained within it;
    (c) an FSC at the appropriate level shall be obtained for companies providing transportation, if it also implies that classified information is stored in contractors' facilities. In any case, personnel handling the consignment shall be appropriately security cleared in accordance with Annex A I;
    (d) prior to any cross-border movement of material classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET, a transportation plan shall be drawn up by the consignor and approved by the EEAS when appropriate in liaison with the NSA/DSAs of both the consignor and the consignee or any other competent security authority concerned;
    (e) journeys shall be point to point to the extent possible, and shall be completed as quickly as circumstances permit;
    (f) whenever possible, routes should be only through Member States. Routes through States other than Member States should only be undertaken when authorised by the EEAS or any other competent security authority of the States of both the consignor and the consignee.

VIII. TRANSFER OF EUCI TO CONTRACTORS LOCATED IN THIRD STATES

32. EUCI shall be transferred to contractors and subcontractors located in third States that have a valid security agreement with the EU in accordance with security measures agreed between the EEAS, as the contracting authority, and the NSA/DSA of the third State concerned where the contractor is registered.

IX. HANDLING AND STORAGE OF INFORMATION CLASSIFIED RESTREINT UE/EU RESTRICTED

33. In liaison, as appropriate, with the NSA/DSA of the Member State the EEAS, as the contracting authority, shall be entitled to conduct visits to contractors'/subcontractors' facilities on the basis of contractual provisions in order to verify that the relevant security measures for the protection of EUCI at the level RESTREINT UE/EU RESTRICTED as required under the contract have been put in place.

34. To the extent necessary under national laws and regulations, NSAs/DSAs or any other competent security authority shall be notified by the EEAS as the contracting authority of contracts or sub-contracts containing information classified RESTREINT UE/EU RESTRICTED.

35. An FSC or a PSC for contractors or subcontractors and their personnel shall not be required for contracts let by the EEAS containing information classified RESTREINT UE/EU RESTRICTED.

36. The EEAS, as the contracting authority, shall examine the responses to invitations to tender for contracts which require access to information classified RESTREINT UE/EU RESTRICTED, notwithstanding any requirement relating to FSC or PSC which may exist under national laws and regulations.

37. The conditions under which the contractor may subcontract shall be in accordance with paragraphs 22-24.

38. Where a contract involves handling information classified RESTREINT UE/EU RESTRICTED in a CIS operated by a contractor, the EEAS as contracting authority shall ensure that the contract or any sub-contract specifies the necessary technical and administrative requirements regarding accreditation of the CIS commensurate with the assessed risk, taking account of all relevant factors. The scope of accreditation of such CIS shall be agreed between the contracting authority and the relevant NSA/DSA.

ANNEX A VI

EXCHANGE OF CLASSIFIED INFORMATION WITH THIRD STATES AND INTERNATIONAL ORGANISATIONS

I. INTRODUCTION

1. This Annex sets out provisions for implementing Article 10 of Annex A.

II. FRAMEWORKS GOVERNING THE EXCHANGE OF CLASSIFIED INFORMATION

2. The EEAS may exchange EUCI with third States or international organisations in accordance with Article 10(1) of Annex A.

   To support the HR in performing the responsibilities set out in Article 218 TFEU:

   (a) the relevant EEAS geographical or thematic department, in consultation with the EEAS Directorate responsible for security, shall, when appropriate, identify the need for a long term exchange of EUCI with the third State or international organisation concerned;

   (b) the EEAS Directorate responsible for security, in consultation with the relevant EEAS geographical department, shall, where appropriate, submit to the HR the draft texts to be proposed to the Council by virtue of Article 218(3),(5), and (6) of TFEU;

   (c) the EEAS Directorate responsible for security shall support the HR in conducting negotiations, in coordination with the relevant services of the Commission and of the General Secretariat of the Council;

(d) in relation to agreements or arrangements with third States for their participation in CSDP crisis management operations as referred to in Article 10(1)(c) of Annex A, the EEAS Crisis Management and Planning Directorate, in consultation with the relevant EEAS services, shall, where appropriate, submit to the HR the draft texts to be proposed to the Council by virtue of Article 218(3),(5), and (6) of TFEU, and shall support the HR in conducting negotiations in coordination with the relevant services of the EEAS and of the General Secretariat of the Council.

3. Where security of information agreements provide for technical implementing arrangements to be agreed between the EEAS Directorate responsible for security – in coordination with the Security Directorate of the Directorate General for Human Resources and Security of the Commission and the Security Office of the General Secretariat of the Council – and the competent security authority of the third State or international organisation in question, such arrangements shall take account of the level of protection provided by the security regulations, structures and procedures in place in the third State or international organisation concerned.

4. Where a long-term need exists for the EEAS to exchange information classified in principle no higher than RESTREINT UE/EU RESTRICTED with a third State or international organisation, and where it has been established that the party in question does not have a sufficiently developed security system for it to be possible to enter into a security of information agreement, the HR may, after having obtained the unanimous favourable opinion of the EEAS Security Committee in accordance with Article 15(5) of this Decision, enter into an administrative arrangement with the competent security authorities of the third State or international organisation in question.

5. No EUCI shall be exchanged by electronic means with a third State or international organisation unless explicitly provided for in the security of information agreement or administrative arrangement.

6. Under an administrative arrangement on the exchange of classified information, the EEAS and the third State or international organisation shall each designate a registry as the main point of entry and exit for classified information exchanged. For the EEAS, this will be the EEAS central registry.

7. Administrative arrangements shall as a general rule take the form of an exchange of letters.

III. ASSESSMENT VISITS

8. Assessment visits referred to in Article 17 of this Decision shall be conducted by mutual agreement with the third State or international organisation concerned, and shall evaluate:
   (a) the regulatory framework applicable for protecting classified information;
   (b) any specific features of the third State or international organisation's security laws, regulations, policies or procedures which may have an impact on the maximum level of classified information that may be exchanged;
   (c) the security measures and procedures currently in place for the protection of classified information; and
   (d) security clearance procedures for the level of EUCI to be released.

9. No EUCI shall be exchanged before an assessment visit has been conducted and the level at which classified information may be exchanged between the parties has been determined, based on the equivalency of the level of protection that will be afforded to it.

   If, pending such an assessment visit, the HR is made aware of any exceptional or urgent reasons for exchanging classified information, the EEAS shall:
   (a) first seek the originator's written consent to establish that there are no objections to release.
   (b) refer to the EEAS Security Authority, who may decide to release, provided that the unanimous favourable opinion of the Member States as represented in the EEAS Security Committee has been obtained.

   If the EEAS cannot establish the originator, the EEAS Security Authority shall assume the originator's responsibility after having obtained the unanimous favourable opinion of the EEAS Security Committee.

IV. AUTHORITY TO RELEASE EUCI TO THIRD STATES OR INTERNATIONAL ORGANISATIONS

10. Where a framework exists in accordance with Article 10(1) of Annex A for exchanging classified information with a third State or international organisation, the decision to release EUCI by the EEAS to a third State or international organisation shall be taken by the EEAS Security Authority, which may delegate such authorisation to senior EEAS officials or other persons under its authority.

11. If the originator of the classified information to be released, including the originators of source material it may contain, is not the EEAS, the EEAS shall first seek the originator's written consent to establish that there are no objections to release. If the EEAS cannot establish the originator, the EEAS Security Authority shall assume the originator's responsibility after having obtained the unanimous favourable opinion of the Member States as represented in the EEAS Security Committee.

V. EXCEPTIONAL AD HOC RELEASE OF EUCI

12. In the absence of one of the frameworks referred to in Article 10(1) of Annex A, and when the interests of the EU or of one or more of its Member States require the release of EUCI for political, operational or urgent reasons, EUCI may exceptionally be released to a third State or international organisation once the following actions have been taken.

    The EEAS Directorate responsible for security shall, after ensuring that conditions referred to in Paragraph 11 above are met:

    (a) to the extent possible, verify with the security authorities of the third State or international organisation concerned that its security regulations, structures and procedures are such that EUCI released to it will be protected in accordance with standards no less stringent than those laid down in this Decision;

    (b) invite the EEAS Security Committee to formulate an opinion, on the basis of the available information, regarding the confidence that can be placed on the security regulations, structures and procedures in the third State or international organisation to which the EUCI is to be released;

(c) refer to the EEAS Security Authority, who may decide to release, provided that the unanimous favourable opinion of the Member States as represented in the EEAS Security Committee has been obtained.

