KOMISIJAS LĒMUMS (ES, Euratom) 2015/444

(2015. gada 13. marts)

par drošības noteikumiem ES klasificētas informācijas aizsardzībai

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību un jo īpaši tā 249. pantu,

ņemot vērā Eiropas Atomenerģijas kopienas dibināšanas līgumu un jo īpaši tā 106. pantu,

ņemot vērā 7. protokolu Par privilēģijām un imunitāti Eiropas Savienībā, kas pievienots Līgumiem, un jo īpaši tā 18. pantu,

tā kā:

(1) Komisijas drošības noteikumus par Eiropas Savienības klasificētas informācijas aizsardzību (ESKI) ir jāpārskata un jāatjaunina, ņemot vērā institucionālos, organizatoriskos, operatīvos un tehnoloģiskos jauninājumus.

(2) Eiropas Komisija kopā ar Beļģijas, Luksemburgas un Itālijas valdībām piedalās vairākos ar drošības jautājumiem saistītos pasākumos tās struktūru galvenajās atrašanās vietās ([1]).

(3) Komisija, Padome un Eiropas Ārējās darbības dienests ir apņēmības pilni piemērot līdzvērtīgus drošības standartus attiecībā uz ESKI aizsardzību.

(4) Ir svarīgi attiecīgā gadījumā sasaistīt Eiropas Parlamentu un citas Savienības iestādes, aģentūras, struktūras un birojus ar klasificētas informācijas aizsardzības principiem, noteikumiem un standartiem, kuri ir nepieciešami, lai aizsargātu Savienības un tās dalībvalstu intereses.

(5) Risku ES klasificētajai informācijai pārvalda kā procesu. Šā procesa mērķis ir noteikt zināmos riskus drošībai, definēt drošības pasākumus, kuru mērķis ir mazināt šādus riskus līdz pieņemamam līmenim atbilstīgi šajā lēmumā izklāstītajiem pamatprincipiem un minimuma standartiem, un piemērot šos pasākumus saskaņā ar padziļinātas aizsardzības koncepciju. Šādu pasākumu efektivitāti nepārtraukti izvērtē.

(6) Komisijā fiziskā drošība, kuras mērķis ir klasificētas informācijas aizsardzība, ietver fizisku un tehnisku aizsardzības pasākumu piemērošanu, kuru mērķis ir nepieļaut neatļautu piekļuvi ESKI.

(7) ESKI pārvaldība ir administratīvu pasākumu piemērošana ar mērķi kontrolēt ESKI visā tās aprites cikla laikā, lai papildinātu šā lēmuma 2., 3. un 5. nodaļā minētos pasākumus un tādējādi palīdzētu atturēt no tīša vai netīša šādas informācijas apdraudējuma vai tās zaudējuma, atklāt šādu apdraudējumu vai zaudējumu un atgūties apdraudējuma vai zaudējuma gadījumā. Šādi pasākumi jo īpaši ir saistīti ar ESKI izveidi, glabāšanu, reģistrāciju, kopēšanu, tulkošanu, klasifikācijas līmeņa pazemināšanu, deklasifikāciju, pārvietošanu un iznīcināšanu, un tie papildina vispārīgos noteikumus par dokumentu pārvaldību Komisijā (Lēmumi 2002/47/EK ([2]), EOTK, Euratom un 2004/563/EK, Euratom ([3])).

([1]) Sk. 2004. gada 31. decembra "*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. gada 20. janvāra "*Accord de sécurité signé entre la Commission et le Gouvernement luxembourgeois*" un 1959. gada 22. jūlija "*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*".

([2]) Komisijas 2002. gada 23. janvāra Lēmums 2002/47/EK, EOTK, Euratom, ar ko groza Komisijas reglamentu (OV L 21, 24.1.2002., 23. lpp.).

([3]) Komisijas 2004. gada 7. jūlija Lēmums 2004/563/EK, Euratom par grozījumiem tās reglamentā (OV L 251, 27.7.2004., 9. lpp.).

(8) Šā lēmuma noteikumi neskar:

a) Regulu (Euratom) Nr. 3 ([1]);

b) Eiropas Parlamenta un Padomes Regulu (EK) Nr. 1049/2001 ([2]);

c) Eiropas Parlamenta un Padomes Regulu (EK) Nr. 45/2001 ([3]);

d) Padomes Regulu (EK, Euratom) Nr. 354/83 ([4]),

IR PIEŅĒMUSI ŠO LĒMUMU.

1. NODAĻA

PAMATPRINCIPI UN MINIMUMA STANDARTI

1. pants

Definīcijas

Šajā lēmumā piemēro šādas definīcijas:

1) "Komisijas dienests" ir Komisijas ģenerāldirektorāts vai dienests, vai Komisijas locekļa kabinets;

2) "kriptogrāfijas materiāls" ir kriptogrāfijas algoritmi, kriptogrāfijas aparatūras un programmatūras moduļi un produkti, tostarp īstenošanas informācija un ar to saistītā dokumentācija un atslēgu materiāls;

3) "deklasifikācija" ir visas drošības klasifikācijas noņemšana;

4) "padziļināta aizsardzība" ir dažādu drošības pasākumu piemērošana, izveidojot daudzslāņu aizsardzību;

5) "dokuments" ir jebkura fiksēta informācija neatkarīgi no tās fiziskā veidola vai iezīmēm;

6) "klasifikācijas līmeņa pazemināšana" ir zemāka drošības klasifikācija līmeņa piešķiršana;

7) "rīkošanās" ar ESKI ir visu veidu darbības, ko ar ESKI veic visā tās aprites cikla laikā. Tajā ietilpst izveide, reģistrācija, apstrāde, pārvietošana, klasifikācijas līmeņa pazemināšana, deklasifikācija un iznīcināšana. Saistībā ar komunikācijas un informācijas sistēmām (KIS) tajā ietilpst arī vākšana, uzrādīšana, pārsūtīšana un glabāšana;

8) "turētājs" ir pienācīgi pilnvarota persona, kurai ir pierādīta vajadzība pēc informācijas, kuras rīcībā ir ESKI un kura tādējādi ir atbildīga par tās aizsardzību;

9) "īstenošanas noteikumi" ir noteikumi vai drošības paziņojumi, kas pieņemti saskaņā ar 5. nodaļu Komisijas Lēmumā (ES, Euratom) 2015/443 ([5]);

10) "materiāli" ir jebkurš medijs, datu nesējs vai iekārtas vai ierīces daļa, kas jau ir izgatavota vai vēl tiek izgatavota;

11) "autors" ir Savienības iestāde, aģentūra vai struktūra, dalībvalsts, trešā valsts vai starptautiska organizācija, kuras pakļautībā klasificēta informācija ir izveidota un/vai nodota Savienības struktūrām;

12) "telpas" ir visa veida nekustamā vai tai pielīdzināma manta, kas atrodas Komisijas īpašumā vai turējumā;

([1]) 1958. gada 31. jūlija Regula (Euratom) Nr. 3 par Eiropas Atomenerģijas kopienas dibināšanas līguma 24. panta piemērošanu (OV 17, 6.10.1958., 406/58. lpp.).
([2]) Eiropas Parlamenta un Padomes 2001. gada 30. maija Regula (EK) Nr. 1049/2001 par publisku piekļuvi Eiropas Parlamenta, Padomes un Komisijas dokumentiem (OV L 145, 31.5.2001., 43. lpp.).
([3]) Eiropas Parlamenta un Padomes 2000. gada 18. decembra Regula (EK) Nr. 45/2001 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Kopienas iestādēs un struktūrās un par šādu datu brīvu apriti (OV L 8, 12.1.2001., 1. lpp.).
([4]) Padomes 1983. gada 1. februāra Regula (EEK, Euratom) Nr. 354/83 par Eiropas Ekonomikas kopienas un Eiropas Atomenerģijas kopienas vēsturisko arhīva materiālu nodošanu atklātībai (OV L 43, 15.2.1983., 1. lpp.).
([5]) Komisijas 2015. gada 13. marta Lēmums (ES, Euratom) 2015/443 par drošību Komisijā (sk. šā *Oficiālā Vēstneša* 41. lpp.).

13) "drošības riska pārvaldības process" ir viss process, kurā ietilpst tādu neparedzētu notikumu apzināšana, kontrole un ietekmes mazināšana, kuri var ietekmēt drošību organizācijā vai kādā no sistēmām, ko tā izmanto. Tas attiecas uz visām darbībām, kas saistītas ar risku, tostarp tā izvērtēšanu, novēršanu, uzņemšanos un izziņošanu;

14) "Civildienesta noteikumi" ir Eiropas Savienības Civildienesta noteikumi un Eiropas Savienības pārējo darbinieku nodarbināšanas kārtība, kas noteikta Padomes Regulā (EEK, Euratom, EOTK) Nr. 259/68 ([1]);

15) "draudi" ir nevēlama incidenta iespējams cēlonis, kas var kaitēt organizācijai vai jebkurai sistēmai, ko tā izmanto; šādiem draudiem var būt gadījuma raksturs, vai tie var būt apzināti (ļaunprātīgi), un tos raksturo draudēšanas elementi, iespējamie mērķi un uzbrukuma metodes;

16) "vājā vieta" ir jebkāda veida nepilnība, ko varētu izmantot vienā vai vairākos draudu gadījumos. Vājā vieta var būt kāda posma iztrūkums vai var būt saistīta ar nepilnību kontrolē attiecībā uz tās stiprumu, pilnīgumu vai konsekvenci, un tai var būt tehnisks, procedurāls, fizisks, organizatorisks vai ar darbību saistīts raksturs.

2. pants

Priekšmets un piemērošanas joma

1. Šajā lēmumā noteikti ESKI aizsardzības pamatprincipi un minimuma drošības standarti.

2. Šo lēmumu piemēro visiem Komisijas dienestiem un visās Komisijas telpās.

3. Neatkarīgi no īpašām norādēm, kas attiecas uz konkrētām darbinieku grupām, šo lēmumu piemēro Komisijas locekļiem, Komisijas darbiniekiem, kuriem ir piemērojami Civildienesta noteikumi un Eiropas Kopienu pārējo darbinieku nodarbināšanas kārtība, darbam Komisijā norīkotajiem valsts ekspertiem (NVE), pakalpojumu sniedzējiem un viņu darbiniekiem, stažieriem un ikvienai personai, kura var piekļūt Komisijas ēkām vai citiem aktīviem vai informācijai, kas ir Komisijas rīcībā.

4. Šā lēmuma noteikumi neskar Lēmumu 2002/47/EK, EOTK, Euratom un Lēmumu 2004/563/EK, Euratom.

3. pants

ESKI definīcija, drošības klasifikācija un marķējums

1. "Eiropas Savienības klasificēta informācija" (ESKI) ir jebkura informācija vai materiāli, kuriem piemērota ES drošības klasifikācija un kuru neatļauta izpaušana var izraisīt dažāda līmeņa kaitējumu Eiropas Savienības vai vienas vai vairāku tās dalībvalstu interesēm.

2. ESKI klasificē kādā no šādiem līmeņiem:

a) *TRES SECRET UE/EU TOP SECRET*: informācija un materiāli, kuru neatļauta izpaušana var radīt ārkārtīgi smagu kaitējumu būtiskām Eiropas Savienības vai vienas vai vairāku dalībvalstu interesēm;

b) *SECRET UE/EU SECRET*: informācija un materiāli, kuru neatļauta izpaušana var radīt nopietnu kaitējumu būtiskām Eiropas Savienības vai vienas vai vairāku dalībvalstu interesēm;

c) *CONFIDENTIEL UE/EU CONFIDENTIAL*: informācija un materiāli, kuru neatļauta izpaušana var radīt kaitējumu būtiskām Eiropas Savienības vai vienas vai vairāku dalībvalstu interesēm;

d) *RESTREINT UE/EU RESTRICTED*: informācija un materiāli, kuru neatļauta izpaušana var būt nevēlama Eiropas Savienības vai vienas vai vairāku dalībvalstu interesēm.

3. ESKI piemēro drošības klasifikācijas marķējumu saskaņā ar 2. punktu. Var piemērot papildu marķējumu, kas nav klasifikācijas marķējums, bet ir paredzēts, lai norādītu saistīto darbības jomu, autoru, ierobežotu izplatīšanu, izmantošanu vai norādītu pieļaujamo izpaušanu.

([1]) Padomes 1968. gada 29. februāra Regula (EEK, Euratom, EOTK) Nr. 259/68, ar ko nosaka Eiropas Kopienu Civildienesta noteikumus un Pārējo darbinieku nodarbināšanas kārtību un nosaka pagaidu pasākumus, kas piemērojami Komisijas ierēdņiem (Pārējo darbinieku nodarbināšanas kārtība) (OV L 56, 4.3.1968., 1. lpp.).

4. pants

Klasifikācijas pārvaldība

1. Ikviens Komisijas loceklis vai Komisijas dienests nodrošina, ka ESKI, ko tas ir izveidojis, ir pienācīgi klasificēta, skaidri apzīmēta ESKI un saglabā klasifikācijas līmeni vienīgi tik ilgi, cik tas nepieciešams.

2. Neskarot 26. pantu, ESKI klasifikācijas līmeņa pazemināšanu vai deklasifikāciju, vai 3. panta 2. punktā minētā marķējumu maiņu vai noņemšanu veic tikai ar autora iepriekšēju rakstisku piekrišanu.

3. Attiecīgā gadījumā īstenošanas noteikumus par rīkošanos ar ESKI, tostarp praktisko klasifikācijas rokasgrāmatu, pieņem saskaņā ar 60. pantu.

5. pants

Klasificētas informācijas aizsardzība

1. ESKI aizsargā saskaņā ar šo lēmumu un tā īstenošanas noteikumiem.

2. Jebkādas ESKI vienības turētājs ir atbildīgs par tās aizsardzību saskaņā ar šo lēmumu un tā īstenošanas noteikumiem, ievērojot noteikumus, kas izklāstīti turpmāk 4. nodaļā.

3. Ja dalībvalstis Komisijas struktūrās vai tīklos ievieš klasificētu informāciju, kam uzlikts valsts drošības klasifikācijas marķējums, Komisija aizsargā šo informāciju saskaņā ar prasībām, kas attiecas uz līdzvērtīga līmeņa ESKI, kā tas izklāstīts I pielikumā ietvertajā drošības klasifikāciju atbilsmju tabulā.

4. ESKI kopumam var piešķirt tāda līmeņa aizsardzību, kas atbilst augstākam klasifikācijas līmenim nekā tā atsevišķām sastāvdaļām piešķirtais klasifikācijas līmenis.

6. pants

Drošības riska pārvaldība

1. Drošības pasākumi ESKI aizsardzībai visā tās aprites cikla laikā jo īpaši ir samērīgi ar drošības klasifikācijas līmeni, informācijas vai materiāla veidu un apjomu, to iekārtu atrašanās vietu un uzbūvi, kurās ESKI atrodas, un vietēji izvērtētiem ļaunprātīgu un/vai noziedzīgu nodarījumu draudiem, tostarp spiegošanu, sabotāžu vai terorismu.

2. Ārkārtas rīcības plānos ņem vērā vajadzību aizsargāt ESKI ārkārtas situācijās, lai nepieļautu neatļautu piekļuvi, izpaušanu, integritātes vai pieejamības zudumu.

3. Visu dienestu darbības nepārtrauktības plānos iekļauj preventīvus un atgūšanas pasākumus, lai mazinātu nozīmīgu starpgadījumu vai incidentu ietekmi uz rīkošanos ar ESKI un tās glabāšanu.

7. pants

Šā lēmuma īstenošana

1. Attiecīgā gadījumā īstenošanas noteikumus šā lēmuma papildināšanai vai atbalstam pieņem saskaņā ar 60. pantu.

2. Komisijas dienesti veic visus viņu kompetencē ietilpstošos nepieciešamos pasākumus, lai nodrošinātu, ka, rīkojoties ar ESKI vai jebkuru citu klasificētu informāciju vai glabājot to, piemēro šo lēmumu un attiecīgos īstenošanas noteikumus.

3. Drošības pasākumi, ko veic, īstenojot šo lēmumu, atbilst principiem par drošību Komisijā, kas noteikti 3. pantā Lēmumā (ES, Euratom) 2015/443.

4. Cilvēkresursu un drošības ĢD ģenerāldirektors izveido Komisijas Drošības iestādi Cilvēkresursu un drošības ģenerāldirektorāta ietvaros. Komisijas Drošības iestāde pilda pienākumus, kas tai uzticēti ar šo lēmumu un tā īstenošanas noteikumiem.

5. Katrā Komisijas dienestā vietējais drošības speciālists (*LSO*), kas minēts 20. pantā Lēmumā (ES, Euratom) Nr. 2015/443, ciešā sadarbībā ar Cilvēkresursu un drošības ģenerāldirektorātu veic šādus vispārīgus pienākumus ESKI aizsardzībai saskaņā ar šo lēmumu:

a) pārvalda darbinieku drošības atļauju pieteikumus;

b) piedalās drošības mācībās un informatīvās sanāksmēs;

c) uzrauga attiecīgā dienesta reģistra kontrolieri (RK);

d) ziņo par drošības prasību pārkāpumiem un ESKI apdraudējumiem;

e) glabā rezerves atslēgas un pierakstus par katru kodu kombināciju;

f) uzņemas citus uzdevumus, kas saistīti ar ESKI aizsardzību vai noteikti īstenošanas noteikumos.