13. In the absence of one of the frameworks referred to in Article 10(1) of Annex A, the third party in question shall undertake in writing to protect the EUCI appropriately.

Appendix A

Definitions

For the purposes of this Decision, the following definitions shall apply:

'Accreditation' means the process leading to a formal statement by the Security Accreditation Authority (SAA) that a system is approved to operate with a defined level of classification, in a particular security mode in its operational environment and at an acceptable level of risk, based on the premise that an approved set of technical, physical, organisational and procedural security measures has been implemented;

'Asset' means anything that is of value to an organisation, its business operations and their continuity, including information resources that support the organisation's mission;

'Authorisation to access EUCI' means an authorisation by the EEAS Security Authority, which is taken in accordance with this Decision after a PSC has been issued by the competent authorities of a Member State, and which certifies that an individual may, provided his 'need-to-know' has been determined, be granted access to EUCI up to a specified level (CONFIDENTIEL UE/EU CONFIDENTIAL or above) until a specified date – see Article 2 of Annex A I;

'Breach' is an act or omission by an individual which is contrary to the security rules laid down in this Decision and/or to the security policies or guidelines setting out any measures necessary for its implementation;

'CIS life-cycle' means the entire duration of existence of a CIS, which includes initiation, conception, planning, requirements analysis, design, development, testing, implementation, operation, maintenance and decommissioning;

'Classified contract' means a contract entered into by the EEAS with a contractor for the supply of goods, execution of works or provision of services, the performance of which requires or involves access to or the creation of EUCI;

'Classified subcontract' means a contract entered into by a contractor of the EEAS with another contractor (i.e. the subcontractor) for the supply of goods, execution of works or provision of services, the performance of which requires or involves access to or the creation of EUCI;

'Communication and information system' (CIS) means any system enabling the handling of information in electronic form. A communication and information system shall comprise the entire assets required for it to operate, including the infrastructure, organisation, personnel and information resources; – see Article 8 (2) of Annex A;

'Compromise of EUCI' means the total or partial disclosure of EUCI to unauthorised persons or entities – see Article 9(2);

'Contractor' means an individual or legal entity possessing the legal capacity to undertake contracts;

'Cryptographic (Crypto) products' are cryptographic algorithms, cryptographic hardware and software modules, and products including implementation details and associated documentation and keying material;

'CSDP operation' means a military or civilian crisis management operation under Title V, Chapter 2, of the TEU;

'Declassification' means the removal of any security classification;

'Defence in depth' means the application of a range of security measures organised as multiple layers of defence;

'Designated Security Authority' (DSA) means an authority responsible to the National Security Authority (NSA) of a Member State which is responsible for communicating to industrial or other entities national policy on all matters of industrial security and for providing direction and assistance in its implementation. The function of DSA may be carried out by the NSA or by any other competent authority;

'Document' means any recorded information regardless of its physical form or characteristics;

'Downgrading' means a reduction in the level of security classification;

'EU classified information' (EUCI) means any information or material the unauthorized disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States, designated by an EU security classification – see Article 2 (f);

'Facility Security Clearance' (FSC) means an administrative determination by an NSA or DSA that, from the security viewpoint, a facility can afford an adequate level of protection to EUCI of a specified security classification level and its personnel who require access to EUCI have been appropriately security cleared and briefed on the relevant security requirements necessary to access and protect EUCI;

'Handling' of EUCI means all possible actions to which EUCI may be subject throughout its life-cycle. It comprises its creation, processing, carriage, downgrading, declassification and destruction. In relation to CIS it also comprises its collection, display, transmission and storage;

'Holder' means a duly authorised individual with an established need-to-know who is in possession of an item of EUCI and is accordingly responsible for protecting it;

'Industrial or other entity' means an entity involved in supplying goods, executing works or providing services; this may be an industrial, commercial, service, scientific, research, educational or development entity or a self-employed individual;

'Industrial security' is the application of measures to ensure the protection of EUCI by contractors or subcontractors in pre-contract negotiations and throughout the life-cycle of classified contracts – see Article 9(1) of Annex A;

'Information Assurance' in the field of communication and information systems is the confidence that such systems will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users. Effective IA shall ensure appropriate levels of confidentiality, integrity, availability, non-repudiation and authenticity. IA shall be based on a risk management process – see Article 8(1) of Annex A;

'Interconnection' means, for the purposes of this Decision, the direct connection of two or more IT systems for the purpose of sharing data and other information resources (e.g. communication) in a unidirectional or multidirectional way– see Annex A IV, paragraph 31;

'Management of classified information' is the application of administrative measures for controlling EUCI throughout its life-cycle to supplement the measures provided for in Articles 5, 6 and 8 and thereby help deter, detect and recover from deliberate or accidental compromise or loss of such information. Such measures relate in particular to the creation, registration, copying, translation, carriage, handling, storage and destruction of EUCI – see Article 7(1) of Annex A;

'Material' means any document or item of machinery or equipment, either manufactured or in the process of manufacture;

'Originator' means the EU institution, agency or body, Member State, third state or international organisation under whose authority classified information has been created and/or introduced into the EU's structures;

'Personnel security' is the application of measures to ensure that access to EUCI is granted only to individuals who have:
- a need-to-know;
- for access to CONFIDENTIEL UE/EU CONFIDENTIAL information or above, been security cleared to the relevant level, or are otherwise duly authorised by virtue of their functions in accordance with national laws and regulations; and
- been briefed on their responsibilities – see Article 5(1) of Annex A;

'Personnel Security Clearance' (PSC) for access to EUCI means a statement by a competent authority of a Member State which is made following completion of a security investigation conducted by the competent authorities of a Member State and which certifies that an individual may, provided his 'need-to-know' has been determined, be granted access to EUCI up to a specified level (CONFIDENTIEL UE/EU CONFIDENTIAL or above) until a specified date; the individual thus described is said to be 'security cleared';

'Personnel Security Clearance Certificate' (PSCC) means a certificate issued by a competent authority establishing that an individual is security cleared and holds a valid PSC or Authorisation from the Head of the Directorate responsible for security for access to EUCI, and which shows the level of EUCI to which that individual may be granted access (CONFIDENTIEL UE/EU CONFIDENTIAL or above), the date of validity of the relevant PSC and the date of expiry of the certificate itself;

'Physical security' is the application of physical and technical protective measures to deter unauthorised access to EUCI – see Article 6 of Annex A;

'Programme/Project Security Instruction' (PSI) means a list of security procedures which are applied to a specific programme/project in order to standardise security procedures. It may be revised throughout the programme/project;

'Registration' means the application of procedures that record the life-cycle of information, including its dissemination and destruction – see Annex A III, paragraph 21;

'Residual risk' means the risk which remains after security measures have been implemented, given that not all threats are countered and not all vulnerabilities can be eliminated;

'Risk' means the potential that a given threat will exploit internal and external vulnerabilities of an organisation or of any of the systems it uses and thereby cause harm to the organisation and to its tangible or intangible assets. It is measured as a combination of the likelihood of threats occurring and their impact;

'Risk acceptance' is the decision to agree to the further existence of a residual risk after risk treatment;

'Risk assessment' consists of identifying threats and vulnerabilities and conducting the related risk analysis, i.e. the analysis of probability and impact;

'Risk communication' consists of developing awareness of risks among CIS user communities, informing approval authorities such risks and reporting them to operating authorities;

'Risk management process' means the entire process of identifying, controlling and minimising uncertain events that may affect the security of an organisation or of any of the systems it uses. It covers the entirety of risk-related activities, including assessment, treatment, acceptance and communication;

'Risk treatment' consists of mitigating, removing, reducing (through an appropriate combination of technical, physical, organisational or procedural measures), transferring or monitoring the risk;

'Security Aspects Letter' (SAL) means a set of special contractual conditions issued by the contracting authority which forms an integral part of any classified contract involving access to or the creation of EUCI, that identifies the security requirements or those elements of the contract requiring security protection – see Annex A V, Section II;

'Security Classification Guide' (SCG) means a document which describes the elements of a programme or contract which are classified, specifying the applicable security classification levels. The SCG may be expanded throughout the life of the programme or contract and the elements of information may be re-classified or downgraded; where an SCG exists it shall be part of the SAL – see Annex A V, Section II;