8. pants

Drošības prasību pārkāpumi un ESKI apdraudējums

1. Drošības prasību pārkāpums rodas personas tādas darbības vai bezdarbības rezultātā, kas ir pretrunā šajā lēmumā un tā īstenošanas noteikumos paredzētajiem drošības noteikumiem.

2. ESKI ir apdraudēta, ja drošības prasību pārkāpuma dēļ tā ir pilnībā vai daļēji izpausta nesankcionētām personām.

3. Par visiem drošības pārkāpumiem vai aizdomām par drošības pārkāpumiem nekavējoties ziņo Komisijas Drošības iestādei.

4. Ja ir zināms vai pastāv pamatotas aizdomas, ka ESKI ir apdraudēta vai zudusi, veic drošības izmeklēšanu saskaņā ar 13. pantu Lēmumā (ES, Euratom) 2015/443.

5. Veic visus vajadzīgos pasākumus, lai:

a) informētu autoru;

b) nodrošinātu, ka faktu apzināšanas nolūkā lietu izmeklē darbinieki, kas nav tieši saistīti ar pārkāpumu;

c) novērtētu iespējamo kaitējumu, kas nodarīts Savienības vai dalībvalstu interesēm;

d) veiktu attiecīgus pasākumus, lai nepieļautu atkārtošanos; kā arī

e) par veiktajiem pasākumiem ziņotu attiecīgajām iestādēm.

6. Personām, kuras ir atbildīgas par šajā lēmumā izklāstīto drošības noteikumu pārkāpšanu, var piemērot disciplināratbildību saskaņā ar Civildienesta noteikumiem. Personām, kuras ir atbildīgas par ESKI apdraudējumu vai zudumu, piemēro disciplināratbildību un/vai cita veida tiesvedību saskaņā ar spēkā esošajiem normatīvajiem aktiem.

2. NODAĻA

DARBINIEKU DROŠĪBA

9. pants

Definīcijas

Šajā nodaļā piemēro šādas definīcijas:

1) "atļauja piekļūt ESKI" ir Komisijas Drošības iestādes lēmums, …ko pieņem pamatojoties uz dalībvalsts kompetentās iestādes apgalvojumu par to, ka Komisijas ierēdnim, citam darbiniekam, vai norīkotam valsts ekspertam, ja ir konstatēts, ka viņam ir vajadzība pēc informācijas, un viņš ir attiecīgi informēts par saviem pienākumiem un atbildību, līdz konkrētam datumam var piešķirt piekļuvi ESKI līdz konkrētam klasifikācijas līmenim (*CONFIDENTIEL UE/EU CONFIDENTIAL* vai augstākam); var uzskatīt, ka tāda persona ir "saņēmusi drošības atļauju";

2) "darbinieku drošības atļaujas piešķiršana" nozīmē tādu pasākumu piemērošanu, kas nodrošina, ka piekļuvi ESKI piešķir tikai personām,

a) kurām ir vajadzība pēc informācijas;

b) kuras attiecīgā gadījumā ir saņēmušas atbilstoša līmeņa drošības atļauju; un

c) kuras ir informētas par viņu pienākumiem un atbildību;

3) "personāla drošības pielaide" (PDP) ir dalībvalsts kompetentās iestādes deklarācija, kas pieņemta pēc tam, kad dalībvalsts kompetentās iestādes veikušas drošības izmeklēšanu, un ar ko apliecina, ka personai, ja ir konstatēts, ka tai ir vajadzība pēc informācijas un tā ir attiecīgi informēta par saviem pienākumiem un atbildību, līdz konkrētam datumam var piešķirt piekļuvi ESKI līdz konkrētam līmenim (*CONFIDENTIEL UE/EU CONFIDENTIAL* vai augstākam);

4) "personāla drošības pielaides apliecība" (PDPA) ir kompetentas iestādes izdota apliecība, kurā teikts, ka personai ir derīga drošības pielaide vai Komisijas Drošības iestādes izdota drošības atļauja, un kurā norādīts tas ESKI klasifikācijas līmenis, līdz kuram personai var piešķirt piekļuvi (*CONFIDENTIEL UE/EU CONFIDENTIAL* vai augstāks), attiecīgās drošības pielaides vai atļaujas derīguma termiņš un pašas apliecības derīguma termiņš;

5) "drošības izmeklēšana" ir izmeklēšanas procedūras, ko saskaņā ar spēkā esošiem valsts normatīvajiem aktiem veic dalībvalsts kompetentā iestāde, lai pārliecinātos, ka nav nekādas nelabvēlīgas informācijas, kas varētu liegt konkrētai personai saņemt drošības pielaidi līdz konkrētam līmenim (*CONFIDENTIEL UE/EU CONFIDENTIAL* vai augstākam).

10. pants

Pamatprincipi

1. Personai piešķir piekļuvi ESKI vienīgi pēc tam, kad:

1) konstatēta personas vajadzība pēc informācijas;

2) persona ir iepazīstināta ar ESKI aizsardzībai paredzētiem drošības noteikumiem un attiecīgajiem drošības standartiem un pamatnostādnēm, un tā ir apliecinājusi savus pienākumus un atbildību saistībā ar šādas informācijas aizsargāšanu;

3) attiecībā uz informāciju, kuras klasifikācijas līmenis ir *CONFIDENTIEL UE/EU CONFIDENTIAL* vai augstāks, persona ir saņēmusi attiecīga līmeņa drošības atļauju vai ieņemamā amata dēļ citā veidā ir pienācīgi pilnvarota saskaņā ar attiecīgās valsts normatīvajiem aktiem.

2. Visas personas, kuru pienākumos var ietilpt vajadzība piekļūt ESKI, kas klasificēta *CONFIDENTIEL UE/EU CONFIDENTIAL* vai augstākā līmenī, saņem attiecīga līmeņa drošības atļauju, pirms tām piešķir piekļuvi šādai ESKI. Attiecīgās personas rakstiski piekrīt, ka tām piemēro darbinieku drošības pielaides procedūru. Pretējā gadījumā personu nevar apstiprināt darbam konkrētajā amatā, tai nevar uzticēt veikt konkrēto funkciju vai uzdevumu, kas ir saistīts ar piekļuvi informācijai, kas klasificēta *CONFIDENTIEL UE/EU CONFIDENTIAL* vai augstākā līmenī.

3. Darbinieku drošības pielaides procedūras izstrādā tā, lai, ņemot vērā attiecīgās personas lojalitāti, patiesumu un uzticamību, noteiktu, vai konkrētai personai drīkst piešķirt piekļuvi ESKI.

4. Personas lojalitāti, patiesumu un uzticamību, lai šai personai varētu piešķirt drošības pielaidi ar mērķi piekļūt informācijai, kas klasificēta *CONFIDENTIEL UE/EU CONFIDENTIAL* vai augstākā līmenī, nosaka ar drošības izmeklēšanas palīdzību, ko veic dalībvalsts kompetentās iestādes saskaņā ar valsts normatīvajiem aktiem.

5. Komisijas Drošības iestāde ir vienīgā atbildīgā par sadarbību ar valsts drošības iestādēm (VDI) vai citām kompetentām valsts iestādēm saistībā ar visiem drošības pielaides jautājumiem. Visi kontakti starp Komisijas dienestiem un to darbiniekiem un VDI un citām kompetentajām iestādēm notiek ar Komisijas Drošības iestādes starpniecību.

11. pants

Drošības atļauju piešķiršanas procedūra

1. Katrs ģenerāldirektors vai dienesta vadītājs Komisijā apzina tos amatus tā vadītajos departamentos, kuru ieņēmējiem, lai veiktu pienākumus, ir vajadzīga piekļuve informācijai, kas klasificēta *CONFIDENTIEL UE/EU CONFIDENTIAL* vai augstākā līmenī, tāpēc tiem ir vajadzīga drošības atļauja.

2. Tiklīdz kļūst zināms, ka persona tiks iecelta amatā, kur vajadzīga piekļuve informācijai, kas klasificēta *CONFIDENTIEL UE/EU CONFIDENTIAL* vai augstākā līmenī, attiecīgā Komisijas dienesta *LSO* informē Komisijas Drošības iestādi, kas nosūta šai personai drošības pielaides anketu, ko sagatavojusi tās dalībvalsts VDI, kuras valstspiederīgais šī persona bija, kad kļuva par Eiropas iestāžu darbinieku. Persona rakstiski piekrīt, ka tai piemēro drošības pielaides procedūru un visīsākajā iespējamā termiņā nosūta aizpildītu aptaujas anketu atpakaļ Komisijas Drošības iestādei.

3. Komisijas Drošības iestāde pārsūta aizpildīto darbinieka drošības pielaides anketu tās dalībvalsts VDI, kuras valstspiedrīgais šī persona bija, kad kļuva par Eiropas iestāžu darbinieku, un lūdz veikt drošības izmeklēšanu saistībā ar ESKI līmeni, kuram šai personai vajadzēs piekļūt.

4. Ja Komisijas Drošības iestādei par personu, kura pieteikusies drošības pielaides saņemšanai, ir zināma drošības izmeklēšanai nozīmīga informācija, Komisijas Drošības iestāde, rīkojoties saskaņā ar attiecīgajiem noteikumiem, šo informāciju paziņo kompetentajai VDI.

5. Pēc drošības izmeklēšanas beigām un cik drīz vien iespējams pēc tam, kad attiecīgā VDI ir paziņojusi savu vispārējo novērtējumu par drošības izmeklēšanas rezultātiem, Komisijas Drošības iestāde:

a) var attiecīgajai personai piešķirt atļauju piekļūt ESKI un ļaut piekļūt konkrēta līmeņa ESKI līdz norādītā termiņa beigām, bet ne ilgāk par 5 gadiem, ja drošības izmeklēšanas rezultātā apstiprinās, ka nav zināma negatīva informācija, kas varētu ļaut apšaubīt personas lojalitāti, patiesumu un uzticamību;

b) ja drošības izmeklēšanas rezultātā nerodas šāda pārliecība, saskaņā ar attiecīgiem noteikumiem to paziņo attiecīgajai personai, kura var lūgt, lai to uzklausa Komisijas Drošības iestāde, kas savukārt var lūgt kompetento VDI sniegt papildu skaidrojumus, ko tā var sniegt saskaņā ar saviem valsts normatīvajiem aktiem. Ja drošības izmeklēšanas rezultātu apstiprina, atļauju piekļūt ESKI, neizsniedz.

6. Drošības izmeklēšanai un tās rezultātiem piemēro normatīvos aktus, kas ir spēkā attiecīgajā dalībvalstī, tostarp par pārsūdzībām. Komisijas Drošības iestādes lēmumus pārsūdz saskaņā ar Civildienesta noteikumiem.

7. Komisija akceptē atļauju piekļūt ESKI, kuru piešķīrusi jebkura cita Savienības iestāde, struktūra vai aģentūra, ar noteikumu, ka tā joprojām ir derīga. Atļauja attiecas uz visiem attiecīgās personas uzdevumiem Komisijā. Savienības iestāde, struktūra vai aģentūra, kurā persona stājas darbā, paziņos attiecīgajai VDI par darba devēja maiņu.

8. Ja persona nesāk darbu 12 mēnešu laikā no dienas, kad Komisijas Drošības iestādei ir paziņots par drošības izmeklēšanas rezultātiem, vai ja persona pārtrauc darbu uz 12 mēnešiem un to šajā laikā nenodarbina ne Komisija, ne kāda cita Savienības iestāde, struktūra vai aģentūra, un tā neieņem amatu dalībvalsts valsts pārvaldē, Komisijas Drošības iestāde vēršas pie attiecīgās VDI, lai saņemtu apstiprinājumu, ka drošības pielaide joprojām ir derīga un atbilstīga.

9. Ja Komisijas Drošības iestādei kļūst zināma informācija par drošības risku, ko izraisa persona, kurai ir derīga drošības atļauja, Drošības iestāde, ievērojot attiecīgos noteikumus, paziņo par to attiecīgajai VDI.

10. Ja VDI informē Komisijas Drošības iestādi, ka tā atsauc apstiprinājumu, kas sniegts saskaņā ar 5. panta a) punktu attiecībā uz personu, kurai ir derīga atļauja piekļūt ESKI, Komisijas Drošības iestāde var lūgt VDI skaidrojumus, ko tā var sniegt saskaņā ar savas valsts normatīvajiem aktiem. Ja attiecīgā VID apstiprina negatīvo informāciju, drošības atļauju atsauc un personai liedz piekļuvi ESKI un amatiem, kuros šāda piekļuve ir iespējama vai kuros minētā persona varētu apdraudēt drošību.

11. Ikvienu lēmumu apturēt vai atcelt atļauju piekļūt ESKI personai, kurai piemērojams šis lēmums, un attiecīgā gadījumā šāda lēmuma iemeslus paziņo attiecīgajai personai, kura var lūgt, lai viņu uzklausītu Komisijas Drošības iestāde. VDI sniegtajai informācijai piemēro atbilstīgos normatīvos aktus, kas ir spēkā attiecīgajā dalībvalstī. Šajā saistībā pieņemtos Komisijas Drošības iestādes lēmumus pārsūdz saskaņā ar Civildienesta noteikumiem.

12. Komisijas dienesti nodrošina, ka valstu eksperti, kas norīkoti uz tādiem amatiem, kam vajadzīga drošības atļauja piekļūt ESKI, pirms stāšanās amatā Komisijas Drošības iestādei uzrāda saskaņā ar valsts normatīvajiem aktiem derīgu PDP vai personāla drošības pielaides apliecību (PDPA), un uz šā pamata Drošības iestāde izsniedz drošības atļauju piekļūt ESKI līdz līmenim, kas atbilst valsts drošības pielaidē minētajam, ar maksimālo derīguma termiņu uz norīkojuma laiku.

Piekļuve ESKI personām, kuru atļauja piekļūt pamatojas uz ieņemamo amatu

13. Komisijas locekļus, kuriem ir piekļuve ESKI, pamatojoties uz ieņemamo amatu saskaņā ar Līgumu, iepazīstina ar drošības pienākumiem, kas attiecas uz ESKI aizsardzību.

Drošības pielaižu un drošības atļauju uzskaite

14. Drošības pielaižu un atļauju, ar ko piešķir piekļuvi ESKI, uzskaiti veic Komisijas Drošības iestāde saskaņā ar šo lēmumu. Uzskaitē ietver vismaz to ESKI klasifikācijas līmeni, kuram personai ir piešķirta piekļuve, drošības pielaides izsniegšanas datumu un derīguma termiņu.

15. Komisijas Drošības iestāde var izsniegt PDPA, norādot ESKI klasifikācijas līmeni, kuram personai var piešķirt piekļuvi (*CONFIDENTIEL UE/EU CONFIDENTIAL* vai augstāks līmenis), attiecīgās ESKI piekļuves atļaujas spēkā stāšanās datumu un apliecības derīguma beigu datumu.

Drošības atļaujas atjaunošana

16. Pēc sākotnējās drošības atļaujas piešķiršanas un ar nosacījumu, ka persona nepārtraukti ir bijusi Eiropas Komisijas vai citas Savienības iestādes, struktūras vai aģentūras darbinieks(-ce), un tai joprojām ir vajadzīga piekļuve ESKI, drošības atļauju piekļūt ESKI pārskata atjaunošanas nolūkā, parasti ik pēc pieciem gadiem, skaitot no dienas, kad paziņots par pēdējās drošības pārbaudes rezultātiem, uz kuriem atļauja balstīta.

17. Komisijas Drošības iestāde var pagarināt esošās drošības atļaujas derīguma termiņu līdz 12 mēnešiem, ja divu mēnešu laikā no dienas, kad nosūtīts atjaunošanas pieprasījums un atbilstošā drošības pielaides anketa, no attiecīgās VDI vai citas kompetentas valsts iestādes nav saņemta negatīva informācija. Ja pēc šā 12 mēnešu laikposma beigām attiecīgā VDI vai cita kompetentā valsts iestāde nav paziņojusi Komisijai Drošības iestādei savu atzinumu, personai nosaka tādus pienākumus, kuru pildīšanai drošības atļauja nav vajadzīga.

12. pants

Drošības atļauju instruktāža

1. Pēc dalības Komisijas Drošības iestādes rīkotā drošības atļaujas instruktāžā, visas personas, kas ir saņēmušas drošības atļauju, rakstiski apliecina, ka ir sapratušas savus pienākumus attiecībā uz ESKI aizsardzību un iespējamām sekām ESKI apdraudējuma gadījumā. Komisijas Drošības iestāde uztur šādu rakstisku apliecinājumu reģistru.

2. Visas personas, kuras ir saņēmušas atļauju piekļūt ESKI vai kurām ir jārīkojas ar ESKI, jau sākotnēji tiek informētas un vēlāk regulāri saņem instruktāžu par draudiem drošībai, un tām ir nekavējoties jāinformē Komisijas Drošības iestāde par jebkuru tuvošanās mēģinājumu vai citu darbību, kas šķiet aizdomīga vai neparasta.