'Security investigation' means the investigative procedures conducted by the competent authority of a Member State in accordance with its national laws and regulations in order to obtain an assurance that nothing adverse is known which would prevent an individual from being granted a national or EU PSC for access to EUCI up to a specified level (CONFIDENTIEL UE/EU CONFIDENTIAL or above);

'Security Operating Procedures' (SecOPs) means a description of the security policy implementation to be adopted, of the operating procedures to be followed and of the personnel responsibilities;

'Sensitive non-classified information' means information or material that the EEAS must protect because of legal obligations laid down in the Treaties or in acts adopted in implementation thereof, and/or because of its sensitivity. Sensitive non-classified information includes, but is not limited to, information or material covered by the obligation of professional secrecy, as referred to in Article 339 TFEU, information covered by the interests protected in Article 4 of Regulation (EC) No 1049/2001 of the European Parliament and of the Council ([1]) read in conjunction with the relevant case-law of the Court of Justice of the European Union or personal data within the scope of Regulation (EC) No 45/2001;

'Specific Security Requirement Statement' (SSRS) means a binding set of security principles to be observed and of detailed security requirements to be implemented, underlying the process of certification and accreditation of CIS;

'TEMPEST' means the investigation, study and control of compromising electromagnetic emanations and the measures to suppress them;

'Threat' means a potential cause of an unwanted incident which may result in harm to an organisation or any of the systems it uses; such threats may be accidental or deliberate (malicious) and are characterised by threatening elements, potential targets and attack methods;

'Vulnerability' means a weakness of any nature that can be exploited by one or more threats. Vulnerability may be an omission or it may relate to a weakness in controls in terms of their strength, completeness or consistency and may be of a technical, procedural, physical, organisational or operational nature.

([1]) Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43).

Appendix B

Equivalence of security classifications

EU	TRES SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
EURATOM	EURA TOP SECRET	EURA SECRET	EURA CONFIDENTIAL	EURA RESTRICTED
Belgium	Très Secret (Loi 11.12.1998) Zeer Geheim (Wet 11.12.1998)	Secret (Loi 11.12.1998) Geheim (Wet 11.12.1998)	Confidentiel (Loi 11.12.1998) Vertrouwelijk (Wet 11.12.1998)	Nota ([1]) below
Bulgaria	Строго секретно	Секретно	Поверително	За служебно ползване
Czech Republic	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Denmark	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Germany	STRENG GEHEIM	GEHEIM	VS ([2]) – VERTRAULICH	VS – NUR FÜR DEN DIENSTGEBRAUCH
Estonia	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Ireland	Top Secret	Secret	Confidential	Restricted
Greece	Άκρως Απόρρητο Abr: ΑΑΠ	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Spain	SECRETO	RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
France	Très Secret Défense	Secret Défense	Confidentiel Défense	Nota ([3]) below
Croatia	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Italy	Segretissimo	Segreto	Riservatissimo	Riservato
Cyprus	Άκρως Απόρρητο Abr: (ΑΑΠ)	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Latvia	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Lithuania	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Luxembourg	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Hungary	‘Szigorúan titkos!’	‘Titkos!’	‘Bizalmas!’	‘Korlátozott terjesztésű!’

Malta	L-Ogħla Segretezza	Sigriet	Kunfidenzjali	Ristrett
Netherlands	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Austria	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Poland	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugal	Muito Secreto	Secreto	Confidencial	Reservado
Romania	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu
Slovenia	Strogo tajno	Tajno	Zaupno	Interno
Slovakia	Prísne tajné	Tajné	Dôverné	Vyhradené
Finland	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Sweden ([4])	HEMLIG/TOP SECRET	HEMLIG/SECRET	HEMLIG/CONFIDENTIAL	HEMLIG/RESTRICTED
	HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG	HEMLIG	HEMLIG
United Kingdom	UK TOP SECRET	UK SECRET	No equivalent ([5])	UK OFFICIAL – SENSITIVE

([1]) Diffusion Restreinte/Beperkte Verspreiding is not a security classification in Belgium. Belgium handles and protects 'RESTREINT UE/EU RESTRICTED' information in a manner no less stringent than the standards and procedures described in the security rules of the Council of the European Union.

([2]) Germany: VS = Verschlusssache.

([3]) France does not use the classification 'RESTREINT' in its national system. France handles and protects 'RESTREINT UE/EU RESTRICTED' information in a manner no less stringent than the standards and procedures described in the security rules of the Council of the European Union.

([4]) Sweden: the security classification markings in the top row are used by the defence authorities and the markings in the bottom row by other authorities.

([5]) The UK handles and protects EUCI marked CONFIDENTIEL UE/EU CONFIDENTIAL in accordance with the protective security requirements for UK SECRET.

SANTRUMPŲ SĄRAŠAS

Santrumpa	Reikšmė
APP	Asmens patikimumo pažymėjimas
APPP	Asmens patikimumo pažymėjimą patvirtinanti pažyma
AVSS	Apsauginės vaizdo stebėjimo sistemos
BSGP	Bendra saugumo ir gynybos politika
BUSP	Bendra užsienio ir saugumo politika
COREPER	Nuolatinių atstovų komitetas
EIVT	Europos Išorės veiksmų tarnyba
EKSD	Europos Komisijos saugumo direktoratas
ESĮI	ES įslaptinta informacija
ESSĮ	ES specialusis įgaliotinis
ĮAS	Įsibrovimo aptikimo sistema
ĮPPP	Įmonės patikimumą patvirtinantis pažymėjimas
ISU	Informacijos saugumo užtikrinimas
ISUI	Informacijos saugumo užtikrinimo institucija
IT	Informacinė technologija
KPI	Kriptografijos patvirtinimo institucija
KPLI	Kriptografijos platinimo institucija
NSI	Nacionalinė saugumo institucija
PRSI	Programos / projekto saugumo instrukcijos
PSI	Paskirtoji saugumo institucija
RAP	Ribų apsaugos priemonė
RIS	Ryšių ir informacinės sistemos, kuriose tvarkoma ESĮI
SAI	Saugumo akreditavimo institucija
SAP	Saugumo aspektų paaiškinimai
SAV	Saugumo akreditavimo valdyba
SecOPs	Saugumo įgyvendinimo patikrinimo dokumentai ir saugios eksploatacijos taisyklės
SSRA	Sistemos saugumo reikmių aktai
SŽV	Slaptumo žymų vadovas
TEI	TEMPEST institucija
TGS	Tarybos Generalinis sekretoriatas
TKI	Tinkamos kvalifikacijos institucija

LIST OF ABBREVIATIONS

Acronym	Meaning
AQUA	Appropriately Qualified Authority
BPS	Boundary Protection Services
CAA	Crypto Approval Authority
CCTV	Closed Circuit Television
CDA	Crypto Distribution Authority
CFSP	Common Foreign and Security Policy
CIS	Communication and Information Systems handling EUCI
COREPER	Committee of Permanent Representatives
CSDP	Common Security and Defence Policy
DSA	Designated Security Authority
EEAS	European External Action Service
ECSD	European Commission Security Directorate
EUCI	EU Classified Information
EUSR	EU Special Representative
FSC	Facility Security Clearance
GSC	General Secretariat of the Council
IA	Information Assurance
IAA	Information Assurance Authority
IDS	Intrusion Detection System
IT	Information Technology
NSA	National Security Authority
PSC	Personnel Security Clearance
PSCC	Personnel Security Clearance Certificate
PSI	Programme/Project Security Instructions
SAA	Security Accreditation Authority
SAB	Security Accreditation Board
SAL	Security Aspects Letter
SecOPs	Security Operating Procedures
SCG	Security Classification Guide
SSRS	System-Specific Security Requirement Statement
TA	TEMPEST Authority

TERMINŲ ŽINYNAS / GLOSSARY OF TERMS AND DEFINITIONS

TERMINŲ ŽINYNAS

A

Akreditavimas – procesas, po kurio Saugumo akreditavimo institucija (SAI) pateikia oficialų pareiškimą, patvirtinantį kad sistemai yra leista veikti, taikant nustatytą slaptumo žymos laipsnį, konkrečiu slaptumo režimu jos operacinėje aplinkoje ir priimtinu rizikos lygiu, laikantis prielaidos, kad įgyvendintas patvirtintas techninių, fizinių, organizacinių ir procedūrinių saugumo priemonių rinkinys.