3. Visas personas, kas beidz pildīt pienākumus, kuri saistīti ar piekļuvi ESKI, tiek iepazīstinātas ar pienākumu arī turpmāk neizpaust ESKI, un vajadzības gadījumā tās apliecina to rakstiski.

13. pants

Drošības pagaidu atļaujas

1. Ārkārtas apstākļos, ja tas ir dienesta interesēs, gaidot pilnīgas drošības izmeklēšanas pabeigšanu, Komisijas Drošības iestāde pēc konsultēšanās ar tās dalībvalsts VDI, kuras valstspiederīgais ir attiecīgā persona, un ar nosacījumu, ka priekškontroles rezultāti apliecina, ka nav zināma nekāda negatīva informācija, personai var piešķirt pagaidu atļauju piekļūt ESKI konkrēta uzdevuma veikšanai, neskarot noteikumus par drošības pielaides atjaunošanu. Šādas pagaidu atļaujas piekļuvei ESKI ir derīgas vienu termiņu, kas nepārsniedz sešus mēnešus, un nesniedz piekļuvi informācijai, kas klasificēta *TRES SECRET UE/EU TOP SECRET* līmenī.

2. Pēc tam, kad saskaņā ar 12. panta 1. punktu saņemta instruktāža, visas personas, kam piešķirta pagaidu atļauja, rakstiski apliecina, ka ir sapratušas savus pienākumus attiecībā uz ESKI aizsargāšanu un iespējamās sekas ESKI apdraudējuma gadījumā. Komisijas Drošības iestāde uztur šādu rakstisku apliecinājumu reģistru.

14. pants

Dalība Komisijas organizētās klasificētās sanāksmēs

1. Komisijas dienesti, kas atbild par tādu sanāksmju rīkošanu, kurās apspriež informāciju, kas klasificēta *CONFIDENTIEL UE/EU CONFIDENTIAL* vai augstākā līmenī, ar *LSO* vai sanāksmes organizatora starpniecību savlaicīgi iepriekš informē Komisijas Drošības iestādi par šādas sanāksmes datumu, laiku, vietu un dalībniekiem.

2. Ievērojot 11. panta 13. punktu, personas, kas nosūtītas piedalīties Komisijas rīkotās sanāksmēs, kurās apspriež informāciju, kas klasificēta *CONFIDENTIEL UE/EU CONFIDENTIAL* vai augstākā līmenī, var tajās piedalīties tikai tad, ja ir apstiprināta viņu drošības pielaide vai drošības atļaujas statuss. Personām, kas Komisijas Drošības iestādei nav uzrādījušas PDPA vai citu drošības pielaides pierādījumu, vai Komisijas dalībniekiem, kuriem nav drošības atļaujas, liedz piekļuvi šādām klasificētām sanāksmēm.

3. Pirms klasificētas sanāksmes organizēšanas atbildīgais sanāksmes organizators vai *LSO* tajā Komisijas dienestā, kas rīko sanāksmi, pieprasa ārējiem dalībniekiem uzrādīt Komisijas Drošības iestādei PDPA vai citu drošības pielaides pierādījumu. Komisijas Drošības iestāde informē *LSO* vai sanāksmes rīkotāju par saņemtajām PDPA vai citiem pierādījumiem par PDP. Attiecīgā gadījumā var izmantot konsolidētu sarakstu ar personu vārdiem un uzvārdiem, sniedzot vajadzīgo drošības pielaides pierādījumu.

4. Ja kompetentās iestādes informē Komisijas Drošības iestādi, ka personai, kuras pienākumos ietilpst apmeklēt Komisijas rīkotās sanāksmes, PDP ir atsaukta, Komisijas Drošības iestāde informē par sanāksmes rīkošanu atbildīgā Komisijas dienesta *LSO*.

15. pants

Iespējama piekļuve ESKI

Kurjeri, apsargi un eskortētāji ir saņēmuši attiecīga līmeņa drošības atļaujas vai par viņiem ir veikta cita veida atbilstīga izmeklēšana saskaņā ar valsts normatīvajiem aktiem, ir saņēmuši instruktāžu par ESKI aizsardzības drošības procedūrām un ir informēti par saviem pienākumiem aizsargāt uzticēto informāciju.

3. NODAĻA

FIZISKĀ DROŠĪBA KLASIFICĒTAS INFORMĀCIJAS AIZSARDZĪBAI

16. pants

Pamatprincipi

1. Fiziskās drošības pasākumu mērķis ir nepieļaut slepenu vai vardarbīgu ielaušanos, atturēt no neatļautām darbībām, kavēt un atklāt šādas neatļautas darbības un ļaut nošķirt darbiniekus attiecībā uz piekļuvi ESKI, pamatojoties uz to vajadzību pēc informācijas. Šādus pasākumus nosaka, pamatojoties uz riska pārvaldības procesu, saskaņā ar šo lēmumu un tā īstenošanas noteikumiem.

2. Fiziskās drošības pasākumi jo īpaši ir paredzēti, lai nepieļautu neatļautu piekļuvi ESKI:

a) nodrošinot, ka ar ESKI rīkojas un to glabā atbilstīgi;

b) ļaujot nošķirt darbiniekus attiecībā uz piekļuvi ESKI, pamatojoties uz to vajadzību pēc informācijas un – attiecīgā gadījumā – drošības atļauju;

c) atturot no neatļautām darbībām, tās novēršot un aizkavējot; Fun

d) neatļaujot vai aizkavējot nepiederošu personu iekļūšanu slepus vai ar spēku.

3. Fiziskās drošības pasākumus īsteno visās telpās, ēkās, birojos, zālēs un citās zonās, kur rīkojas ar ESKI vai to glabā, tostarp zonās, kur atrodas 5. nodaļā minētās komunikācijas un informācijas sistēmas.

4. Zonas, kurās glabā ESKI, kas klasificēta *CONFIDENTIEL UE/EU CONFIDENTIAL* vai augstākā līmenī, izveido par drošības zonām saskaņā ar šo nodaļu, un tās apstiprina Komisijas Drošības akreditācijas iestāde.

5. Lai aizsargātu ESKI, kas klasificēta *CONFIDENTIEL UE/EU CONFIDENTIAL* vai augstākā līmenī, izmanto vienīgi Komisijas Drošības iestādes apstiprinātas iekārtas vai ierīces.

17. pants

Fiziskās drošības prasības un pasākumi

1. Fiziskās drošības pasākumus izvēlas, pamatojoties uz draudu novērtējumu, ko veikusi Komisijas Drošības iestāde, attiecīgā gadījumā apspriežoties ar citiem Komisijas dienestiem, citām Savienības iestādēm, aģentūrām vai struktūrām un/vai dalībvalstu kompetentajām iestādēm. Komisija ESKI aizsargāšanai savās telpās piemēro riska pārvaldības procesu, lai nodrošinātu, ka novērtētajam riskam pretnostata samērīga līmeņa fizisko aizsardzību. Riska pārvaldības procesā ņem vērā visus attiecīgos faktorus, jo īpaši:

a) ESKI klasifikācijas līmeni;

b) ESKI formātu un apjomu, ņemot vērā, ka liels ESKI daudzums vai apkopojums var prasīt stingrākus aizsardzības pasākumus;

c) apkārtējo vidi un to ēku un zonu uzbūvi, kurās atrodas ESKI; un

d) novērtētos draudus, ko rada izlūkošanas dienesti, kuru mērķis ir Savienība, tās iestādes, struktūras vai aģentūras vai dalībvalstis, un sabotāža, terorisms un citas graujošas vai kriminālas darbības.

2. Piemērojot padziļinātas aizsardzības koncepciju, Komisijas Drošības iestāde nosaka piemērotu īstenojamo fiziskās drošības pasākumu kopumu. Šim nolūkam Komisija Drošības dienests izstrādā minimuma standartus, normas un kritērijus, ko nosaka īstenošanas noteikumos.

3. Komisijas Drošības iestāde ir pilnvarota pārmeklēt personas pie ieejas vai izejas, lai novērstu materiālu neatļautu ienešanu vai ESKI neatļautu iznešanu no telpām vai ēkām.

4. Ja pastāv risks, ka ESKI varētu būt atstāta novārtā, arī nejauši, attiecīgie Komisijas dienesti veic atbilstošus pasākumus, kurus nosaka Komisijas Drošības iestāde, lai novērstu šo risku.

5. Attiecībā uz jaunām iekārtām fiziskās drošības prasības un to darbības specifikācijas nosaka ar Komisijas Drošības iestādes piekrišanu jau iekārtu plānošanas un izstrādes stadijā. Jau esošās iekārtās fiziskās drošības prasības īsteno saskaņā ar minimuma standartiem, normām un kritērijiem, kas noteikti īstenošanas noteikumos.

18. pants

Iekārtas ESKI fiziskai aizsardzībai

1. Fiziskai ESKI aizsardzībai izveido divu veidu fiziski aizsargātas zonas:

a) administratīvās zonas; un

b) drošības zonas (tostarp tehniski drošas drošības zonas).

2. Komisijas Drošības akreditācijas iestāde nosaka, vai zona atbilst prasībām, lai to varētu kvalificēt pie administratīvām zonām, drošības zonām vai tehniski drošām drošības zonām.

3. Attiecībā uz administratīvām zonām:

a) izveido redzami nospraustu perimetru, kurā var pārbaudīt personas un, ja iespējams, transportlīdzekļus;

b) piekļuvi bez eskorta piešķir tikai personām, kurām ir pienācīga Komisijas Drošības iestādes vai citas kompetentās iestādes atļauja; un

c) visas pārējās personas vienmēr eskortē vai piemēro līdzvērtīgu kontroli.

4. Attiecībā uz drošības zonām:

a) izveido redzami nospraustu un aizsargātu perimetru, kurā visu veidu iekļūšanu un izkļūšanu kontrolē ar caurlaižu vai individuālās identifikācijas sistēmu;

b) piekļuvi bez eskorta piešķir tikai personām, kurām ir drošības pielaide un īpaša atļauja iekļūt zonā, pamatojoties uz vajadzību pēc informācijas;

c) visas pārējās personas vienmēr eskortē vai piemēro līdzvērtīgu kontroli.

5. Gadījumos, kad piekļuve drošības zonai praktiskām vajadzībām nozīmē tiešu piekļuvi klasificētai informācijai, kas tajā atrodas, piemēro šādus papildu nosacījumus:

a) skaidri norāda augstāko tās informācijas drošības klasifikācijas līmeni, kura parasti atrodas šajā zonā;

b) visiem apmeklētājiem ir nepieciešama īpaša atļauja iekļūt zonā, un viņus vienmēr eskortē, visiem apmeklētājiem ir pienācīga drošības pielaide, ja vien nav veikti pasākumi, lai nodrošinātu, ka piekļuve ESKI nav iespējama.

6. Drošības zonas, kuras ir aizsargātas pret slepenu noklausīšanos ar skaņas pārtveršanu, apzīmē par tehniski drošām drošības zonām. Piemēro šādas papildu prasības:

a) šādas zonas ir aprīkotas ar ielaušanās konstatācijas sistēmu (IKS), tās ir slēgtas, kad tajās neviena nav, vai apsargātas, kad tajās kāds uzturas. Visas atslēgas pārvalda saskaņā ar 20. pantu;

b) pārbauda visas personas, kas ienāk šajās zonās, un materiālus, ko tajās ienes;

c) šādās zonās Komisijas Drošības iestāde veic regulāras fiziskas un/vai tehniskas pārbaudes. Minētās pārbaudes veic arī katru reizi pēc neatļautas iekļūšanas vai aizdomām par šādu iekļūšanu; un

d) šādās zonās neizmanto neatļautas sakaru līnijas, neatļautus tālruņus vai citas neatļautas sakaru ierīces un elektriskas vai elektroniskas iekārtas.

7. Neatkarīgi no 6. punkta d) apakšpunkta pirms dažādu tipu sakaru iekārtu, elektroiekārtu un elektronisku sakaru iekārtu izmantošanas zonās, kur notiek sanāksmes vai veic darbu ar informāciju, kas klasificēta *SECRET UE/EU SECRET* un augstākā līmenī, un ja draudi ESKI tiek atzīti par augstiem, tās pārbauda Komisijas Drošības iestāde, lai nodrošinātu, ka ar šādām ierīcēm netīšām vai nelikumīgi nepārraidītu nekādu saprotamu informāciju ārpus drošības zonas perimetra.

8. Drošības zonas, kurās dienesta personāls neuzturas visu diennakti, attiecīgā gadījumā pārbauda tūlīt pēc parastā darba laika beigām un nejauši izvēlētos intervālos ārpus parastā darba laika, ja vien tajās nav uzstādīta IKS.

9. Administratīvās zonas ietvaros uz laiku var izveidot drošības zonas un tehniski drošas drošības zonas, lai organizētu slepenu sanāksmi vai citiem līdzīgiem mērķiem.

10. Attiecīgā Komisijas dienesta *LSO* izstrādā drošības darba procedūras (*SecOPs*) katrai drošības zonai, par kuru tas ir atbildīgs, un saskaņā šo lēmumu un tā īstenošanas noteikumiem nosaka:

a) ESKI klasifikācijas līmeni, ar kuru var rīkoties un kuru var glabāt zonā;

b) kādi pārraudzības un aizsardzības pasākumi jāveic;

c) kurām personām ir atļauts iekļūt zonā bez eskorta, pamatojoties uz vajadzības pēc informācijas principu un drošības atļauju;

d) attiecīgā gadījumā – eskortēšanas vai ESKI aizsardzības procedūras, atļaujot citām personām piekļūt zonai;

e) citus attiecīgus pasākumus un procedūras.

11. Drošības zonās izveido glabātavas. Sienas, grīdas, griestus, logus un aizslēdzamas durvis apstiprina Komisijas Drošības iestāde, un tās nodrošina aizsardzību, kas ir līdzvērtīga tāda seifa sniegtajai aizsardzībai, kurš apstiprināts tāda paša klasifikācijas līmeņa ESKI glabāšanai.

19. pants

Fiziskās aizsardzības pasākumi rīcībai ar ESKI un tās glabāšanai

1. Ar ESKI, kas klasificēta *RESTREINT UE/EU RESTRICTED* līmenī, var rīkoties:

a) drošības zonā;

b) administratīvā zonā, ja ESKI ir aizsargāta pret nesankcionētu personu piekļuvi; vai

c) ārpus drošības vai administratīvās zonas, ja informācijas turētājs pārvieto ESKI saskaņā ar 31. pantu un ja viņš veic kompensējošus pasākumus, kas izklāstīti īstenošanas noteikumos, lai nodrošinātu, ka ESKI ir aizsargāta pret nesankcionētu personu piekļuvi.

2. ESKI, kas klasificēta *RESTREINT UE/EU RESTRICTED* līmenī, glabā piemērotās aizslēdzamās biroja mēbelēs administratīvā zonā vai drošības zonā. To uz laiku var glabāt ārpus administratīvās vai drošības zonas, ja informācijas turētājs veic kompensējošus pasākumus, kas izklāstīti īstenošanas noteikumos.

3. Ar ESKI, kas klasificēta *CONFIDENTIEL UE/EU CONFIDENTIAL* vai *SECRET UE/EU SECRET* līmenī, var rīkoties:

a) drošības zonā;

b) administratīvā zonā, ja ESKI ir aizsargāta pret nesankcionētu personu piekļuvi; vai

c) ārpus drošības vai administratīvās zonas, ja informācijas turētājs:

   i) veic kompensējošus pasākumus, kas izklāstīti īstenošanas noteikumos, lai nodrošinātu, ka ESKI ir aizsargāta pret nesankcionētu personu piekļuvi;

   ii) nodrošina, ka ESKI vienmēr ir viņa personīgā kontrolē; un

   iii) gadījumā, ja dokumenti ir papīra formā, par šo faktu ir informējis attiecīgo reģistru.

4. ESKI, kas klasificēta *CONFIDENTIEL UE/EU CONFIDENTIAL* un *SECRET UE/EU SECRET* līmenī, glabā drošības zonā seifā vai glabātavā.

5. Ar ESKI, kas klasificēta *TRES SECRET UE/EU TOP SECRET* līmenī, var rīkoties drošības zonā, kuru izveido un uztur Komisijas Drošības iestāde un kuru Komisijas Drošības akreditācijas iestāde akreditējusi attiecīgajam drošības līmenim.

6. ESKI, kas klasificēta *TRES SECRET UE/EU TOP SECRET* līmenī, glabā drošības zonā, kuru attiecīgajam līmenim akreditējusi Komisijas Drošības akreditācijas iestāde, ievērojot vienu no šiem nosacījumiem:

a) saskaņā ar 18. punktu seifā, piemērojot vienu vai vairākus papildu kontroles pasākumus:

   1) nepārtrauktu aizsardzību vai pārbaudes, ko veic ar attiecīgu drošības pielaidi apveltīts drošības personāls vai dienesta personāls;

   2) apstiprinātu ielaušanās kontroles sistēmu (IKS) apvienojumā ar drošības operatīvajiem darbiniekiem

   vai

b) glabātavā, kas aprīkota ar IKS, apvienojumā ar drošības operatīvajiem darbiniekiem.

20. pants

ESKI aizsardzībai izmantoto atslēgu un kodu kombināciju pārvaldība

1. Biroju, telpu, glabātuvju un seifu atslēgu un kodu kombināciju pārvaldības procedūras nosaka īstenošanas noteikumos saskaņā ar 60. pantu. Šādas procedūras aizsargā pret neatļautu piekļuvi.

2. Kodu kombinācijas iegaumē pēc iespējas mazs to personu skaits, kam ir vajadzība tās zināt. To seifu un glabātavu kodu kombinācijas, kuros glabājas ESKI, maina:

a) saņemot jaunu seifu;

b) ja darbinieku lokā, kas zina šo kodu kombināciju, ir notikušas izmaiņas;

c) ja ir radies apdraudējums vai ir aizdomas, ka tas varētu būt radies;

d) veicot slēdzenes apkopi vai remontu; un

e) vismaz reizi 12 mēnešos.

4. NODAĻA

ES KLASIFICĒTAS INFORMĀCIJAS PĀRVALDĪBA

21. pants

Pamatprincipi

1. Visi ESKI dokumenti jāpārvalda saskaņā ar Komisijas politiku par dokumentu pārvaldību un līdz ar to tie jāreģistrē, jādokumentē, jāglabā un visbeidzot jāiznīcina, jānoņem paraugi vai jāiekļauj vēsturiskajos arhīvos saskaņā ar vispārējo Komisijas līmeņa uzglabājamo dokumentu sarakstu Komisijas dokumentiem.

2. Informāciju, kas klasificēta *CONFIDENTIEL UE/EU CONFIDENTIAL* vai augstākā līmenī, drošības nolūkā reģistrē, pirms to izplata un to saņemot. Informāciju, kas klasificēta *TRES SECRET UE/EU TOP SECRET* līmenī, reģistrē īpašos reģistros.

3. Komisijā, ESKI reģistra sistēmu izveido saskaņā ar 27. panta noteikumiem.

4. Komisijas dienestus un telpas, kurās rīkojas ar ESKI vai to glabā, regulāri pārbauda Komisijas Drošības iestāde.

5. ESKI pārvieto starp dienestiem un telpām ārpus fiziski aizsargātām zonām šādā veidā:

a) parasti ESKI pārsūta ar elektroniskiem līdzekļiem, kurus aizsargā ar kriptogrāfijas produktiem, kas apstiprināti atbilstīgi 5. nodaļai;

b) ja neizmanto a) punktā minētos līdzekļus, ESKI pārvieto vai nu:

   i) izmantojot elektroniskus informācijas nesējus (piemēram, zibatmiņas, kompaktdiskus, cietos diskus), kurus aizsargā ar kriptogrāfijas produktiem, kas apstiprināti atbilstīgi 5. nodaļai; vai

   ii) visos pārējos gadījumos, kā paredzēts īstenošanas noteikumos.

22. pants

Klasifikācijas un marķējumi

1. Informāciju klasificē, ja tā ir jāaizsargā, lai nodrošinātu tās konfidencialitāti, saskaņā ar 3. panta 1. punktu.

2. ESKI autors atbild par drošības klasifikācijas līmeņa noteikšanu saskaņā ar attiecīgajiem īstenošanas noteikumiem, standartiem un pamatnostādnēm par klasifikāciju un par sākotnējo informācijas izplatīšanu.

3. ESKI klasifikācijas līmeni nosaka saskaņā ar 3. panta 2. punktu un attiecīgajiem īstenošanas noteikumiem.

4. Drošības klasifikāciju norāda skaidri un pareizi neatkarīgi no tā, vai ESKI ir papīra, mutiskā, elektroniskā vai kādā citā formātā.

5. Konkrēta dokumenta atsevišķām daļām (piemēram, lappusēm, punktiem, iedaļām, pielikumiem, papildinājumiem un pievienojumiem) var būt vajadzīga atšķirīga klasifikācija, un tos attiecīgi marķē, tostarp glabājot elektroniskā formātā.

6. Vispārējais dokumenta vai lietas klasifikācijas līmenis ir vismaz tikpat augsts, cik tā komponentam ar visaugstāko klasifikācijas līmeni. Kad apkopo informāciju no dažādiem avotiem, galaproduktu pārskata, lai noteiktu tā vispārējo drošības klasifikācijas līmeni, jo tam var būt nepieciešams piešķirt augstāku klasifikācijas līmeni nekā atsevišķām tā sastāvdaļām.

7. Dokumentus, kas ietver daļas ar dažādiem klasifikācijas līmeņiem, pēc iespējas veido tā, lai daļas ar dažādiem klasifikācijas līmeņiem varētu viegli identificēt un vajadzības gadījumā atdalīt.

8. Pavadvēstules vai piezīmes klasifikācijas līmenis ir tikpat augsts kā tai pievienoto dokumentu visaugstākais klasifikācijas līmenis. Informācijas autors skaidri norāda, kādā līmenī to klasificē, kad tā ir atdalīta no pievienotajiem dokumentiem, izmantojot atbilstīgu marķējumu, piemēram:

CONFIDENTIEL UE/EU CONFIDENTIAL

bez pielikuma(-iem) *RESTREINT UE/EU RESTRICTED*

23. pants

Marķējums

Papildus vienam no drošības klasifikācijas marķējumiem, kas noteikti 3. panta 2. punktā, uz ESKI var būt šādi papildu marķējumi:

a) identifikators, kas norāda autoru;

b) brīdinājumi, kodu vārdi vai akronīmi, ar ko precizē darbības jomu, uz kuru attiecas dokuments, vai norāda konkrētus izplatīšanas nosacījumus, pamatojoties uz vajadzību pēc informācijas, vai lietošanas ierobežojumus;

c) marķējumi attiecībā uz nodošanu;

d) attiecīgā gadījumā datums vai konkrēts notikums, pēc kura informācijai var pazemināt klasifikācijas līmeni vai to var deklasificēt.

24. pants

Klasifikācijas marķējumu saīsinājumi

1. Var izmantot standartizētus klasifikācijas marķējumu saīsinājumus, lai norādītu atsevišķu teksta daļu klasifikācijas līmeni. Saīsinājumi neaizstāj pilnos klasifikācijas marķējumus.

2. ES klasificētajos dokumentos var izmantot šādus standarta saīsinājumus, lai norādītu tāda teksta iedaļu vai daļu klasifikācijas līmeni, kas ir mazāks par vienu lapu:

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

25. pants

ESKI izveide

1. Izveidojot ES klasificētu dokumentu:

a) katru lappusi skaidri marķē atbilstīgi klasifikācijas līmenim;

b) katru lappusi numurē;

c) uz dokumenta raksta reģistrācijas numuru un tematu, kurš pats par sevi nav klasificēta informācija, ja vien tam nav klasificētas informācijas marķējums;

d) dokumentu datē;

e) dokumentiem, kas klasificēti *SECRET UE/EU SECRET* vai augstākā līmenī, katrā lappusē norāda eksemplāra numuru, ja tie jāizplata vairākos eksemplāros.

2. Ja ESKI nav iespējams piemērot 1. punktu, saskaņā ar īstenošanas noteikumiem veic citus piemērotus pasākumus.

26. pants

ESKI klasifikācijas līmeņa pazemināšana un deklasifikācija

1. Izveidojot informāciju, tās autors, ja iespējams, norāda, vai var pazemināt ESKI klasifikācijas līmeni vai to deklasificēt konkrētā datumā vai pēc konkrēta notikuma.

2. Ikviens Komisijas dienests, kas ir ESKI autors, regulāri pārskata savu ESKI, lai pārliecinātos, vai attiecīgais klasifikācijas līmenis joprojām ir piemērots. Īstenošanas noteikumos paredz sistēmu Komisijā sagatavotās reģistrētās ESKI klasifikācijas līmeņa pārskatīšanai ne retāk kā ik pēc pieciem gadiem. Šāda pārskatīšana nav nepieciešama, ja autors jau no sākuma ir norādījis, ka informācijas klasifikācijas līmeni var automātiski pazemināt vai deklasificēt un uz informācijas ir attiecīgs marķējums.

3. Komisijas sagatavotu informāciju, kas klasificēta *RESTREINT UE/EU RESTRICTED* līmenī, uzskata par automātiski deklasificētu pēc trīsdesmit gadiem saskaņā ar Regulu (EEK, Euratom) Nr. 354/83, kurā grozījumi izdarīti ar Padomes Regulu (EK, Euratom) Nr. 1700/2003 ([1]).

27. pants

ESKI reģistrācijas sistēma Komisijā

1. Neskarot 52. panta 5. punktu, katrā Komisijas dienestā, kurā rīkojas ar ESKI vai glabā ESKI, kas klasificēta *CONFIDENTIEL UE/EU CONFIDENTIAL* un *SECRET UE/EU SECRET* līmenī, uztur vietējo ESKI reģistru, lai nodrošinātu, ka rīcība ar ESKI notiek saskaņā ar šo lēmumu.

2. ESKI reģistrs, ko pārvalda Ģenerālsekretariāts, ir Komisijas centrālais ESKI reģistrs. Tas darbojas kā:

— Komisijas Ģenerālsekretariāta vietējais ESKI reģistrs,

— Komisijas locekļu privāto biroju ESKI reģistrs, ja vien tiem nav savs vietējais ESKI reģistrs,

— to ģenerāldirektorātu vai dienestu ESKI reģistrs, kam nav sava vietējā ESKI reģistra,

— galvenais iekļūšanas un izkļūšanas punkts informācijai, kas klasificēta, sākot no *RESTREINT UE/EU RESTRICTED* un beidzot ar *SECRET UE/EU SECRET*, ar kuru apmainās Komisija un tās dienesti un trešās valstis un starptautiskās organizācijas un, ja tas īpaši paredzēts, arī ar citām Savienības iestādēm, aģentūrām un struktūrām.

3. Komisijas Drošības iestāde nozīmē reģistru, kas Komisijā darbojas kā galvenā saņēmēja un nosūtītāja iestāde informācijai, kas klasificēta *TRES SECRET UE/EU TOP SECRET* līmenī. Vajadzības gadījumā var izveidot pakārtotus reģistrus, kurā rīkojas ar šādu informāciju reģistrēšanas nolūkā.

4. Pakārtotie reģistri bez skaidras un rakstiskas centrālā *TRES SECRET UE/EU TOP SECRET* informācijas reģistra atļaujas nedrīkst *TRES SECRET UE/EU TOP SECRET* dokumentus nosūtīt ne citiem tā paša centrālā reģistra pakārtotajiem reģistriem, ne ārējiem reģistriem.

5. Izveidotie ESKI reģistri ir drošības zonas, kas definētas 3. nodaļā, un tos akreditē Komisijas Drošības akreditācijas iestāde (DAI).

28. pants

Reģistra kontrolieris

1. Katru ESKI reģistru pārvalda reģistra kontrolieris (RK).

2. RK saņem atbilstīgu drošības pielaidi.

3. RK darbu pārrauga attiecīgā Komisijas dienesta *LSO*, ciktāl tas attiecas uz noteikumu par rīcību ar ESKI dokumentiem piemērošanu un attiecīgo drošības noteikumu, standartu un pamatnostādņu ievērošanu.

4. RK tam uzticētā ESKI reģistra pārvaldības pienākumu ietvaros un saskaņā ar šo lēmumu un attiecīgajiem īstenošanas noteikumiem, standartiem un pamatnostādnēm pilda šādus vispārējus uzdevumus:

— pārvalda darbības, kas saistītas ar ESKI reģistrāciju, saglabāšanu, reproducēšanu, tulkošanu, pārraidi, nosūtīšanu un iznīcināšanu vai nodošana vēstures arhīvu dienestam,

— regulāri pārbauda vajadzību saglabāt informācijas klasifikāciju,

— uzņemas citus uzdevumus, kas saistīti ar ESKI aizsardzību un noteikti īstenošanas noteikumos.

29. pants

ESKI reģistrācija drošības nolūkā

1. Šajā lēmumā reģistrācija drošības nolūkā (turpmāk "reģistrācija") ir tādu procedūru piemērošana, kas reģistrē ESKI aprites ciklu, tostarp tā izplatīšanu.

([1]) Padomes 2003. gada 22. septembra Regula (EK, Euratom) Nr. 1700/2003, ar kuru groza Regulu (EEK, Euratom) Nr. 354/83 par Eiropas Ekonomikas kopienas un Eiropas Atomenerģijas kopienas vēsturisko arhīva materiālu nodošanu atklātībai (OV L 243, 27.9.2003., 1. lpp.).

2. Visu informāciju vai materiālus, kas klasificēti *CONFIDENTIEL UE/EU CONFIDENTIAL* un augstākā līmenī, reģistrē attiecīgos reģistros, kad organizatoriskā vienība to saņem vai nosūta.

3. Ja ar ESKI rīkojas vai to glabā, izmantojot komunikācijas un informācijas sistēmu (KIS), reģistrācijas procedūras var veikt ar procesiem, kas norisinās KIS ietvaros.

4. Sīkākus noteikumus par ESKI reģistrāciju drošības nolūkā nosaka īstenošanas noteikumos.

30. pants

ES klasificētu dokumentu kopēšana un tulkošana

1. TRÈS *SECRET UE/EU TOP SECRET* dokumentus nekopē un netulko bez autora iepriekšējas rakstiskas piekrišanas.

2. Ja *SECRET UE/EU SECRET* vai zemāka klasifikācijas līmeņa dokumenta autors nav noteicis brīdinājumus attiecībā uz minēto dokumentu kopēšanu vai tulkošanu, šādus dokumentus var kopēt vai tulkot pēc to turētāja rīkojuma.

3. Drošības pasākumi, kas piemērojami oriģināldokumentam, ir piemērojami tā kopijām un tulkojumiem.

31. pants

ESKI pārvietošana

1. ESKI pārvieto tādā veidā, lai to aizsargātu no neatļautas izpaušanas pārvietošanas laikā.

2. ESKI pārvietošanai piemēro aizsardzības pasākumus, kas:

— atbilst pārvietotās ESKI klasifikācijas līmenim un

— ir pielāgoti pārvietošanai konkrētajos apstākļos, jo īpaši atkarībā no tā, vai ESKI pārvieto:

  — Komisijas ēkas vai noslēgtas Komisijas ēku grupas iekšienē,

  — starp Komisijas ēkām, kas atrodas vienā un tajā pašā dalībvalstī,

  — Savienībā,

  — no Savienības uz kādas trešās valsts teritoriju un

  — ir pielāgoti ESKI veidam un formātam.

3. Šie aizsardzības pasākumi ir sīki izklāstīti īstenošanas noteikumos vai 42. pantā minēto projektu un programmu gadījumā kā neatņemama sastāvdaļa ir ietverti attiecīgās programmas vai projekta drošības instrukcijās (PDI).

4. Īstenošanas noteikumos vai PDI ietver ESKI līmenim atbilstošus noteikumus par:

— pārvietošanas veidu, piemēram, rokas bagāžā, ar diplomātisko vai militāro kurjeru, pārvietošana pa pastu vai ar komerciālu kurjeru,

— ESKI iepakojumu,

— tehniskiem pretpasākumiem attiecībā uz ESKI, ko pārvieto ar elektroniskiem līdzekļiem,

— citiem procesuāliem, fiziskiem vai elektroniskiem pasākumiem,

— reģistrācijas procedūrām,

— drošības atļaujas saņēmušu darbinieku izmantošanu.

5. Ja ESKI pārvieto ar elektroniskiem līdzekļiem, neatkarīgi no 21. panta 5. punkta attiecīgajos īstenošanas noteikumos paredzētos aizsardzības pasākumus var papildināt ar attiecīgiem tehniskiem pretpasākumiem, kurus apstiprina Komisijas Drošības iestāde, lai mazinātu informācijas pazaudēšanas vai apdraudējuma risku.

32. pants

ESKI iznīcināšana

1. ES klasificētos dokumentus, kas vairs nav vajadzīgi, var iznīcināt, ņemot vērā noteikumus par arhīviem un Komisijas noteikumus par dokumentu pārvaldību un arhivēšanu, jo īpaši kopējo Komisijas uzglabājamo dokumentu sarakstu.

2. ESKI, kas klasificēta *CONFIDENTIEL UE/EU CONFIDENTIAL* un augstākā līmenī, iznīcina ESKI reģistra atbildīgais RK pēc turētāja vai kompetentās iestādes rīkojuma. Par RK attiecīgi atjaunina reģistrācijas žurnālus un pārējo reģistrācijas informāciju.

3. Dokumentus, kas klasificēti *SECRET UE/EU SECRET* vai *TRES SECRET UE/EU TOP SECRET* līmenī, iznīcina RK tāda liecinieka klātbūtnē, kuram ir vismaz tāda līmeņa pielaide, kas atbilst iznīcināmā dokumenta klasifikācijas līmenim.