Asmens patikimumo pažymėjimas (APP), kuriuo suteikiama teisė susipažinti su ESĮI – valstybės narės kompetentingos institucijos patvirtinimas, kuris pateikiamas valstybės narės kompetentingoms institucijoms baigus patikimumo tyrimą ir kuriuo pažymima, kad atitinkamam asmeniui, nustačius, kad jis atitinka principą „būtina žinoti“, suteikiamas leidimas iki nurodytos datos susipažinti su atitinkamo lygio slaptumo žyma (CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio lygio slaptumo žyma) pažymėta ESĮI. Laikoma, kad asmens, kuriam taikoma ši apibrėžtis, patikimumas patikrintas.

Asmens patikimumo pažymėjimą patvirtinanti pažyma (APPP) yra EIVT saugumo institucijos išduota pažyma, kurioje nurodoma, kad asmens patikimumas yra patikrintas, ir nurodomas ESĮI, su kuria tam asmeniui gali būti leista susipažinti, slaptumo žymos lygis, atitinkamo APP galiojimo laikas ir pačios pažymos galiojimo laikas.

B

BSGP operacija – karinio ar civilinio krizių valdymo operacija.

D

Darbuotojai, už kurių įdarbinimą atsakinga EIVT, – būstinėje ir Europos Sąjungos delegacijose dirbantys EIVT darbuotojai ir kiti Europos Sąjungos delegacijų darbuotojai, nepaisant jų administracinio statuso ar to, kokia administracija juos paskyrė, taip pat, kaip nustatyta šiame sprendime, vyriausiasis įgaliotinis ir, jei taikytina, kiti darbuotojai, kurie dirba EIVT būstinės patalpose.

Dokumentas – bet kokia fiksuota informacija, neatsižvelgiant į jos fizinę formą ar charakteristikas.

Duomenys – informacija tokios formos, kad ją būtų galima perduoti, registruoti arba tvarkyti.

E

ES įslaptinta informacija

ES įslaptinta informacija (ESĮI) – bet kuri informacija arba medžiaga, kuriai suteikta ES slaptumo žyma ir kurią neteisėtai atskleidus galėtų būti padaryta tam tikro dydžio žala Europos Sąjungos arba vienos ar kelių valstybių narių interesams.

ES įslaptinta informacija (ESĮI) – bet kokia informacija ir medžiaga, pažymėta slaptumo žymomis TRÈS SECRET UE/EU TOP SECRET, SECRET UE/EU SECRET, CONFIDENTIEL UE/EU CONFIDENTIAL arba RESTREINT UE/EU RESTRICTED, kurią atskleidus be leidimo gali būti padaryta įvairaus laipsnio žalos Europos Sąjungos interesams arba vienos ar daugiau valstybių narių interesams, neatsižvelgiant į tai, ar ta informacija buvo parengta institucijose, įstaigose, tarnybose ar agentūrose, įsteigtose pagal Sutartis arba jomis remiantis, ar yra gauta iš valstybių narių, trečiųjų šalių ar tarptautinių organizacijų. Šiuo atveju informacija ir medžiaga žymima slaptumo žyma:

TRÈS SECRET UE/EU TOP SECRET – tai informacija ir medžiaga, kurią atskleidus be leidimo gali būti padaryta ypatingai didelė žala

esminiams Europos Sąjungos arba vienos ar daugiau valstybių narių interesams;

SECRET UE/EU SECRET – tai informacija ir medžiaga, kurią atskleidus be leidimo gali būti rimtai pakenkta esminiams Europos Sąjungos arba vienos ar daugiau valstybių narių interesams;

CONFIDENTIEL UE/EU CONFIDENTIAL – tai informacija ir medžiaga, kurią atskleidus be leidimo gali būti pakenkta esminiams Europos Sąjungos arba vienos ar daugiau valstybių narių interesams;

RESTREINT UE/EU RESTRICTED – tai informacija ir medžiaga, kurių atskleidimas be leidimo gali būti nenaudingas Europos Sąjungos arba vienos ar daugiau valstybių narių interesams.

Lygiavertė įslaptinta informacija – įslaptinta informacija, kurią parengė valstybės narės, trečiosios valstybės arba tarptautinės organizacijos, kuri pažymėta slaptumo žyma, lygiaverte vienai iš slaptumo žymų, naudojamų ESĮI, ir kurią Europos Parlamentui perdavė Taryba arba Komisija.

ESĮI administravimas – visi galimi veiksmai, kurie gali būti atliekami su ESĮI per visą jos gyvavimo ciklą. Tai apima ESĮI parengimą, apdorojimą, gabenimą, slaptumo žymos laipsnio sumažinimą, išslaptinimą ir sunaikinimą. RIS atžvilgiu tai taip pat apima ESĮI rinkimą, skelbimą, perdavimą ir saugojimą.

ESĮI tvarkymas – visi galimi veiksmai, kurie gali būti atliekami su ESĮI per visą jos gyvavimo ciklą. Tai apima ESĮI rengimą, registravimą, apdorojimą, gabenimą, slaptumo mažinimą, išslaptinimą ir sunaikinimą. Ryšių ir informacinių sistemų (RIS) atžvilgiu tai taip pat apima ESĮI rinkimą, skelbimą, perdavimą ir saugojimą.

ESĮI neteisėtas atskleidimas – visiškas ar dalinis ESĮI atskleidimas leidimo neturintiems asmenims ar subjektams (žr. 9 straipsnio 2 dalį);

EIVT darbuotojai – EIVT pareigūnai ir kiti tarnautojai, įskaitant valstybių narių diplomatinių tarnybų darbuotojus, kurie paskiriami laikinaisiais darbuotojais, taip pat komandiruoti nacionaliniai ekspertai.

EIVT patalpos – visos EIVT įstaigos, įskaitant pastatus, biurus, ka-

binetus ir kitas zonas, taip pat zonos, kuriose saugomos ryšių ir informacinės sistemos (įskaitant zonas, kuriose tvarkoma ES įslaptinta informacija (ESĮI)) ir kuriose EIVT vykdo nuolatinę ar laikiną veiklą.

EIVT saugumo interesai – darbuotojai, už kurių įdarbinimą atsakinga EIVT, EIVT patalpos, išlaikytiniai, fiziniai ištekliai, įskaitant ryšių ir informacines sistemas, informacija ir lankytojai.

F

Fizinis saugumas – fizinių ir techninių apsaugos priemonių taikymas siekiant užkirsti kelią leidimo neturintiems asmenims susipažinti su ESĮI.

G

Grėsmė

Grėsmė – galima nepageidaujamo incidento, dėl kurio gali būti padaryta žala organizacijai ar jos naudojamoms sistemoms, priežastis. Tokios grėsmės gali būti atsitiktinės arba tyčinės (piktybinės); jas apibūdina pavojingi elementai, galimi taikiniai ir puolimo būdai.

Grėsmė – galimas nepageidaujamas atvejis, dėl kurio gali būti padaryta žala organizacijai ar jos naudojamoms sistemoms; tokios grėsmės gali būti atsitiktinės arba tyčinės (piktybinės); jas apibūdina pavojingi elementai, galimi taikiniai ir puolimo būdai.

Grėsmė saugumui – bet koks įvykis arba veiksnys, galintis, kaip pagrįstai galima tikėtis, turėti neigiamos įtakos saugumui, jeigu nebus imtasi atsako ir jis nebus kontroliuojamas.

Didelė grėsmė saugumui – grėsmė saugumui, dėl kurios, kaip pagrįstai galima tikėtis, gali būti prarasta gyvybė, patirtas sunkus sužalojimas ar žala sveikatai, padaryta didelė turtinė žala, atskleista itin slapta informacija, sutrikdytos IT sistemos arba sužlugdyti svarbūs Komisijos

vykdomieji gebėjimai.

Tiesioginė grėsmė saugumui – grėsmė saugumui, kylanti, kai apie tai iš anksto nežinoma arba sužinoma likus labai mažai laiko.

I

Informacija – rašytinė ar žodinė informacija, kokia bebūtų jos laikmena ar autorius.