4. Reģistrētājs un liecinieks, ja ir vajadzīga viņa klātbūtne, paraksta iznīcināšanas apliecību, ko iekļauj reģistrā. Par ESKI reģistru atbildīgais RK glabā *TRES SECRET UE/EU TOP SECRET* dokumentu iznīcināšanas apliecības vismaz desmit gadus un *CONFIDENTIEL UE/EU CONFIDENTIAL* vai *SECRET UE/EU SECRET* dokumentu iznīcināšanas apliecības – vismaz piecus gadus.

5. Klasificētos dokumentus, tostarp tos, kas klasificēti *RESTREINT UE/EU RESTRICTED* līmenī, iznīcina ar tādām metodēm, kuras nosaka īstenošanas noteikumos un kuras atbilst attiecīgiem ES vai līdzvērtīgiem standartiem.

6. ESKI izmantotu elektronisko informācijas nesēju iznīcina saskaņā ar procedūru, ko nosaka īstenošanas noteikumos.

33. pants

ESKI iznīcināšana ārkārtas situācijās

1. Pamatojoties uz vietējiem apstākļiem, Komisijas dienesti, kuru rīcībā ir ESKI, izstrādā plānus ES klasificētu materiālu aizsardzībai krīzes gadījumos, tostarp, vajadzības gadījumā, iznīcināšanu ārkārtas gadījumos un evakuācijas plānus. Tie ietver norādījumus, kas uzskatāmi par nepieciešamiem, lai nepieļautu ESKI nokļūšanu nesankcionētu personu rīcībā.

2. *CONFIDENTIEL UE/EU CONFIDENTIAL* un *SECRET UE/EU SECRET* materiālu aizsardzības un/vai iznīcināšanas pasākumi nekādā gadījumā negatīvi neietekmē *TRES SECRET UE/EU TOP SECRET* materiāla aizsardzību vai iznīcināšanu, tostarp šifrēšanas aparatūru, kuras aizsargāšanai ir lielāka prioritāte nekā visiem citiem uzdevumiem.

3. Ārkārtas situācijā, ja pastāv nenovēršams ESKI neatļautas izpaušanas risks, ESKI turētājs to iznīcina tā, lai šo informāciju nevarētu atjaunot ne pilnīgi, ne daļēji. Autoru un izcelsmes reģistru informē par reģistrētās ESKI ārkārtas iznīcināšanu.

4. Sīkākus noteikumus par ESKI iznīcināšanu nosaka īstenošanas noteikumos.

5. NODAĻA

ES KLASIFICĒTAS INFORMĀCIJAS AIZSARDZĪBA KOMUNIKĀCIJAS UN INFORMĀCIJAS SISTĒMĀS (KIS)

34. pants

Informācijas aizsardzības pamatprincipi

1. Informācijas aizsardzība (IA) komunikācijas un informācijas sistēmu jomā ir pārliecība, ka šādas sistēmas aizsargās informāciju, kas tajā atrodas, un darbosies, kā tas ir paredzēts, kad nepieciešams un likumīgu lietotāju kontrolē.

2. Efektīva informācijas aizsardzība nodrošina atbilstīga līmeņa:

autentiskumu: garantiju, ka informācija ir īsta un saņemta no *bona fide* avotiem;

pieejamību: tai var piekļūt un to var izmantot pēc pilnvarotas iestādes pieprasījuma;

konfidencialitāti: informāciju neatklāj nesankcionētām personām, iestādēm vai procesiem;

integritāti: spēju nosargāt informācijas un aktīvu precizitāti un pilnīgumu;

neapstrīdamību: spēju pierādīt, ka darbība vai notikums ir noticis, lai vēlāk nevarētu noliegt, ka šāds notikums vai darbība ir notikusi.

3. IA pamatā ir riska pārvaldības process.

35. pants

Definīcijas

Šajā nodaļā piemēro šādas definīcijas:

a) "akreditācija" ir oficiāla atļauja un apstiprinājums, ko komunikācijas un informācijas sistēmai piešķir Drošības akreditācijas iestāde (DAI), ka tās darbības vidē var apstrādāt ESKI, pēc tam, kad ir oficiāli validēts drošības plāns un tā pareiza īstenošana;

b) "akreditācijas process" ir vajadzīgie pasākumi un uzdevumi, kas jāveic pirms Drošības akreditācijas iestāde veic akreditāciju. Šos pasākumus un uzdevumus nosaka akreditācijas procesa standartos;

c) "komunikācijas un informācijas sistēma" (KIS) ir jebkura sistēma, kas ļauj rīkoties ar informāciju elektroniskā formātā. Komunikācijas un informācijas sistēma ietver visus aktīvus, kas nepieciešami tās darbībai, tostarp infrastruktūru, personālu un informācijas resursus;

d) "atlikušais risks" ir risks, kas pastāv pēc drošības pasākumu īstenošanas, ņemot vērā to, ka ne pret visiem draudiem var cīnīties un ne visas vājās vietas var likvidēt;

e) "risks" ir iespēja, ka konkrēti draudi, izmantojot organizācijas vai kādas tās izmantotas sistēmas iekšēju vai ārēju vājo vietu, radīs kaitējumu organizācijai un tās materiālajiem un nemateriālajiem aktīviem. To izsaka kā draudu rašanās iespējamības un to ietekmes apvienojumu;

f) "riska uzņemšanās" ir lēmums, ar ko apzinās, ka pēc riska novēršanas pasākumu īstenošanas joprojām pastāv atlikušais risks;

g) "riska izvērtējums" ir draudu un vājo vietu noteikšana un attiecīgas riska analīzes veikšana, t. i., varbūtības un ietekmes analīze;

h) "informēšana par risku" ir KIS lietotāju kopienu informētības par riskiem uzlabošana, informējot apstiprināšanas iestādes par šiem riskiem un ziņojot par tiem rīcības iestādēm;

i) "riska novēršana" ir riska pavājināšana, likvidēšana, mazināšana (izmantojot atbilstīgu tehnisku, fizisku, organizatorisku vai procedūras pasākumu apvienojumu), nodošana vai uzraudzība.

36. pants

KIS rīcībai ar ESKI

1. Komunikācijas un informācijas sistēmās ar ESKI rīkojas atbilstīgi IA koncepcijai.

2. Attiecībā uz KIS, kurās rīkojas ar ESKI, atbilstība Komisijas informācijas sistēmu drošības politikai, kā minēts Komisijas Lēmumā C (2006) 3602 ([1]), nozīmē, ka:

a) informācijas sistēmu drošības politikas īstenošanai visā informācijas sistēmas aprites ciklā piemēro pieeju "plāno–dari–pārbaudi–rīkojies";

b) drošības vajadzības nosaka, izmantojot darbības ietekmes novērtējumu;

c) informācijas sistēmai un tās datiem ir jāveic oficiāla aktīvu klasifikācija;

([1]) C (2006) 3602 (2006. gada 16. augusts) par informācijas sistēmu drošību, ko izmanto Eiropas Komisija.

d) ir jāīsteno visi obligātie drošības pasākumi, kas noteikti informācijas sistēmu drošības politikā;

e) jāpiemēro riska pārvaldības process, kas ietver šādus posmus: draudu un vājo vietu apzināšana, riska novērtēšana, riska novēršana, riska uzņemšanās un informēšanas par risku;

f) tiek definēts, īstenots, pārbaudīts un pārskatīts drošības plāns, tostarp drošības politika un drošības darba procedūras.

3. Visi darbinieki, kas iesaistīti rīcībai ar ESKI paredzētu KIS plānošanā, izstrādē, testēšanā, darbībā, pārvaldībā vai izmantošanā, ziņo Drošības akreditācijas iestādei par visiem potenciāliem drošības trūkumiem, incidentiem, pārkāpumiem vai apdraudējumiem, kas var ietekmēt KIS un/vai tajā ietvertās ESKI aizsardzību.

4. Ja ESKI aizsargā ar kriptogrāfijas produktiem, tos apstiprina šādi:

a) priekšroku dod produktiem, kurus ir apstiprinājusi Padome vai Padomes ģenerālsekretārs, kas darbojas kā Padomes kriptogrāfijas apstiprinātāja iestāde, pēc Komisijas drošības ekspertu grupas ieteikuma;

b) ja tas pamatots ar konkrētiem operatīviem apsvērumiem, Komisija kriptogrāfijas apstiprinātāja iestāde (KAI) pēc Komisijas drošības ekspertu grupas ieteikuma var atbrīvot no a) punktā minētās prasības un piešķirt pagaidu apstiprinājumu uz noteiktu termiņu.

5. Pārsūtot, apstrādājot un glabājot ESKI elektroniskā veidā, izmanto apstiprinātus kriptogrāfijas produktus. Neatkarīgi no šīs prasības ārkārtas apstākļos vai īpašās tehniskās konfigurācijās var piemērot īpašas procedūras pēc tam, kad ir saņemts KAI apstiprinājums.

6. Lai aizsargātu KIS, kurās rīkojas ar informāciju, kas klasificēta *CONFIDENTIEL UE/EU CONFIDENTIAL* vai augstākā līmenī, pret šādas informācijas apdraudējumu, ko izraisa netīšas elektromagnētiskas emisijas, īsteno drošības pasākumus ("*TEMPEST* drošības pasākumi"). Šādi drošības pasākumi ir samērīgi ar ekspluatācijas risku un informācijas klasifikācijas līmeni.

7. Komisijas drošības iestāde pilda šādas funkcijas:

— IA iestāde (IAI),

— drošības akreditācijas iestāde (DAI),

— *TEMPEST* iestāde (TI),

— kriptogrāfijas apstiprinātāja iestāde (KAI),

— kriptogrāfijas produktu izplatīšanas iestāde (KPII).

8. Komisijas drošības iestāde katrai sistēmai iecelļ IA operatīvo iestādi.

9. Funkciju, kas aprakstītas 7. un 8. punktā, pienākumi tiks noteikti īstenošanas noteikumos.

37. pants

KIS akreditācija rīcībai ar ESKI

1. Visas KIS, kurās apstrādā ESKI, tiek akreditētas, pamatojoties uz ietekmes novērtējumu, kura detalizācijas pakāpei ir jābūt samērīgai ar vajadzīgo aizsardzības līmeni.

2. Akreditācijas process ietver attiecīgās KIS drošības plāna oficiālu apstiprināšanu, ko veic Komisijas DAI, lai pārliecinātos, ka:

a) riska pārvaldības process, kā minēts 36. panta 2. punktā, ir veikts pareizi;

b) sistēmas īpašnieks ir apzināti uzņēmies atlikušo risku un

c) saskaņā ar šo lēmumu ir panākts pietiekams KIS un tajā ietvertās ESKI aizsardzības līmenis.

3. Komisijas DAI izsniedz akreditācijas paziņojumu, kurā nosaka augstāko ESKI klasifikācijas līmeni, ar kādu atļauts strādāt KIS, kā arī attiecīgos darbības noteikumus un nosacījumus. Tas neskar uzdevumus, kas uzticēti Drošības akreditācijas padomei un noteikti 11. pantā Eiropas Parlamenta un Padomes Regulā (ES) Nr. 512/2014 ([1]).

4. Kopīga drošības akreditācijas padome ir atbildīga par tādu KIS akreditāciju, kurās iesaistītas vairākas puses. Tās sastāvā ir DAI pārstāvji no katras iesaistītās puses, un to vada Komisijas DAI pārstāvis.

5. Akreditācijas process ietver virkni uzdevumu, ko uzņemas iesaistītās puses. Par akreditācijas lietas un dokumentācijas sagatavošanu ir atbildīgs vienīgi KIS īpašnieks.

6. Akreditāciju veic Komisijas DAI, kura jebkurā KIS aprites cikla brīdī ir tiesīga:

a) pieprasīt piemērot akreditācijas procesu;

b) revidēt vai pārbaudīt KIS;

c) ja darbības nosacījumi vairs nav izpildīti, pieprasīt definēt un efektīvi īstenot drošības uzlabošanas plānu skaidri noteiktā termiņā, ar iespēju atsaukt KIS darbības atļauju, līdz nosacījumi atkal būs izpildīti.

7. Akreditācijas procesu izveido kā akreditācijas procesa standartu KIS, kurā rīkojas ar ESKI, un to pieņem saskaņā ar Lēmuma C (2006) 3602 10. panta 3. punktu.

38. pants

Ārkārtas apstākļi

1. Neatkarīgi no šīs nodaļas noteikumiem ārkārtas gadījumā, piemēram, gaidāmas vai iestājušās krīzes laikā, konflikta vai kara situācijā vai ārkārtas operatīvajā situācijā, var piemērot turpmāk aprakstītās īpašās procedūras.

2. Ar kompetentās iestādes piekrišanu ESKI var pārsūtīt, izmantojot kriptogrāfijas produktus, kas apstiprināti lietošanai zemākam klasifikācijas līmenim, vai nešifrētā veidā, ja kavēšanās varētu radīt kaitējumu, kas nepārprotami būtu lielāks par kaitējumu, ko radītu klasificētā materiāla izpaušana, un ja:

a) sūtītājam un saņēmējam nav vajadzīgo kriptogrāfijas iekārtu un

b) klasificēto materiālu nevar laicīgi nodot, izmantojot citus līdzekļus.

3. Klasificētā informācijā, kas nosūtīta 1. punktā izklāstītajos apstākļos, nav marķējuma vai norāžu, kas to ļautu atšķirt no neklasificētas informācijas vai informācijas, ko var aizsargāt ar pieejamu kriptogrāfijas iekārtu. Informācijas saņēmējus par tās klasifikācijas līmeni nekavējoties informē ar citiem līdzekļiem.

4. Tam seko ziņojums kompetentajai iestādei un Komisijai drošības ekspertu grupai.

6. NODAĻA

INDUSTRIĀLĀ DROŠĪBA

39. pants

Pamatprincipi

1. Industriālā drošība ir tādu ESKI aizsardzības nodrošināšanas pasākumu piemērošana:

a) klasificētu līgumu ietvaros, kurus veic:

i) kandidāti vai konkursa pretendenti visā konkursa un līguma slēgšanas procedūras laikā;

ii) līgumslēdzēji vai apakšuzņēmēji visā klasificēto līgumu aprites ciklā;

([1]) Eiropas Parlamenta un Padomes 2014. gada 16. aprīļa Regula (ES) Nr. 512/2014, ar kuru groza Regulu (ES) Nr. 912/2010, ar ko izveido Eiropas Globālās navigācijas satelītu sistēmas (GNSS) aģentūru (OV L 150, 20.5.2014., 72. lpp.).

b) klasificētu dotāciju nolīgumu ietvaros, kurus veic:

i) pieteikumu iesniedzēji dotāciju piešķiršanas procedūras laikā;

ii) saņēmēji visā klasificētā dotāciju nolīguma aprites ciklā

2. Šādi līgumi vai dotāciju nolīgumi nav saistīti ar informāciju, kas klasificēta TRÈS *SECRET UE/EU TOP SECRET* līmenī.

3. Ja vien nav noteikts citādi, šīs nodaļas noteikumus par klasificētiem līgumiem vai līgumslēdzējiem piemēro arī klasificētiem apakšlīgumiem vai apakšuzņēmējiem.

40. pants

Definīcijas

Šajā nodaļā piemēro šādas definīcijas:

a) "klasificēts līgums" ir pamatlīgums vai līgums, kas minēts Padomes Regulā (EK, Euratom) Nr. 1605/2002 ([1]), par kustamu vai nekustamu aktīvu piegādi, būvdarbu veikšanu vai pakalpojumu sniegšanu, kuru Komisija vai kāds no tās dienestiem ir noslēdzis ar līgumslēdzēju un kura izpildei ir nepieciešama vai kura izpilde ir saistīta ar ESKI izveidi, rīkošanos ar to vai ESKI glabāšanu;

b) "klasificēts apakšlīgums" ir līgums par kustamu vai nekustamu aktīvu piegādi, būvdarbu veikšanu vai pakalpojumu sniegšanu, kuru Komisijas vai kāda tās dienesta līgumslēdzējs ir noslēdzis ar citu līgumslēdzēju (t. i., apakšuzņēmēju) un kura izpildei ir nepieciešama vai kura izpilde ir saistīta ar ESKI izveidi, rīkošanos ar to vai ESKI glabāšanu;

c) "klasificēts dotāciju nolīgums" ir nolīgums, ar ko Komisijai piešķir dotāciju, kā minēts I daļas VI sadaļā Regulā (EK, Euratom) Nr. 1605/2002, kura izpildei ir nepieciešama vai kura izpilde ir saistīta ar ESKI izveidi, rīkošanos ar to vai ESKI glabāšanu;

d) "izraudzītā drošības iestāde" (IDI) ir iestāde, kas pakļauta dalībvalsts valsts drošības iestādei (VDI) un ir atbildīga par to, ka rūpniecības vai citas struktūras ir informētas par valsts politiku visā industriālās drošības jomā, kā arī par virzību un palīdzību tās īstenošanā. IDI uzdevumus var veikt VDI vai jebkura cita kompetentā iestāde.

41. pants

Procedūra attiecībā uz klasificētiem līgumiem vai dotāciju nolīgumiem

1. Ikviens Komisijas dienests kā līgumslēdzēja iestāde nodrošina, ka, piešķirot klasificētu līgumus vai dotāciju nolīgumus, šajā nodaļā izklāstītie industriālās drošības minimuma standarti ir minēti vai iekļauti līgumā.

2. Lai sasniegtu 1. punkta mērķus, Komisijas kompetentie dienesti konsultējas ar Cilvēkresursu un drošības ģenerāldirektorātu un jo īpaši ar tā Drošības direktorātu, un nodrošina, ka līgumu un apakšlīgumu paraugos un dotāciju nolīgumu paraugos ir iekļauti noteikumi, kas atspoguļo ESKI aizsardzības pamatprincipus un minimuma standartus, kas attiecīgi jāievēro līgumslēdzējiem un apakšuzņēmējiem, un dotāciju nolīgumu saņēmējiem.

3. Komisija cieši sadarbojas ar VDI, IDI un ikvienu citu attiecīgās dalībvalsts kompetento iestādi.

4. Ja līgumslēdzēja iestāde plāno uzsākt procedūru, kuras mērķis ir noslēgt klasificētu līgumu vai dotāciju nolīgumu, tā avisos procedūras posmos pspriežas ar Komisijas Drošības iestādi par jautājumiem, kas saistīti ar procedūras klasifikāciju un atsevišķiem tās klasificētiem elementiem.

5. Paraugi un modeļi klasificētiem līgumiem un apakšlīgumiem, klasificētiem dotāciju nolīgumiem, līgumu paziņojumiem, norādēm par apstākļiem, kad ir nepieciešama iekārtas drošības pielaide (IDP), programmām vai projekta drošības instrukcijām (PDI), drošības aspektu vēstulēm (DAV), apmeklējumiem, ESKI pārsūtīšanai un pārvietošanai saskaņā ar klasificētu līgumu vai klasificētu dotāciju nolīgumu, pēc apspriešanās ar Komisijas drošības ekspertu grupu tiek izklāstīti īstenošanas noteikumos par industriālo drošību.

([1]) Padomes 2002. gada 25. jūnija Regula (EK, Euratom) Nr. 1605/2002 par Finanšu regulu, ko piemēro Eiropas Kopienu vispārējam budžetam (OV L 248, 16.9.2002., 1. lpp.).

6. Komisijas var noslēgt klasificētu līgumu vai dotāciju nolīgumu, ar ko uztic uzdevumus, kas ietver vai ir saistīti ar piekļuvi ESKI, rīkošanos ar to vai ESKI glabāšanu, ko veic ekonomikas dalībnieki, kas reģistrēti dalībvalstī vai trešā valstī, kura noslēgusi nolīgumu vai administratīvu vienošanos saskaņā ar šā lēmuma 7. nodaļu.

42. pants

Drošības elementi klasificētā līgumā vai dotāciju nolīgumā

1. Klasificētā līgumā vai dotāciju nolīgumā iekļauj šādus drošības elementus.

Programmas vai projekta drošības instrukcijas

a) "Programmas vai projekta drošības instrukcija" (PDI) ir to drošības procedūru saraksts, kuras piemēro konkrētai programmai vai projektam, lai standartizētu drošības procedūras. To var pārskatīt visā programmas vai projekta darbības laikā.

b) Cilvēkresursu un drošības ģenerāldirektorāts izstrādā vispārīgu PDI, un Komisijas dienesti, kas atbild par programmām vai projektiem, kuri saistīti ar ESKI glabāšanu vai rīkošanos ar to, attiecīgā gadījumā var izstrādāt speciālu PDI, kas balstās uz vispārīgo PDI.

c) Speciālo PDI jo īpaši izstrādā programmām un projektiem, ko raksturo ievērojams apjoms, mērogs vai sarežģītība, vai daudzi un/vai dažādi līgumslēdzēji, saņēmēji un citi partneri un iesaistītās ieinteresētās personas, piemēram, attiecībā uz viņu juridisko statusu. Speciālo PDI izstrādā Komisijas dienests(-i), kas pārvalda programmu vai projektu, ciešā sadarbībā ar Cilvēkresursu un drošības ģenerāldirektorātu.

d) Cilvēkresursu un drošības ģenerāldirektorāts iesniedz gan vispārīgo, gan speciālo PDI Komisijas drošības ekspertu grupai, lai saņemtu konsultāciju.

Drošības aspektu vēstule

a) "Drošības aspektu vēstule" (DAV) ir līgumslēdzējas iestādes izdots īpašu līguma nosacījumu kopums, kas ir tāda klasificēta līguma neatņemama sastāvdaļa, kurš saistīts ar piekļuvi ESKI vai ar ESKI izveidi, un kurā identificē drošības prasības un tos līguma elementus, kam vajadzīga drošības aizsardzība.

b) Ar attiecīgo līgumu saistītās drošības prasības izklāsta drošības aspektu vēstulē (DAV). Attiecīgā gadījumā DAV iekļauj Drošības klasifikācijas rokasgrāmatu (DKK), un tā ir neatņemama klasificēta līguma vai apakšlīguma sastāvdaļa.

c) DAV iekļauj noteikumus par to, ka līgumslēdzējam vai saņēmējam ir jāievēro šajā lēmumā ietvertie minimuma standarti. Līgumslēdzēja iestāde nodrošina, ka DAV ir norādīts, ka šo minimuma standartu neievērošana var būt pietiekams pamats līguma vai dotāciju nolīguma izbeigšanai.

2. Gan PDI, gan DAV obligāts drošības elements ir DKK:

a) "drošības klasifikācijas rokasgrāmata" (DKK) ir dokuments, kurā raksturotas programmas, līguma vai dotāciju nolīguma klasificētās sastāvdaļas, norādot piemērojamos drošības klasifikācijas līmeņus. DKK var papildināt visā programmas, līguma vai dotāciju nolīguma darbības laikā, turklāt informācijas sastāvdaļas var pārklasificēt vai pazemināt to klasifikācijas līmeni; ja pastāv DKK, tā ir DAV sastāvdaļa.

b) Pirms izsludināt konkursu vai pirms piešķirt klasificētu līgumu, Komisijas dienests kā līgumslēdzēja iestāde nosaka tās informācijas drošības klasifikāciju, kuru sniedz kandidātiem un pretendentiem vai līgumslēdzējiem, kā arī tās informācijas drošības klasifikāciju, ko izveidos līgumslēdzējs. Šajā nolūkā tas saskaņā ar šo lēmumu un tā īstenošanas noteikumiem un pēc apspriešanās ar Komisijas Drošības iestādi sagatavo drošības klasifikācijas rokasgrāmatu (DKK), kas jāizmanto līguma izpildei.

c) Lai noteiktu dažādu klasificēta līguma elementu drošības klasifikāciju, piemēro šādus principus:

i) izstrādājot DKK, Komisijas dienests kā līgumslēdzēja iestāde ņem vērā visus attiecīgos drošības aspektus, tostarp drošības klasifikāciju, ko informācijas autors piešķīris informācijai, kas paredzēta un apstiprināta izmantošanai līgumā;

ii) līguma klasifikācijas kopējais līmenis nedrīkst būt zemāks par jebkuras tā sastāvdaļas augstāko klasifikācijas līmeni; un

iii) vajadzības gadījumā līgumslēdzēja iestāde ar Komisijas Drošības iestādes starpniecību sadarbojas ar dalībvalstu VDI, IDI vai jebkuru citu iesaistīto kompetento drošības iestādi, ja mainās tādas informācijas klasifikācija, ko līgumslēdzēji izveidojuši vai kas tiem sniegta līguma izpildei, un ja jāveic attiecīgas izmaiņas DKK.

43. pants

Līgumslēdzēju un saņēmēju darbinieku piekļuve ESKI

Līgumslēdzējas vai piešķīrējas iestādes nodrošina, ka klasificētā līgumā vai klasificētā dotācijas nolīgumā ietver noteikumus, kuros norādīts, ka līgumslēdzēja, apakšuzņēmēja vai saņēmēja darbiniekiem, kuriem, izpildot klasificētu līgumu, apakšlīgumu vai dotāciju nolīgumu, ir vajadzīga piekļuve ESKI, šādu piekļuvi piešķir tikai tad, ja:

a) darbinieks ir saņēmis attiecīga līmeņa drošības atļauju vai citādā veidā ir pienācīgi pilnvarots un ir noskaidrota viņa vajadzība pēc informācijas;

b) darbinieks ir iepazīstināts ar ESKI aizsardzībai piemērojamiem drošības noteikumiem un ir apliecinājis savus pienākumus saistībā ar šādas informācijas aizsargāšanu;

c) darbiniekiem ir attiecīgas VDI, IDI vai citas kompetentas iestādes izsniegta atbilstīga līmeņa drošības pielaide attiecībā uz informāciju, kas klasificēta *CONFIDENTIEL UE/EU CONFIDENTIAL* vai *SECRET UE/EU SECRET* līmenī.

44. pants

Iestādes drošības pielaide

1. "Iestādes drošības pielaide" (IDP) ir administratīvs atzinums, ko izsniedz VDI, IDI vai cita kompetenta drošības iestāde par to, ka no drošības viedokļa iestāde var nodrošināt ESKI piešķirtajam drošības klasifikācijas līmenim atbilstošu aizsardzības līmeni

2. IDP piešķir dalībvalsts VDI vai IDI, vai jebkura cita dalībvalsts kompetentā drošības iestāde, lai atbilstīgi valsts normatīvajiem aktiem apliecinātu, ka ekonomikas dalībnieks var nodrošināt pietiekamu ESKI aizsardzību attiecīgā klasifikācijas līmenī (*CONFIDENTIEL UE/EU CONFIDENTIAL* vai *SECRET UE/EU SECRET*) savās telpās; šādu IDP iesniedz Komisijai Drošības iestādei, kas to pārsūta Komisijas dienestam, kas darbojas kā līgumslēdzējas vai piešķīrēja iestāde, pirms kandidāts, pretendents vai līgumslēdzējs vai dotācijas pieteikuma iesniedzējs vai saņēmējs var saņemt piekļuvi ESKI.

3. Ja vajadzīgs, līgumslēdzēja iestāde ar Komisijas Drošības iestādes starpniecību paziņo attiecīgajai VDI, IDI vai jebkurai citai kompetentajai drošības iestādei, ka līguma izpildīšanai ir vajadzīga IDP. Ja iepirkuma procedūras vai dotāciju piešķiršanas procedūras gaitā ir jāsniedz piekļuve ESKI, kas klasificēta *CONFIDENTIEL UE/EU CONFIDENTIAL* vai *SECRET UE/EU SECRET* līmenī, pieprasa uzrādīt IDP vai PDP.

4. Līgumslēdzēja iestāde vai piešķīrēja iestāde piešķir klasificētu līgumu vai dotāciju nolīgumu izraudzītajam pretendentam vai dalībniekam tikai tad, kad saņemts tās dalībvalsts VDI, IDI vai kādas citas kompetentās drošības iestādes apstiprinājums, kurā reģistrēti iesaistītie līgumslēdzēji vai apakšuzņēmēji, ka viņiem ir izsniegta atbilstīga IDP, ja tas vajadzīgs.

5. Ja VDI, IDI vai cita kompetenta drošības iestāde, kas ir izdevusi IDP paziņo Komisijas Drošības iestādei par izmaiņām, kas ietekmē IDP, tā informē Komisijas dienestu, kas darbojas kā līgumslēdzēja vai piešķīrēja iestāde. Apakšlīguma gadījumā attiecīgi informē VDI, IDI vai citu kompetento drošības iestādi.

6. Ja attiecīgā VDI, IDI vai kāda cita kompetentā drošības iestāde atsauc IDP, tas ir pietiekams pamats līgumslēdzējai vai piešķīrējai iestādei izbeigt klasificētu līgumu vai izslēgt attiecīgo kandidātu, pretendentu vai pieteikuma iesniedzēju no konkursa. Šāda veida noteikumu iekļauj līgumu un dotāciju nolīgumu paraugos.

45. pants

Noteikumi par klasificētiem līgumiem un dotāciju nolīgumiem

1. Ja kandidātam, pretendentam vai pieteikuma iesniedzējam nodod ESKI jau iepirkuma procedūras laikā, uzaicinājumā iesniegt piedāvājumus vai uzaicinājumā iesniegt priekšlikumus iekļauj prasību, ka kandidātam, pretendentam vai pieteikuma iesniedzējam, kurš neiesniedz piedāvājumu vai kuru neizvēlas, noteiktā termiņā ir jāatdod atpakaļ visi klasificētie dokumenti.

2. Līgumslēdzēja vai piešķīrēja iestāde paziņo, izmantojot Komisijas Drošības iestādi, kompetentajai VDI, IDI vai jebkurai citai kompetentai drošības iestādei, ka klasificēts līgums vai dotāciju nolīgums ir piešķirts, un attiecīgos datus, piemēram, līgumslēdzēja(-u) vai saņēmēja vārdu, uzvārdu/nosaukumu, līguma termiņu un maksimālo klasifikācijas līmeni.

3. Ja šādu līgumu vai dotāciju nolīgumu izbeidz, līgumslēdzēja vai piešķīrēja iestāde nekavējoties ar Komisijas Drošības iestādes starpniecību to paziņo tās dalībvalsts VDI, IDI vai jebkurai citai kompetentai drošības iestādei, kurā līgumslēdzējs vai dotācijas saņēmējs ir reģistrēts.

4. Klasificēta līguma vai dotāciju nolīguma, vai dotācijas saņēmēja līdzdalības izbeigšanas gadījumā līgumslēdzējs vai dotācijas saņēmējam parasti ir pienākums atdot atpakaļ līgumslēdzējai vai piešķīrējai iestādei visu viņu rīcībā esošo ESKI.

5. Drošības aspektu vēstulē nosaka īpašus noteikumus par ESKI iznīcināšanu klasificēta līguma vai klasificēta dotāciju nolīguma darbības laikā vai pēc tā izbeigšanas.

6. Ja līgumslēdzējam vai dotācijas saņēmējam ir atļauts saglabāt ESKI pēc klasificēta līguma vai klasificēta dotāciju nolīguma darbības beigām, līgumslēdzējs vai dotācijas saņēmējs turpina ievērot šajā lēmumā noteiktos minimuma standartus un aizsargāt ESKI konfidencialitāti.

46. pants

Īpaši noteikumi par klasificētiem līgumiem

1. Nosacījumus par ESKI aizsardzību, saskaņā ar kuriem līgumslēdzējs var slēgt apakšlīgumu, definē gan uzaicinājumā iesniegt pieteikumus, gan klasificētajā līgumā.

2. Pirms līgumslēdzējs atsevišķas klasificēta līguma daļas nodod apakšuzņēmējam, tas saņem līgumslēdzējas iestādes atļauju. Apakšlīgumu, kas saistīts ar piekļuvi ESKI, nevar slēgt ar apakšuzņēmēju, kas reģistrēts trešā valstī, izņemto, ja pastāv tiesiskais regulējums attiecībā uz informācijas drošību, kā noteikts 7. nodaļā.

3. Līgumslēdzējs ir atbildīgs par to, lai visas apakšlīguma darbības tiktu veiktas saskaņā ar šajā lēmumā noteiktajiem minimuma standartiem un sniedz ESKI apakšuzņēmējam tikai ar iepriekšēju līgumslēdzējas iestādes rakstisku piekrišanu.

4. Attiecībā uz ESKI, ko izveido vai ar ko rīkojas līgumslēdzējs, par tās autoru uzskata Komisiju, un autoram paredzētās tiesības īsteno līgumslēdzēja iestāde.

47. pants

Ar klasificētiem līgumiem saistīti apmeklējumi

1. Ja Komisijas vai līgumslēdzēja, vai dotācijas saņēmēja darbiniekam nepieciešama piekļuve informācijai, kas klasificēta *CONFIDENTIEL UE/EU CONFIDENTIAL* vai *SECRET UE/EU SECRET* līmenī, vienam otra telpās klasificēta līguma vai dotāciju nolīguma izpildei, apmeklējumus organizē sadarbībā ar VDI, IDI vai jebkuru citu attiecīgo kompetento drošības iestādi. Par šādiem apmeklējumiem informē Komisijas Drošības iestādi. Tomēr konkrētu programmu vai projektu gadījumā VDI, IDI vai cita kompetentā drošības iestāde var piekrist procedūrai, saskaņā ar kuru šādus apmeklējumus var organizēt tieši.

2. Visiem apmeklētājiem ir attiecīgā drošības pielaide, un tie atbilst vajadzības pēc informācijas principam attiecībā uz piekļuvi ESKI, kas saistīta ar klasificēto līgumu.

3. Apmeklētājiem nodrošina piekļuvi tikai tai ESKI, kura saistīta ar apmeklējuma mērķi.

4. Sīkāk izstrādāti noteikumi ir izklāstīti īstenošanas noteikumos.

5. Šajā lēmumā un 4. punktā minētajos īstenošanas noteikumos paredzēto noteikumu par apmeklējumiem saistībā ar klasificētiem līgumiem ievērošana ir obligāta.

48. pants

ESKI nosūtīšana un pārvietošana saistībā ar klasificētiem līgumiem vai klasificētiem dotāciju nolīgumiem

1. Attiecībā uz ESKI elektronisku nosūtīšanu piemēro šā lēmuma 5. nodaļas attiecīgos noteikumus.

2. Attiecībā uz ESKI pārvietošanu saskaņā ar valsts normatīvajiem aktiem piemēro šā lēmuma 4. nodaļas noteikumus un šā lēmuma īstenošanas noteikumus.