Informacijos saugumo užtikrinimas (ISU) ryšių ir informacinių sistemų srityje – užtikrinimas, kad tokiose sistemose tvarkoma informacija bus apsaugota ir kad, valdant teisėtiems naudotojams, jos veiks taip, kaip turi veikti, ir tada, kada turi veikti. Veiksmingas ISU užtikrina tinkamą konfidencialumo, vientisumo, prieinamumo, atsakomybės už veiksmus prisiėmimo ir autentiškumo lygį. ISU grindžiamas rizikos valdymo procesu.

Išlaikytiniai – darbuotojų, už kurių įdarbinimą Europos Sąjungos delegacijose atsakinga EIVT, šeimos nariai, kurie yra darbuotojų namų ūkio dalyviai, kaip pranešta priimančiosios valstybės užsienio reikalų ministerijai.

Išslaptinimas – bet kokios slaptumo žymos panaikinimas.

Į

Įslaptinta informacija – ES įslaptinta informacija ir lygiavertė įslaptinta informacija.

Įslaptintos informacijos administravimas – administracinių ESĮI kontrolės visą jos gyvavimo ciklą priemonių taikymas siekiant atgrasyti nuo tokios informacijos sąmoningo ar tikslingo atskleidimo arba praradimo, nustatyti tokius atvejus ir pašalinti jų padarinius. Tokios priemonės visų pirma yra susijusios su ESĮI rengimu, registravimu, kopijavimu, vertimu, gabenimu, tvarkymu, saugojimu ir naikinimu.

Įmonės patikimumą patvirtinantis pažymėjimas (ĮPPP) – NSI ar PSI administracinis patvirtinimas, kad saugumo požiūriu patalpose gali būti užtikrinta nurodyto slaptumo žymos lygio ESĮI tinkama apsauga ir kad buvo tinkamai patikrintas jose dirbančio personalo narių, kuriems reikia susipažinti su ESĮI, patikimumas bei jie buvo informuoti apie atitinkamus saugumo reikalavimus, būtinus norint susipažinti su ESĮI ir ją apsaugoti.

Įslaptinta sutartis – EIVT ir rangovo sudaryta prekių tiekimo, darbų vykdymo arba paslaugų teikimo sutartis, kurią vykdant reikia susipažinti su ESĮI ar ją rengti arba suteikiama galimybė su ja susipažinti ar ją rengti.

Įslaptinta subrangos sutartis – EIVT rangovo ir kito rangovo (t. y. subrangovo) sudaryta prekių tiekimo, darbų vykdymo arba paslaugų teikimo sutartis, kurią vykdant reikia susipažinti su ESĮI ar ją rengti arba suteikiama galimybė su ja susipažinti ar ją rengti.

Įgyvendinimo taisyklės – taisyklės arba saugumo pranešimai.

K

Konfidenciali informacija – įslaptinta informacija ir neįslaptinta kita konfidenciali informacija.

Kita konfidenciali informacija – bet kokia kita neįslaptinta konfidenciali informacija, įskaitant informaciją, kuriai taikomos duomenų apsaugos taisyklės arba kuriai taikoma tarnybinės paslapties prievolė, ir kuri parengta Europos Parlamente ar Europos Parlamentui perduota kitų institucijų, įstaigų, tarnybų ir agentūrų, įsteigtų pagal Sutartis arba jomis remiantis, ar valstybių narių.

Kita žyma – kitai konfidencialiai informacijai suteikiama žyma, pagal kurią atpažįstami iš anksto nustatyti konkretūs dokumento naudojimo nurodymai arba jame aptariama sritis. Šia žyma taip pat gali būti pažymėta įslaptinta informacija siekiant nustatyti papildomus jos naudojimo reikalavimus.

Kitos žymos panaikinimas – bet kokios kitos žymos panaikinimas.

Komisijos padalinys – Komisijos generalinis direktoratas arba tarnyba, arba Komisijos nario kabinetas.

Kriptografinė medžiaga – kriptografiniai algoritmai, techninės ir programinės kriptografinės įrangos moduliai, priemonės, apimančios vykdymo informaciją bei susijusius dokumentus ir raktų duomenis.

Krizinė situacija – bet kokios kilmės aplinkybė, įvykis, incidentas ar ekstremalioji situacija (arba jų seka ar derinys), keliantys didelę arba tiesioginę grėsmę saugumui Komisijoje.

L

Laipsnio sumažinimas – įslaptinimo laipsnio sumažinimas.

Leidimas – sprendimas suteikti asmeninę prieigą prie konkretaus laipsnio įslaptintos informacijos, kurį priima Parlamento pirmininkas, jei sprendimas susijęs su Europos Parlamento nariais, arba generalinis sekretorius, jei sprendimas susijęs su Europos Parlamento pareigūnais ir kitais Europos Parlamento darbuotojais, kurie dirba frakcijose, remdamasis teigiamais nacionalinės institucijos pagal nacionalinę teisę ir pagal I priedo 2 dalies nuostatas atlikto asmens patikimumo patikrinimo rezultatais.

Leidimas susipažinti su ESĮI – EIVT saugumo institucijos leidimas, kuris suteikiamas pagal šį sprendimą, po to, kai valstybės narės kompetentingos institucijos suteikia APP, ir kuriuo pažymima, kad atitinkamam asmeniui, nustačius, kad jis atitinka principą „būtina žinoti“, suteikiamas leidimas iki nurodytos datos susipažinti su atitinkamo lygio slaptumo žyma (CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio lygio slaptumo žyma) pažymėta ESĮI. Laikoma, kad asmens, kuriam taikoma ši apibrėžtis, patikimumas patikrintas.

Likutinė rizika – rizika, kuri lieka po to, kai buvo įgyvendintos saugumo priemonės, atsižvelgiant į tai, kad ne nuo visų grėsmių apsisaugo-

ma ir ne visi pažeidžiamumo aspektai gali būti pašalinti.

M

Medžiaga – dokumentas arba bet kokie pagaminti ar gaminami įrenginiai ar įranga.

Medžiaga – terpė, duomenų laikmena arba pagaminti ar gaminami įrenginiai ar įranga.

N

Naudojimo nurodymai – techniniai nurodymai Europos Parlamento tarnyboms dėl konfidencialios informacijos valdymo.

Neskelbtina neįslaptinta informacija – informacija arba medžiaga, kurią EIVT privalo apsaugoti dėl Sutartyse ir priimtuose jų įgyvendinimo aktuose nustatytų teisinių prievolių ir (arba) dėl jos neskelbtinumo. Neskelbtina neįslaptinta informacija apima (bet neapsiriboja) informaciją ar medžiagą, kuriai taikoma tarnybinės paslapties saugojimo prievolė, informaciją, kuri susijusi su interesais, saugomais Europos Parlamento ir Tarybos reglamento kartu su atitinkama Europos Sąjungos Teisingumo Teismo praktika, arba asmens duomenis, patenkančius į Reglamento (EB) Nr. 45/2001 taikymo sritį.

Nuodugni apsauga – saugumo priemonių, kurios grupuojamos į kelis apsaugos lygius, taikymas.

P

Paskirtoji saugumo institucija (PSI) – valstybės narės nacionalinei saugumo institucijai (NSI) atsakinga institucija, kuri atsako už pramonės ar kitų subjektų informavimą apie nacionalinę politiką visais pramoninio saugumo klausimais ir duoda nurodymus bei padeda ją įgyvendinti. PSI funkciją gali vykdyti NSI arba kita kompetentinga institucija.

Patikimumo tyrimas – tyrimo procedūros, kurias, vadovaudamasi valstybėje narėje galiojančiais įstatymais ir kitais teisės aktais, atlieka kompetentinga institucija, siekdama gauti užtikrinimą, kad nėra jokios nepalankios informacijos, kuri neleistų asmeniui išduoti nacionalinio arba ES asmens patikimumo pažymėjimo, suteikiančio galimybę susipažinti su tam tikro lygio ESĮI (CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio lygio slaptumo žyma pažymėta informacija).

Patalpos – bet koks nekilnojamasis ar jam prilyginamas Komisijos turtas ir nuosavybė.

Pavojų kontrolė – bet kokia saugumo priemonė, kuria pagrįstai galima tikėtis veiksmingai kontroliuoti pavojų saugumui: užkirsti jam kelią, jį mažinti, jo išvengti arba jį perkelti.

Pavojaus prevencija – saugumo priemonės, kuriomis pagrįstai galima tikėtis sumažinti, atitolinti arba pašalinti pavojų saugumui.

Pavojus saugumui – įvykio keliamos grėsmės lygio, pažeidžiamumo lygio ir galimo poveikio derinys.

Pažeidimas – šiame sprendime nustatytoms saugumo taisyklėms ir (arba) saugumo strategijoms ar gairėms, kuriose nustatytos šių taisyklių įgyvendinimo priemonės, priešingas asmens veiksmas arba neveikimas;

Pažeidžiamumas – bet kokio pobūdžio trūkumas, kuriuo gali būti naudojamasi vienos ar daugiau grėsmių atveju. Pažeidžiamumas gali atsirasti dėl neveikimo arba gali būti susijęs su negriežta, neišsamia arba nenuoseklia kontrole ir gali būti techninio, procedūrinio, fizinio, organizacinio ar veiklos pobūdžio.

Personalo patikimumas – priemonių taikymas, siekiant užtikrinti, kad galimybė susipažinti su ESĮI būtų suteikta tik asmenims:

- kuriems „būtina žinoti“;
- kurių patikimumas patikrintas atitinkamu lygiu ir suteikta teisė prieiti prie informacijos, pažymėtos CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio lygio saugumo žyma, arba

kiti tinkami leidimai pagal nacionalinius įstatymus ir kitus teisės aktus;

– kurie yra informuoti apie savo pareigas.

Pramonės arba kitas subjektas – subjektas, tiekiantis prekes, vykdantis darbus arba teikiantis paslaugas; tai gali būti pramonės, prekybos, paslaugų, mokslo, mokslinių tyrimų, švietimo ar vystymo subjektas arba savarankiškai dirbantis asmuo.

Pramoninis saugumas – priemonių, kurias rangovai arba subrangovai taiko derybų dėl sutarčių sudarymo metu ir visą įslaptintų sutarčių gyvavimo ciklą, siekdami užtikrinti ESĮI apsaugą, taikymas. Paprastai tokiose sutartyse nenumatoma galimybė susipažinti su slaptumo žyma TRES SECRET UE/EU TOP SECRET pažymėta informacija.

Principas „būtina žinoti“ – asmens būtinybė susipažinti su konfidencialia informacija, kad jis galėtų atlikti oficialias pareigas ar užduotį;

Programos / projekto saugumo instrukcijos – (PRSI) saugumo procedūrų, kurios yra taikomos konkrečiai programai / projektui siekiant standartizuoti saugumo procedūras, sąrašas. Jos gali būti tikslinamos įgyvendinant programą / projektą.

R

Rangovas – fizinis arba juridinis asmuo, turintis teisnumą ir veiksnumą sudaryti sutartis.

Registravimas – procedūrų, kuriomis užregistruojamas informacijos gyvavimo ciklas, įskaitant jo platinimą ir sunaikinimą, taikymas.

Rengėjas – konfidencialios informacijos tinkamai įgaliotas autorius.

Rengėjas – ES institucija, agentūra ar įstaiga, valstybė narė, trečioji valstybė ar tarptautinė organizacija, kurios atsakomybe įslaptinta informacija buvo parengta ir (arba) pateikta naudoti ES struktūrose.

RIS gyvavimo ciklas – visa RIS egzistavimo trukmė, įskaitant inicijavimą, koncepciją, planavimą, reikalavimų analizę, projektavimą, sukūrimą, bandymą, įdiegimą, veikimą ir priežiūrą bei naudojimo nutraukimą.

Rizika

Rizika – galimybė, kad tam tikros grėsmės atveju bus pasinaudota organizacijos ar sistemų vidiniu ir išoriniu pažeidžiamumu ir taip bus padaryta žala organizacijai ir jos materialiajam ar nematerialiajam turtui. Ji įvertinama atsižvelgiant į kylančios grėsmės tikimybę ir į jos poveikį.

Rizikos pripažinimas – sprendimas atlikus rizikos tvarkymą pripažinti, kad vis dar yra likutinė rizika.

Rizikos įvertinimas – grėsmių ir pažeidžiamų sričių nustatymas bei susijusios rizikos analizės, t. y. galimumo ir poveikio analizės, atlikimas.

Informavimas apie riziką – RIS vartotojų bendruomenės informuotumo apie riziką didinimas, patvirtinimo institucijų informavimas apie tokią riziką ir pranešimų vykdančiosioms institucijoms teikimas.

Saugumo rizikos valdymo procesas – visas nebūtinai galinčių įvykti atvejų, kurie gali paveikti organizacijos arba jos naudojamų sistemų saugumą, nustatymo, kontrolės ir mažinimo procesas. Jis apima visą su rizika susijusią veiklą, įskaitant jos įvertinimą, valdymą, pripažinimą ir informavimą apie ją.

Rizikos valdymas – rizikos silpninimas, šalinimas, mažinimas (taikant tinkamas technines, fizines, organizacines arba procedūrines priemones), perkėlimas arba stebėjimas.

Ryšių ir informacinė sistema (RIS) – sistema, sudaranti sąlygas tvarkyti informaciją elektroniniu būdu. Ryšių ir informacinė sistema apima visas sistemos dalis, kurių reikia jos veikimui užtikrinti, įskaitant infrastruktūrą, organizavimą, personalą ir informacijos išteklius (šaltinius).

S

Saugios eksploatacijos taisyklės (SecOPs) – saugumo politikos įgyvendinimo, kurį ketinama patvirtinti, eksploatacijos taisyklių, kurių reikia laikytis, ir personalo atsakomybės aprašas.

Saugumo aspektų paaiškinimas (SAP) – specialių sutartinių sąlygų rinkinys, kurį parengia perkančioji institucija ir kuris yra įslaptintos sutarties, pagal kurią gali būti susipažįstama su ESĮI arba tokia informacija gali būti rengiama, sudėtinė dalis – jame nurodomi saugumo reikalavimai arba sutarties dalys, kurių saugumą būtina užtikrinti.

Saugumas Komisijoje – asmenų, turto ir informacijos saugumas Komisijoje, visų pirma fizinė asmenų ir turto neliečiamybė, informacijos ir ryšių ir informacinių sistemų vientisumas, konfidencialumas ir prieinamumas, taip pat nevaržomas Komisijos veiklos vykdymas.

Saugumo pranešimai – techninės įgyvendinimo priemonės, nustatytos II priede.

Saugumo priemonė – bet kokia priemonė, kurios imamasi vadovaujantis šiuo sprendimu siekiant kontroliuoti pavojus saugumui.

Saugumo rizikos valdymo procesas – visas nebūtinai galinčių įvykti įvykių, kurie gali paveikti organizacijos arba jos naudojamų sistemų saugumą, nustatymo, kontrolės ir padarinių mažinimo procesas. Jis apima visą su rizika susijusią veiklą, įskaitant jos įvertinimą, valdymą, pripažinimą ir informavimą apie ją.

Sąjungos delegacija – delegacijos į trečiąsias šalis ir tarptautines organizacijas.

Sistemos saugumo reikmių aktas (SSRA) – saugumo principų, kurių reikia laikytis, ir išsamių saugumo reikalavimų, kuriuos reikia įgyvendinti, rinkinys, kuris yra RIS sertifikavimo ir akreditavimo pagrindas.

Slaptumo mažinimas – aukštesnio slaptumo lygio keitimas žemesniu slaptumo lygiu.

Slaptumo žymos laipsnio sumažinimas – slaptumo žymos lygio sumažinimas.

Slaptumo žymų vadovas (SŽV) – dokumentas, kuriame aprašomi programos arba sutarties įslaptintos dalys, nurodant taikomus slaptumo žymų laipsnius. SŽV gali būti papildomas programos arba sutarties vykdymo laikotarpiu, o informacijos dalims gali būti suteiktos naujos slaptumo žymos arba jų slaptumo žymos laipsnis gali būti sumažintas; tais atvejais, kai yra parengtas SŽV, jis yra SAP dalis.

Š

Šifravimo priemonės – šifravimo algoritmai, šifravimo techninės ir programinės įrangos moduliai, priemonės, apimančios vykdymo informaciją bei susijusius dokumentus ir raktų duomenis.

T

TEMPEST – elektromagnetinio spinduliavimo, dėl kurio neteisėtai atskleidžiama informacija, tikrinimas, tyrimas bei kontrolė ir jo šalinimo priemonės.