3. Nosakot drošības pasākumus klasificēto materiālu pārvietošanai ar kravu pārvadājumiem, piemēro šādus principus:

a) drošību garantē visos transportēšanas posmos, sākot ar nosūtīšanas vietu līdz galamērķim;

b) sūtījumam piešķirto drošības līmeni nosaka augstākais iekļauto materiālu klasifikācijas līmenis;

c) pirms materiālu, kas klasificēts *CONFIDENTIEL UE/EU CONFIDENTIAL* vai *SECRET UE/EU SECRET* līmenī, pārvieto pāri robežām, sūtītājs sagatavo transportēšanas plānu un iesaistītā VDI, IDI vai kāda cita attiecīgā kompetentā drošības iestāde to apstiprina;

d) maršruti, cik vien iespējams, ir tieši no izcelsmes vietas līdz galamērķim, un tos veic tik ātri, cik apstākļi pieļauj;

e) ja iespējams, maršruti ved tikai caur dalībvalstīm. Maršruti caur valstīm, kas nav dalībvalstis, būtu jāizvēlas tikai tad, kad ir saņemta atļauja gan no sūtītāja, gan no saņēmēja dalībvalsts VDI, IDI vai kādas citas attiecīgās kompetentās drošības iestādes.

49. pants

ESKI pārsūtīšana līgumslēdzējiem vai dotāciju saņēmējiem trešās valstīs

ESKI tiek pārsūtīta līgumslēdzējiem vai dotāciju saņēmējiem, kas atrodas trešās valstīs, atbilstīgi drošības pasākumiem, par kuriem vienojusies Komisijas Drošības iestāde, Komisijas dienests, kas ir līgumslēdzēja vai piešķīrēja iestāde, un tās trešās valsts VDI, IDI vai cita kompetentā drošības iestāde, kurā līgumslēdzējs vai dotācijas saņēmējs ir reģistrēts.

50. pants

Rīkošanās ar informāciju, kas klasificēta *RESTREINT UE/EU RESTRICTED* līmenī, saistībā ar klasificētiem līgumiem vai klasificētiem dotāciju nolīgumiem

1. Informācijas, kas klasificēta *RESTREINT UE/EU RESTRICTED* līmenī, aizsardzība, ja ar to rīkojas vai to glabā saskaņā ar klasificētu līgumu vai dotāciju nolīgumu, pamatojas uz proporcionalitātes un izmaksu efektivitātes principu.

2. IDP vai PDP nav vajadzīga saistībā ar klasificētiem līgumiem vai klasificētiem dotāciju nolīgumiem, kas ietver rīkošanos ar informāciju, kas klasificēta *RESTREINT UE/EU RESTRICTED* līmenī.

3. Ja līgums vai dotāciju nolīgums ietver rīkošanos ar informāciju, kas klasificēta *RESTREINT UE/EU RESTRICTED* līmenī, līgumslēdzēja vai dotāciju saņēmēja izmantotās komunikācijas un informācijas sistēmās, līgumslēdzēja vai piešķīrēja iestāde, apspriedusies ar Komisijas Drošības iestādi, nodrošina, ka līgumā vai dotāciju nolīgumā ir noteiktas nepieciešamās tehniskās un administratīvās prasības attiecībā uz KIS akreditāciju, kas ir samērīgas ar novērtēto risku, ņemot vērā visus atbilstīgos faktorus. Komisijas Drošības iestāde un attiecīgā VDI vai IDI savstarpēji vienojas par šādas KIS akreditācijas vai apstiprinājuma apjomu.

7. NODAĻA

KLASIFICĒTAS INFORMĀCIJAS APMAIŅU AR CITĀM SAVIENĪBAS IESTĀDĒM, AĢENTŪRĀM, STRUKTŪRĀM UN BIROJIEM, AR DALĪBVALSTĪM UN AR TREŠĀM VALSTĪM UN STARPTAUTISKĀM ORGANIZĀCIJĀM

51. pants

Pamatprincipi

1. Ja Komisija vai viens no tās dienestiem konstatē, ka ir vajadzīga ESKI apmaiņa ar citu Savienības iestādi, aģentūru, struktūru vai biroju, vai ar trešo valsti vai starptautisku organizāciju, veic visu nepieciešamo, lai šim nolūkam izveidotu atbilstošu tiesisko vai administratīvo regulējumu, kas var ietvert informācijas drošības nolīgumus vai administratīvās vienošanās, ko noslēdz saskaņā ar attiecīgajiem noteikumiem.

2. Neskarot 57. pantu, ESKI apmaiņa ar citu Savienības iestādi, aģentūru, struktūru vai biroju vai ar trešo valsti vai starptautisku organizāciju notiek tikai tad, ja ir izveidots un darbojas šāds atbilstošs tiesiskais vai administratīvais regulējums un ir pietiekamas garantijas, ka Savienības iestāde, aģentūra, struktūra vai birojs vai trešā valsts, vai attiecīgā starptautiskā organizācija piemēro līdzvērtīgus pamatprincipus un minimuma standartus klasificētas informācijas aizsardzībai.

52. pants

ESKI apmaiņu ar citām Savienības iestādēm, aģentūrām, struktūrām un birojiem

1. Pirms noslēgt administratīvu vienošanos par ESKI apmaiņu ar citu Savienības iestādi, aģentūru, struktūru vai biroju, Komisija pārliecinās, ka attiecīgā Savienības iestāde, aģentūra, struktūra vai birojs:

a) ir izveidojusi tiesisko regulējumu ESKI aizsardzībai, kas nosaka pamatprincipus un minimuma standartus, kas ir līdzvērtīgi tiem, kas paredzēti šajā lēmumā un tā īstenošanas noteikumos;

b) piemēro drošības standartus un pamatnostādnes par darbinieku drošību, fizisko drošību, ESKI pārvaldību un komunikācijas un informācijas sistēmu (KIS) drošību, kas garantē līdzvērtīgu ESKI aizsardzības līmeni tam, kādu nodrošina Komisija;

c) marķē tās izveidoto klasificēto informāciju kā ESKI.

2. Cilvēkresursu un drošības ģenerāldirektorāts ciešā sadarbībā ar citiem kompetentajiem Komisijas dienestiem ir galvenais dienests Komisijā, kas noslēdz administratīvas vienošanās par ESKI apmaiņu ar citām Savienības iestādēm, aģentūrām, struktūrām vai birojiem.

3. Administratīvās vienošanās parasti noslēdz vēstuļu apmaiņas veidā, ko Komisijas vārdā paraksta Cilvēkresursu un drošības ĢD ģenerāldirektors.

4. Pirms noslēgt administratīvu vienošanos par ESKI apmaiņu, Komisijas Drošības iestāde dodas novērtējuma apmeklējumā, lai novērtētu ESKI aizsardzības tiesisko regulējumu un pārliecinātos par ESKI aizsardzībai īstenoto pasākumu efektivitāti. Administratīvā vienošanās stājas spēkā un ESKI apmaiņa notiek tikai tad, ja šā novērtējuma rezultāts ir apmierinošs un pēc apmeklējuma izteiktie ieteikumi ir ņemti vērā. Lai pārbaudītu, vai administratīvā vienošanās tiek ievērota un vai drošības pasākumi joprojām atbilst pamatprincipiem un minimuma standartiem, par kuriem panākta vienošanās, regulāri veic atkārtotus novērtējuma apmeklējumus.

5. Komisijā ESKI reģistrs, ko pārvalda Ģenerālsekretariāts, parasti ir galvenais ieejas un izejas punkts, caur kuru notiek klasificētas informācijas apmaiņa ar citām Savienības iestādēm, aģentūrām, struktūrām un birojiem. Tomēr, ja, ņemot vērā drošības, organizatoriskos vai operatīvos apsvērumus, tas ir piemērotāk, lai aizsargātu ESKI, ieejas un izejas punkti, caur kuriem notiek klasificētas informācijas apmaiņa attiecīgo Komisijas dienestu kompetences ietvaros, ir vietējie ESKI reģistri, kas izveidoti Komisijas dienestos saskaņā ar šo lēmumu un tā īstenošanas noteikumiem.

6. Komisijas drošības ekspertu grupu informē par administratīvo vienošanos noslēgšanu saskaņā ar 2. punktu.

53. pants

ES klasificētas informācijas apmaiņa ar dalībvalstīm

1. ESKI apmaiņa ar dalībvalstīm un tās nodošana dalībvalstīm var notikt tikai ar nosacījumu, ka tās aizsargā šo informāciju saskaņā ar prasībām, kas piemērojamas līdzvērtīga valsts drošības klasifikācijas līmeņa klasificētai informācijai, kā tas izklāstīts drošības klasifikāciju līdzvērtības tabulā I pielikumā.

2. Ja dalībvalstis Eiropas Savienības struktūrās vai tīklos ievieš klasificētu informāciju, kam piemērots valsts drošības klasifikācijas marķējums, Komisija aizsargā šo informāciju saskaņā ar prasībām, kas attiecas uz līdzvērtīga līmeņa ESKI, kā tas izklāstīts I pielikumā paredzētajā drošības klasifikāciju atbilsmju tabulā.

54. pants

ESKI apmaiņa ar trešām valstīm un starptautiskām organizācijām

1. Ja Komisija konstatē, ka tai ir ilgtermiņa vajadzība apmainīties ar klasificētu informāciju ar trešām valstīm vai starptautiskām organizācijām, tiek veikts viss nepieciešamais, lai šim nolūkam izveidotu atbilstošu tiesisko vai administratīvo regulējumu, kas var ietvert informācijas drošības nolīgumus vai administratīvās vienošanās, ko noslēdz saskaņā ar attiecīgajiem noteikumiem.

2. Šā panta 1. punktā minētie informācijas drošības nolīgumi un administratīvās vienošanās ietver noteikumus, kas nodrošina, ka gadījumos, kad trešās valstis vai starptautiskās organizācijas saņem ESKI, šai informācijai nodrošina tādu aizsardzību, kas atbilst tās klasifikācijas līmenim un saskaņā ar minimuma standartiem, kuri ir līdzvērtīgi šajā lēmumā paredzētajiem.

3. Komisijas var noslēgt administratīvu vienošanos saskaņā ar 56. pantu, ja ESKI klasifikācijas līmenis parasti nav augstāks par *RESTREINT UE/EU RESTRICTED*.

4. Šā panta 3. punktā minētās administratīvās vienošanās ietver noteikumus, kas nodrošina, ka gadījumos, kad trešās valstis vai starptautiskās organizācijas saņem ESKI, šai informācijai nodrošina tādu aizsardzību, kas atbilst tās klasifikācijas līmenim, un saskaņā ar minimuma standartiem, kuri ir līdzvērtīgi šajā lēmumā paredzētajiem. Par informācijas drošības nolīgumu vai administratīvo vienošanos noslēgšanu konsultējas ar Komisijas drošības ekspertu grupu.

5. Lēmumu Komisijā sagatavotu ESKI nodot trešai valstij vai starptautiskai organizācijai pieņem Komisijas dienests, kas ir ESKI autors Komisijā, izskatot katru gadījumu atsevišķi un atbilstīgi šādas informācijas būtībai un saturam, saņēmēja vajadzībai pēc informācijas un tam, kādu labumu no nodošanas gūst Savienība. Ja Komisija nav tās klasificētās informācijas vai informāciju saturošo materiālu autors, kuru nodošana ir vēlama, Komisijas dienests, kura rīcībā ir klasificētā informācija, vispirms lūdz rakstisku autora piekrišanu nodošanai. Ja autoru nevar noteikt, Komisija dienests, kura rīcībā ir šī klasificētā informācija, uzņemas autora atbildību pēc apspriešanās ar Komisiju drošības ekspertu grupu.

55. pants

Informācijas drošības nolīgumi

1. Informācijas drošības nolīgumus ar trešām valstīm vai starptautiskajām organizācijām slēdz saskaņā ar LESD 218. pantu.

2. Informācijas drošības nolīgumos:

a) paredz pamatprincipus un minimuma standartus, ar ko reglamentē klasificētas informācijas apmaiņu starp Savienību un trešo valsti vai starptautisku organizāciju;

b) nosaka arī tehniskos īstenošanas pasākumus, par kuriem jāvienojas attiecīgo Savienības iestāžu un struktūru kompetentajām drošības iestādēm un trešās valsts vai attiecīgās starptautiskās organizācijas kompetentajai drošības iestādei. Šādos pasākumos ņem vērā aizsardzības līmeni, ko nodrošina trešās valsts vai attiecīgās starptautiskās organizācijas drošības noteikumi, struktūras un procedūras;

c) paredz, ka pirms attiecīgajā līgumā paredzētās klasificētās informācijas apmaiņas ir jāpārliecinās, ka saņemošā puse ir spējīga atbilstīgā veidā aizsargāt klasificētu informāciju, kas tai nodota.

3. Ja saskaņā ar 51. panta 1. punktu ir konstatēta nepieciešamība apmainīties ar klasificētu informāciju, Komisija attiecīgā gadījumā apspriežas ar Eiropas Ārējās darbības dienestu, Padomes Ģenerālsekretariātu un citām Savienības iestādēm un struktūrām, lai noteiktu, vai būtu jāiesniedz ieteikums saskaņā ar LESD 218. panta 3. punktu.

4. ESKI elektronisku apmaiņu atļauts veikt tikai tad, ja tas skaidri noteikts informācijas drošības nolīgumā vai tehniskajos īstenošanas pasākumos.

5. Komisijā ESKI reģistrs, ko pārvalda Ģenerālsekretariāts, parasti ir galvenais ieejas un izejas punkts, caur kuru notiek informācijas apmaiņa ar trešām valstīm un starptautiskām organizācijām. Tomēr, ja, ņemot vērā drošības, organizatoriskos vai operatīvos apsvērumus, tas ir piemērotāk, lai aizsargātu ESKI, ieejas un izejas punkti, caur kuriem notiek klasificētas informācijas apmaiņa attiecīgo Komisijas dienestu kompetences ietvaros, ir vietējie ESKI reģistri, kas izveidoti Komisijas dienestos saskaņā ar šo lēmumu un tā īstenošanas noteikumiem.

6. Lai izvērtētu attiecīgo trešās valsts vai attiecīgās starptautiskās organizācijas drošības noteikumu, struktūru un procedūru efektivitāti, Komisija sadarbībā ar citām Savienības iestādēm, aģentūrām vai struktūrām piedalās novērtējuma apmeklējumos, savstarpēji vienojoties ar attiecīgo trešo valsti vai starptautisko organizāciju. Minētajos novērtējuma apmeklējumos izvērtē:

a) regulējumu, ko piemēro klasificētas informācijas aizsardzībai;

b) drošības politikas īpašos rādītājus un veidu, kā organizē drošību trešā valstī vai starptautiskā organizācijā, kas varētu ietekmēt tādas klasificētas informācijas līmeni, ar kuru var apmainīties;

c) spēkā esošos drošības pasākumus un procedūras un

d) drošības pielaides procedūras, ko piemēro tāda līmeņa ESKI, ko paredzēts nodot.

56. pants

Administratīvie pasākumi

1. Ja Savienības politiskā vai tiesiskā regulējuma kontekstā pastāv ilgtermiņa vajadzība organizēt tādas klasificētas informācijas apmaiņu ar trešo valsti vai starptautisku organizāciju, kura parasti nav klasificēta augstākā līmenī kā *RESTREINT UE/EU RESTRICTED*, un ja Komisijas Drošības iestāde pēc apspriešanās ar Komisijas drošības ekspertu grupu jo īpaši ir konstatējusi, ka iesaistītajai pusei nav pietiekami attīstītas drošības sistēmas, lai tā varētu noslēgt informācijas drošības nolīgumu, Komisija var nolemt slēgt administratīvu vienošanos ar attiecīgās trešās valsts vai starptautiskās organizācijas iestādēm.

2. Šādas administratīvas vienošanās parasti slēdz vēstuļu apmaiņas veidā.

3. Pirms vienošanās noslēgšanas veic novērtējuma apmeklējumu. Komisijas drošības ekspertu grupu informē par novērtējuma apmeklējuma rezultātiem. Taču, ja pastāv ārkārtas iemesli klasificētas informācijas steidzamai apmaiņai, ESKI var nodot, ja tiek darīts viss iespējamais, lai minēto izvērtējuma apmeklējumu veiktu pēc iespējas drīz.

4. ESKI elektronisku apmaiņu atļauts veikt tikai tad, ja tas ir skaidri noteikts administratīvās vienošanās tekstā.

57. pants

ESKI ārkārtas un *ad hoc* nodošana

1. Ja nav noslēgts ne informācijas drošības nolīgums, ne administratīva vienošanās un ja Komisija vai viens no tās dienestiem konstatē, ka Savienības politiskā un tiesiskā regulējuma kontekstā pastāv ārkārtas nepieciešamība nodot ESKI trešai valstij vai starptautiskai organizācijai, Komisijas Drošības iestāde kopā ar attiecīgās trešās valsts vai starptautiskās organizācijas drošības iestādēm pēc iespējas pārbauda, vai tās drošības noteikumi, struktūras un procedūras ir tādas, ka ESKI, ko tai nodos, būs aizsargāta pēc standartiem, kas nav mazāk stingri par šajā lēmumā paredzētajiem.

2. Lēmumu nodot ESKI attiecīgai trešai valstij vai starptautiskai organizācijai pēc apspriešanās ar Komisijas Drošības ekspertu grupu pieņem Komisija, pamatojoties uz priekšlikumu, ko iesniedz Komisijas loceklis, kas atbild par drošības jautājumiem.

3. Saskaņā ar Komisijas lēmumu nodot ESKI un tikai ar iepriekšēju rakstisku autora, tostarp tajā ietverto izejmateriālu autoru, piekrišanu, kompetentais Komisijas dienests nosūta attiecīgo informāciju, kurai ir nodošanas marķējums, kas norāda to trešo valsti vai starptautisko organizāciju, kurai tā ir nodota. Pirms vai faktiskās nodošanas laikā attiecīgā trešā puse rakstiski apņemas aizsargāt saņemto ESKI saskaņā ar šajā lēmumā izklāstītajiem pamatprincipiem un minimuma standartiem.

8. NODAĻA

NOBEIGUMA NOTEIKUMI

58. pants

Iepriekšējā lēmuma aizstāšana

Ar šo lēmumu atceļ un aizstāj Komisijas Lēmumu 2001/844/EK, EOTK, Euratom ([1]).

59. pants

Klasificēta informācija, kas izveidota pirms šā lēmuma stāšanās spēkā

1. Visu ESKI, kas klasificēta atbilstīgi Lēmumam 2001/844/EK, EOTK, Euratom turpina aizsargāt saskaņā ar šā lēmuma noteikumiem.

2. Visu klasificēto informāciju, kas bija Komisijas rīcībā dienā, kad stājās spēkā Komisijas Lēmums 2001/844/EK, EOTK, Euratom, izņemot Euratom klasificēto informāciju:

a) ja to ir izveidojusi Komisija, turpina uzskatīt par pārklasificētu par *RESTREINT UE* pēc noklusējuma, ja vien tās autors līdz 2002. gada 31. janvārim nav piešķīris tai citu klasifikāciju un informējis visus attiecīgā dokumenta adresātus;

b) ja to ir izveidojuši autori ārpus Komisijas, saglabā tās sākotnējo klasifikāciju un tādējādi ar to rīkojas kā ar līdzvērtīga līmeņa ESKI, izņemot, ja autors piekrīt informāciju deklasificēt vai pazemināt tās klasifikācijas līmeni.

60. pants

Īstenošanas noteikumi un drošības paziņojumi

1. Ja nepieciešams pieņemt šā lēmuma īstenošanas noteikumus, par to, pilnībā ievērojot iekšējo reglamentu, pieņems atsevišķu Komisijas pilnvarojošo lēmumu tam Komisijas loceklim, kas ir atbildīgs par drošības jautājumiem.

2. Kad saskaņā ar iepriekš minēto Komisijas lēmumu saņemts pilnvarojums, Komisijas loceklis, kas ir atbildīgs par drošības jautājumiem, var izstrādāt drošības paziņojumus, kuros izklāstītas drošības pamatnostādnes un paraugprakse šā lēmuma un tā īstenošanas noteikumu piemērošanas jomā.

3. Komisija var deleģēt uzdevumus, kas minēti šā panta pirmajā un otrajā punktā, Cilvēkresursu un drošības ĢD ģenerāldirektoram ar atsevišķu deleģēšanas lēmumu, pilnībā ievērojot iekšējo reglamentu.

61. pants

Stāšanās spēkā

Šī regula stājas spēkā nākamajā dienā pēc tās publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī*.

Briselē, 2015. gada 13. martā

Komisijas vārdā –

priekšsēdētājs

Jean-Claude JUNCKER

([1]) Komisijas 2001. gada 29. novembra Lēmums 2001/844/EK, EOTK, Euratom, ar ko groza tās iekšējo reglamentu (OV L 317, 3.12.2001., 1. lpp.).

I PIELIKUMS

DROŠĪBAS KLASIFIKĀCIJU ATBILSTĪBA

ES	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
Beļģija	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.).	zemsvītras ([1]) piezīme
Bulgārija	Строго секретно	Секретно	Поверително	За служебно ползване
Čehijas Republika	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Dānija	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Vācija	Streng geheim	Geheim	VS ([2]) – Vertraulich	VS – Nur für den Dienstgebrauch
Igaunija	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Īrija	Top Secret	Secret	Confidential	Restricted
Grieķija	Άκρως Απόρρητο Abr: ΑΑΠ	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Spānija	Secreto	Reservado	Confidencial	Difusión Limitada
Francija	Très Secret Défense	Secret Défense	Confidentiel Défense	zemsvītras ([3]) piezīme |
Horvātija	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Itālija	Segretissimo	Segreto	Riservatissimo	Riservato
Kipra	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
Luksemburga	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Ungārija	"Szigorúan titkos!"	"Titkos!"	"Bizalmas!"	"Korlátozott terjesztésű!"
Malta	L-Ogħla Segretezza	Sigriet	Kunfidenzjali	Ristrett
Nīderlande	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Austrija	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Polija	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugāle	Muito Secreto	Secreto	Confidencial	Reservado

ES	TRES SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET,	CONFIDENTIEL UE/EU CONFIDENTIAL,	RESTREINT UE/EU RESTRICTED,
Rumānija	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu
Slovēnija	Strogo tajno	Tajno	Zaupno	Interno
Slovākija	Prísne tajné	Tajné	Dôverné	Vyhradené
Somija	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Zviedrija ([4])	HEMLIG/TOP SECRET HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG/SECRET HEMLIG	HEMLIG/CONFIDENTIAL HEMLIG	HEMLIG/RESTRICTED HEMLIG
Apvienotā Karaliste	UK TOP SECRET	UK SECRET	Ekvivalenta nav ([5])	UK OFFICIAL – SENSITIVE

([1]) "Diffusion Restreinte/Beperkte Verspreiding" Beļģijā nav drošības klasifikācija. Beļģija ar "RESTREINT UE/EU RESTRICTED" informāciju rīkojas un to aizsargā tikpat stingri, kā noteikts Eiropas Savienības Padomes drošības noteikumu standartos un procedūrās.

([2]) Vācija – VS = "Verschlusssache".

([3]) Francija savā valsts sistēmā nelieto klasifikāciju "RESTREINT". Francija ar "RESTREINT UE/EU RESTRICTED" informāciju rīkojas un to aizsargā tikpat stingri, kā noteikts Eiropas Savienības Padomes drošības noteikumu standartos un procedūrās.

([4]) Zviedrija – drošības klasifikācijas marķējumu augšējā rindā izmanto aizsardzības iestādes un marķējumu apakšējā rindā – pārējās iestādes.

([5]) Apvienotā Karaliste ar ESKI, kas marķēta kā "CONFIDENTIEL UE/EU CONFIDENTIAL" rīkojas un aizsargā to saskaņā ar drošības aizsardzības prasībām, ko piemēro "UK SECRET".

II PIELIKUMS

AKRONĪMU SARAKSTS

Akronīms	Nozīme
KI	Kriptogrāfijas iestāde
KAI	Kriptogrāfijas apstiprināšanas iestāde
CCTV	Slēgta tīkla televīzijas kameras
KII	Kriptogrāfijas izplatīšanas iestāde
KIS	Komunikācijas un informācijas sistēmas, kurās rīkojas ar ESKI
IDI	Izraudzītā drošības iestāde
ESKI	ES klasificēta informācija
IDP	Iestādes drošības pielaide
IA	Informācijas aizsardzība
IAA	Informācijas aizsardzības iestāde
IAS	Ielaušanās atklāšanas sistēma
IT	Informācijas tehnoloģija
LSO	Vietējais drošības speciālists
VDI	Valsts drošības iestāde
PDP	Personāla drošības pielaide
PDPA	Personāla drošības pielaides apliecība
PDI	Programmas/projekta drošības instrukcijas
RK	Reģistra kontrolieris
DAI	Drošības akreditācijas iestāde
DAV	Drošības aspektu vēstule
DKK	Drošības klasifikācijas rokasgrāmata
SecOPs	Drošības darba procedūras
TI	*TEMPEST* iestāde
LESD	Līgums par Eiropas Savienības darbību

III PIELIKUMS

VALSTS DROŠĪBAS IESTĀŽU SARAKSTS

BEĻĢIJA

Autorité nationale de Sécurité
SPF Affaires étrangères, Commerce extérieur et Coopération au Développement
15, rue des Petits Carmes
BE-1000 Bruxelles
Sekretariāta tālr.: +32 25014542
Fakss: +32 25014596
E-pasts: nvo-ans@diplobel.fed.be

BULGĀRIJA

State Commission on Information Security
(Informācijas drošības valsts komisija)
90 Cherkovna Str.
1505 Sofia
Tālr.: +359 29333600
Fakss: +359 29873750
E-pasts: dksi@government.bg
Tīmekļa vietne: www.dksi.bg

ČEHIJAS REPUBLIKA

Národní bezpečnostní úřad
(Valsts drošības iestāde)
Na Popelce 2/16
150 06 Praha 56
Tālr.: +420 257283335
Fakss: +420 257283110
E-pasts: czech.nsa@nbu.cz
Tīmekļa vietne: www.nbu.cz

DĀNIJA

Politiets Efterretningstjeneste
(Dānijas Drošības izlūkošanas dienests)
Klausdalsbrovej 1
2860 Søborg
Tālr.: +45 33148888
Fakss: +45 33430190

Forsvarets Efterretningstjeneste
(Dānijas Aizsardzības izlūkošanas dienests)
Kastellet 30
2100 Copenhagen Ø
Tālr.: +45 33325566
Fakss: +45 33931320

VĀCIJA

Bundesministerium des Innern
Referat ÖS III 3
Alt-Moabit 101 D
11014 Berlin
Tālr.: +49 30186810
Fakss: +49 30186811441
E-pasts: oesIII3@bmi.bund.de

IGAUNIJA

National Security Authority Department
(Valsts drošības iestādes departaments)
Estonian Ministry of Defence
(Igaunijas Aizsardzības ministrija)
Sakala 1
15094 Tallinn
Tālr.: +372 7170113 0019, +372 7170117
Fakss: +372 7170213
E-pasts: nsa@mod.gov.ee

GRIEĶIJA

Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Διακλαδική Διεύθυνση Στρατιωτικών Πληροφοριών (ΔΔΣΠ)
Διεύθυνση Ασφαλείας και Αντιπληροφοριών
ΣΤΓ 1020 -Χολαργός (Αθήνα)
Ελλάδα
Tālr.: +30 2106572045 (ώρες γραφείου)
+ 30 2106572009 (ώρες γραφείου)
Fakss: +30 2106536279 + 30 2106577612

Hellenic National Defence General Staff (HNDGS)
(Grieķijas valsts aizsardzības ģenerālštābs)
Military Intelligence Sectoral Directorate
(Militāro izlūkdatu nozares direktorāts)
Security Counterintelligence Directorate
(Drošības pretizlūkošanas direktorāts)
GR-STG 1020 Holargos – Athens
Tālr.: +30 2106572045
+ 30 2106572009
Fakss: +30 2106536279, +30 2106577612

SPĀNIJA

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
28023 Madrid
Tālr.: +34 913725000
Fakss: +34 913725808
E-pasts: nsa-sp@areatec.com

FRANCIJA

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
Tālr.: +33 171758177
Fakss: + 33 171758200

HORVĀTIJA

Office of the National Security Council
(Valsts drošības padomes birojs)
Croatian NSA
Jurjevska 34
10000 Zagreb
Croatia
Tālr.: +385 14681222
Fakss: + 385 14686049
Tīmekļa vietne: www.uvns.hr

ĪRIJA

National Security Authority
Department of Foreign Affairs
76 – 78 Harcourt Street
Dublin 2
Tālr.: +353 14780822
Fakss: +353 14082959

ITĀLIJA

Presidenza del Consiglio dei Ministri
D.I.S. – U.C.Se.
Via di Santa Susanna, 15
00187 Roma
Tālr.: +39 0661174266
Fakss: +39 064885273

KIPRA

ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ
ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Υπουργείο Άμυνας
Λεωφόρος Εμμανουήλ Ροΐδη 4
1432 Λευκωσία, Κύπρος
Tālr.: +357 22807569, +357 22807643,
+357 22807764
Fakss: +357 22302351

Ministry of Defence (Aizsardzības ministrija)
Minister's Military Staff (Ministra militārais štābs)
National Security Authority (NSA) (Valsts drošības iestāde)
4 Emanuel Roidi street
1432 Nicosia
Tālr.: +357 22807569, +357 22807643,
+357 22807764
Fakss: +357 22302351
E-pasts: cynsa@mod.gov.cy

LATVIJA

Valsts Drošības iestāde (*National Security Authority*)
Latvijas Republikas Satversmes aizsardzības birojs (*Constitution Protection Bureau of the Republic of Latvia*)
P.O. Box 286
LV-1001 Riga
Tālr.: +371 67025418
Fakss: +371 67025454
E-pasts: ndi@sab.gov.lv

LIETUVA

Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija
(Lietuvas Republikas Noslēpumu aizsardzības koordinācijas Komisija Valsts Drošības iestāde)
Gedimino 40/1
LT-01110 Vilnius
Tālr.: +370 706 66701, +370 706 66702
Fakss: +370 706 66700
E-pasts: nsa@vsd.lt

LUKSEMBURGA

Autorité nationale de Sécurité
Boîte postale 2379
1023 Luxembourg
Tālr.: +352 24782210 central
+ 352 24782253 direct
Fakss: +352 24782243

UNGĀRIJA

Nemzeti Biztonsági Felügyelet
Ungārijas Valsts drošības iestāde
H-1024 Budapest, Szilágyi Erzsébet fasor 11/B
Tālr.: +36 (1) 7952303
Fakss: +36 (1) 7950344

Pasta adrese:
H-1357 Budapest, PO Box 2
E-pasts: nbf@nbf.hu
Tīmekļa vietne: www.nbf.hu

MALTA

Ministry for Home Affairs and National Security
(Iekšlietu un valsts drošības ministrija)
P.O. Box 146
MT-Valletta
Tālr.: +356 21249844
Fakss: +356 25695321

NĪDERLANDE

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20010
2500 EA Den Haag
Tālr.: +31 703204400
Fakss: +31 703200733

Ministerie van Defensie
Beveiligingsautoriteit
Postbus 20701
2500 ES Den Haag
Tālr.: +31 703187060
Fakss: +31 703187522

AUSTRIJA

Informationssicherheitskommission
Bundeskanzleramt
Ballhausplatz 2
1014 Wien
Tālr.: +43 1531152594
Fakss: +43 1531152615
E-pasts: ISK@bka.gv.at

POLIJA

Agencja Bezpieczeństwa Wewnętrznego – ABW
(Iekšējās drošības aģentūra)
2A Rakowiecka St.
00-993 Warszawa
Tālr.: +48 22 58 57 944
Fakss: +48 22 58 57 443
E-pasts: nsa@abw.gov.pl
Tīmekļa vietne: www.abw.gov.pl

PORTUGĀLE

Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Rua da Junqueira, 69
1300-342 Lisboa
Tālr.: +351 213031710
Fakss: +351 213031711

RUMĀNIJA

Oficiul Registrului Național al Informațiilor Secrete de Stat
(Rumānijas VDI – ORNISS Klasificētas informācijas valsts reģistra birojs)
4 Mures Street
012275 Bucharest
Tālr.: +40 212245830
Fakss: +40 212240714
E-pasts: nsa.romania@nsa.ro
Tīmekļa vietne: www.orniss.ro

SLOVĒNIJA

Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
1000 Ljubljana
Tālr.: +386 14781390
Fakss: +386 14781399
E-pasts: gp.uvtp@gov.si

SLOVĀKIJA

Národný bezpečnostný úrad
(Valsts drošības iestāde)
Budatínska 30 P.O.
P.O. Box 16
850 07 Bratislava
Tālr.: +421 268692314
Fakss: +421 263824005
Tīmekļa vietne: www.nbusr.sk

SOMIJA

National Security Authority (Valsts Drošības iestāde)
Ministry for Foreign Affairs (Ārlietu ministrija)
P.O. Box 453
FI-00023 Government
Tālr.: 16055890
Fakss: +358 916055140
E-pasts: NSA@formin.fi

ZVIEDRIJA

Utrikesdepartementet
(Ārlietu ministrija)
SSSB
SE-103 39 Stockholm
Tālr.: +46 84051000
Fakss: +46 87231176
E-pasts: ud-nsa@foreign.ministry.se

APVIENOTĀ KARALISTE

UK National Security Authority
Room 335, 3rd Floor
70 Whitehall
London
SW1A 2AS
Tālr. Nr. 1: +44 2072765649
Tālr. Nr. 2: +44 2072765497
Fakss: +44 2072765651
E-pasts: UK-NSA@cabinet-office.x.gsi.gov.uk