Turtas – visas kilnojamasis ir nekilnojamasis Komisijos turtas ir nuosavybė.

Turėtojas – tinkamą leidimą turintis asmuo, kuris atitinka principą „būtina žinoti“ ir turi ESĮI dalį bei yra atitinkamai atsakingas už jos apsaugą.

U

Už saugumą atsakingas Komisijos narys – Komisijos narys, kurio atsakomybės sričiai priklauso Žmogiškųjų išteklių ir saugumo generalinis direktoratas.

GLOSSARY OF TERMS AND DEFINITIONS

A

Accreditation means the process leading to a formal statement by the Security Accreditation Authority (SAA) that a system is approved to operate with a defined level of classification, in a particular security mode in its operational environment and at an acceptable level of risk, based on the premise that an approved set of technical, physical, organisational and procedural security measures have been implemented.

Asset means anything that is of value to an organisation, its business operations and their continuity, including information resources that support the organisation's mission.

Assets means all movable and immovable property and possessions of the Commission.

Authorisation to access EUCI means an authorisation by the EEAS Security Authority, which is taken in accordance with this Decision after a PSC has been issued by the competent authorities of a Member State, and which certifies that an individual may, provided his 'need-to-know' has been determined, be granted access to EUCI up to a specified level (CONFIDENTIEL UE/EU CONFIDENTIAL or above) until a specified date.

Authorisation means a decision adopted by the President, if it concerns Members of the European Parliament, or by the Secretary-General, if it concerns officials of the European Parliament and other European Parliament employees working for political groups, to grant an individual access to classified information up to a specific level, on the basis of a positive result of a security screening (vetting) carried out by a national authority under national law and pursuant to the provisions.

B

Breach is an act or omission by an individual which is contrary to the security rules and/or to the security policies or guidelines setting out any measures necessary for its implementation.

C

CIS life-cycle means the entire duration of existence of a CIS, which includes initiation, conception, planning, requirements analysis, design, development, testing, implementation, operation, maintenance and decommissioning.

Classified contract means a contract entered into by the EEAS with a contractor for the supply of goods, execution of works or provision of services, the performance of which requires or involves access to or the creation of EUCI.

Classified subcontract means a contract entered into by a contractor of the EEAS with another contractor (i.e. the subcontractor) for the supply of goods, execution of works or provision of services, the performance of which requires or involves access to or the creation of EUCI.

Classified information means 'EU classified information' and 'equivalent classified information'.

Commission department means any Commission Directorate-General or service, or any Cabinet of a Member of the Commission.

Communication and Information System or CIS means any system enabling the handling of information in electronic form, including all assets required for its operation, as well as the infrastructure, organisation, personnel and information resources.

Compromise of EUCI means the total or partial disclosure of EUCI to unauthorised persons or entities.

Confidential information means 'classified information', and non-classified 'other confidential information'.

Contractor means an individual or legal entity possessing the legal capacity to undertake contracts.

Control of risks shall mean any security measure that can reasonably be expected to effectively control a risk to security by its prevention, mitigation, avoidance or transfer.

Crisis situation means a circumstance, event, incident or emergency (or a succession or combination thereof) posing a major or an immediate threat to security in the Commission regardless of its origin.

Cryptographic (Crypto) material (products) means cryptographic algorithms, cryptographic hardware and software modules, and products including implementation details and associated documentation and keying material.

CSDP operation means a military or civilian crisis management operation.

D

Data means information in a form that allows it to be communicated, recorded or processed.

Declassification means the removal of any security classification.

Defence in depth means the application of a range of security measures organised as multiple layers of defence.

Document means any recorded information, regardless of its physical form or characteristics.

Dependants means the members of the family of the staff member placed under the responsibility of the EEAS in Union Delegations forming part of their respective household as notified to the Ministry for

Foreign Affairs of the receiving State.

Designated Security Authority (DSA) means an authority responsible to the National Security Authority (NSA) of a Member State which is responsible for communicating to industrial or other entities national policy on all matters of industrial security and for providing direction and assistance in its implementation. The function of DSA may be carried out by the NSA or by any other competent authority.

Downgrading means a reduction in the level of security classification.

E

EEAS premises means all EEAS establishments, including buildings, offices, rooms and other areas, as well as areas housing communication and information systems (including those handling EUCI), where the EEAS conducts permanent or temporary activities.

EEAS security interests means the Staff placed under the responsibility of the EEAS, EEAS premises, dependants, physical assets, including communication and information systems, information, and visitors.

EU classified information (EUCI) means any information or material the unauthorized disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States, designated by an EU security classification.

F

Facility Security Clearance (FSC) means an administrative determination by an NSA or DSA that, from the security viewpoint, a facility can afford an adequate level of protection to EUCI of a specified security classification level and its personnel who require access to EUCI have been appropriately security cleared and briefed on the relevant security requirements necessary to access and protect EUCI.

H

Handling instructions means technical instructions issued to the European Parliament's services concerning the management of confidential information.

Handling of EUCI means all possible actions to which EUCI may be subject throughout its life-cycle. It comprises its creation, registration, processing, carriage, downgrading, declassification and destruction. In relation to Communication and Information Systems (CIS) it also comprises its collection, display, transmission and storage.

Holder means a duly authorised individual with an established need-to-know who is in possession of an item of EUCI and is accordingly responsible for protecting it.

I

Implementing rules means any set of rules or security notices adopted in accordance with Commission Decision.

Industrial or other entity means an entity involved in supplying goods, executing works or providing services; this may be an industrial, commercial, service, scientific, research, educational or development entity or a self-employed individual.

Industrial security is the application of measures to ensure the protection of EUCI by contractors or subcontractors in pre-contract negotiations and throughout the life-cycle of classified contracts.

Information

Information means any written or oral information, whatever the medium and whoever the author may be.

Confidential information means 'classified information', and non-classified 'other confidential information'.

Classified information means ‘EU classified information’ and ‘equivalent classified information’.

EU classified information (EUCI) means any information or material designated by a EU security classification, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States.

EU classified information (EUCI) means any information and material, classified as ‘TRÈS SECRET UE/EU TOP SECRET’, ‘SECRET UE/EU SECRET’, ‘CONFIDENTIEL UE/EU CONFIDENTIAL’ or ‘RESTREINT UE/EU RESTRICTED’, unauthorised disclosure of which could cause varying degrees of prejudice to Union interests or to those of one or more of its Member States, whether or not such information originates within the institutions, bodies, offices or agencies established by virtue or on the basis of the Treaties. In this regard, information and material classified at the level:

‘TRÈS SECRET UE/EU TOP SECRET’ is information and material the unauthorised disclosure of which could cause exceptionally grave prejudice to the essential interests of the Union or of one or more of the Member States;

‘SECRET UE/EU SECRET’ is information and material the unauthorised disclosure of which could seriously harm the essential interests of the Union or of one or more of the Member States;

‘CONFIDENTIEL UE/EU CONFIDENTIAL’ is information and material the unauthorised disclosure of which could harm the essential interests of the Union or of one or more of the Member States;

‘RESTREINT UE/EU RESTRICTED’ is information and material the unauthorised disclosure of which could be disadvantageous to the interests of the Union or of one or more of the Member States.

Equivalent classified information means classified information issued by Member States, third States or international organisations which bears a security classification marking equivalent to one of the security classification markings used for EUCI and which has been forwarded to the European Parliament by the Council or the Commission.

Other confidential information means any other non-classified confidential information, including information covered by data protection rules or by the obligation of professional secrecy, created in the European Parliament or forwarded to the European Parliament by other institutions, bodies, offices and agencies established by virtue or on the basis of the Treaties or by Member States.

Sensitive non-classified information means information or material that the EEAS must protect because of legal obligations laid down in the Treaties or in acts adopted in implementation thereof, and/or because of its sensitivity. Sensitive non-classified information includes, but is not limited to, information or material covered by the obligation of professional secrecy.

Information assurance in the field of communication and information systems is the confidence that such systems will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users. Effective IA shall ensure appropriate levels of confidentiality, integrity, availability, non-repudiation and authenticity. IA shall be based on a risk management process.

Interconnection means, for the purposes of this Decision, the direct connection of two or more IT systems for the purpose of sharing data and other information resources (e.g. communication) in a unidirectional or multidirectional way.

M

Management of classified information is the application of administrative measures for controlling EUCI throughout its life-cycle to supplement the measures provided for in Articles 5, 6 and 8 and thereby help deter, detect and recover from deliberate or accidental compromise or loss of such information. Such measures relate in particular to the creation, registration, copying, translation, carriage, handling, storage and destruction of EUCI.

Marking means a sign affixed to 'other confidential information' intended to identify predefined specific instructions about its handling or the field covered by a given document. It may also be affixed to classified information, in order to impose additional requirements for its handling.

Material means any document or item of machinery or equipment, either manufactured or in the process of manufacture.

Material means any medium, data carrier or item of machinery or equipment, either manufactured or in the process of manufacture.

Member of the Commission responsible for security means a Member of the Commission under whose authority the Directorate-General for Human Resources and Security falls.

N

Need to know means the need of a person to have access to confidential information in order to be able to perform an official function or a task.

O

Originator means the EU institution, agency or body, Member State, third state or international organisation under whose authority classified information has been created and/or introduced into the EU's structures.

P

Personnel security is the application of measures to ensure that access to EUCI is granted only to individuals who have:

- a need-to-know;

- for access to CONFIDENTIEL UE/EU CONFIDENTIAL information or above, been security cleared to the relevant level, or are otherwise duly authorised by virtue of their functions in accordance with

national laws and regulations; and

- been briefed on their responsibilities.

Personnel Security Clearance (PSC) for access to EUCI means a statement by a competent authority of a Member State which is made following completion of a security investigation conducted by the competent authorities of a Member State and which certifies that an individual may, provided his 'need-to-know' has been determined, be granted access to EUCI up to a specified level (CONFIDENTIEL UE/ EU CONFIDENTIAL or above) until a specified date; the individual thus described is said to be 'security cleared'.

Personnel Security Clearance Certificate (PSCC) means a certificate issued by a competent authority establishing that an individual is security cleared and holds a valid PSC or Authorisation from the Head of the Directorate responsible for security for access to EUCI, and which shows the level of EUCI to which that individual may be granted access (CONFIDENTIEL UE/EU CONFIDENTIAL or above), the date of validity of the relevant PSC and the date of expiry of the certificate itself.

Physical security is the application of physical and technical protective measures to deter unauthorised access to EUCI.

Premises means any immovable or assimilated property and possessions of the Commission.

Prevention of risk shall mean security measures that can reasonably be expected to impede, delay or stop a risk to security.

Programme/Project Security Instruction (PSI) means a list of security procedures which are applied to a specific programme/project in order to standardise security procedures. It may be revised throughout the programme/project.

R

Registration means the application of procedures that record the life-cycle of information, including its dissemination and destruction.

Risk

Risk means the potential that a given threat will exploit internal and external vulnerabilities of an organisation or of any of the systems it uses and thereby cause harm to the organisation and to its tangible or intangible assets. It is measured as a combination of the likelihood of threats occurring and their impact.

Risk acceptance is the decision to agree to the further existence of a residual risk after risk treatment.

Risk assessment consists of identifying threats and vulnerabilities and conducting the related risk analysis, i.e. the analysis of probability and impact.

Risk to security means the combination of the threat level, the level of vulnerability and the possible impact of an event.

Risk communication consists of developing awareness of risks among CIS user communities, informing approval authorities such risks and reporting them to operating authorities.

(Security) Risk management process means the entire process of identifying, controlling and minimising uncertain events that may affect the security of an organisation or of any of the systems it uses. It covers the entirety of risk-related activities, including assessment, treatment, acceptance and communication.

Risk treatment consists of mitigating, removing, reducing (through an appropriate combination of technical, physical, organisational or procedural measures), transferring or monitoring the risk.

Residual risk means the risk which remains after security measures have been implemented, given that not all threats are countered and not

all vulnerabilities can be eliminated.

Prevention of risk shall mean security measures that can reasonably be expected to impede, delay or stop a risk to security.

S

Security

Security Aspects Letter (SAL) means a set of special contractual conditions issued by the contracting authority which forms an integral part of any classified contract involving access to or the creation of EUCI that identifies the security requirements or those elements of the contract requiring security protection.

Security Classification Guide (SCG) means a document which describes the elements of a programme or contract which are classified, specifying the applicable security classification levels. The SCG may be expanded throughout the life of the programme or contract and the elements of information may be re-classified or downgraded; where an SCG exists it shall be part of the SAL.

Security investigation means the investigative procedures conducted by the competent authority of a Member State in accordance with its national laws and regulations in order to obtain an assurance that nothing adverse is known which would prevent an individual from being granted a national or EU PSC for access to EUCI up to a specified level (CONFIDENTIEL UE/EU CONFIDENTIAL or above).

Security in the Commission means the security of persons, assets and information in the Commission, and in particular the physical integrity of persons and assets, the integrity, confidentiality and availability of information and communication and information systems, as well as the unobstructed functioning of Commission operations.

Security measure means any measure taken in accordance with this Decision for purposes of controlling risks to security.

Security notices means the implementing measures.

Security Operating Procedures (SecOPs) means a description of the security policy implementation to be adopted, of the operating procedures to be followed and of the personnel responsibilities.

Security risk management process means the entire process of identifying, controlling and minimising uncertain events that may affect the security of an organisation or of any of the systems it uses. It covers the entirety of risk-related activities, including assessment, treatment, acceptance and communication.

Sensitive non-classified information means information or material that the EEAS must protect because of legal obligations laid down in the Treaties or in acts adopted in implementation thereof, and/or because of its sensitivity. Sensitive non-classified information includes, but is not limited to, information or material covered by the obligation of professional secrecy.

Specific Security Requirement Statement (SSRS) means a binding set of security principles to be observed and of detailed security requirements to be implemented, underlying the process of certification and accreditation of CIS.

Staff

EEAS staff means EEAS officials and other servants, including personnel from the diplomatic services of the Member States appointed as temporary agents, and seconded national experts.

Staff placed under the responsibility of the EEAS means the EEAS staff at Headquarters and in Union Delegations and all other staff in Union Delegations, regardless of their administrative status or origin, as well as, in the context of this decision, the High Representative and, as appropriate, other staff resident in EEAS Headquarters premises.

Staff Regulations means the Staff Regulations of officials of the European Union and the Conditions of Employment of other servants of the European Union.

T

Threat

Threat means a potential cause of an unwanted incident which may result in harm to an organisation or any of the systems it uses; such threats may be accidental or deliberate (malicious) and are characterised by threatening elements, potential targets and attack methods.

Threat to security means an event or agent that can reasonably be expected to adversely affect security if not responded to and controlled.

Immediate threat to security means a threat to security which occurs with no or with extremely short advance warning.

Major threat to security means a threat to security that can reasonably be expected to lead to loss of life, serious injury or harm, significant damage to property, compromise of highly sensitive information, disruption of IT systems or of essential operational capacities of the Commission.

TEMPEST means the investigation, study and control of compromising electromagnetic emanations and the measures to suppress them.

U

Union Delegation means delegations to third countries and international organisations.

Unmarking means the removal of any marking.

V

Vulnerability means a weakness of any nature that can reasonably be expected to adversely affect security in the Commission, if exploited by one or more threats.

Vulnerability means a weakness of any nature that can be exploited by one or more threats. Vulnerability may be an omission or it may relate to a weakness in controls in terms of their strength, completeness or consistency and may be of a technical, procedural, physical, organisational or operational nature.

JUNGTINIŲ TAUTŲ IR EUROPOS SĄJUNGOS INFORMACIJOS APSAUGA

NORMINIŲ TEISĖS AKTŲ RINKINYS

THE PROTECTION OF THE UNITED NATIONS AND THE EUROPEAN UNION INFORMATION

LEGISLATIVE INSTRUMENTS REPORT

Sudarytojas Andrius Tekorius
Atsakingasis redaktorius dr. Vladas Tumalavičius
Korektūrą lietuvių kalba atliko Rūta Matukonienė
Korektūrą anglų kalba atliko Dovilė Radovičiūtė
Viršelio dizainerė Laima Adlytė
Maketuotoja Jolanta Girnytė

Išleido Generolo Jono Žemaičio Lietuvos karo akademija,
Šilo g. 5A, LT-10322 Vilnius