►**B**

PADOMES LĒMUMS

(2013. gada 23. septembris)

par drošības noteikumiem ES klasificētas informācijas aizsardzībai

(2013/488/ES)

(OV L 274, 15.10.2013., 1. lpp.)

Grozīts ar:

		Oficiālais Vēstnesis		
		Nr.	Lappuse	Datums
►**M1**	Padomes Lēmums 2014/233/ES (2014. gada 14. aprīlis)	L 125	72	26.4.2014.

▼B

PADOMES LĒMUMS

(2013. gada 23. septembris)

par drošības noteikumiem ES klasificētas informācijas aizsardzībai

(2013/488/ES)

EIROPAS SAVIENĪBAS PADOME,

ņemot vērā Līgumu par Eiropas Savienības darbību un jo īpaši tā 240. panta 3. punktu,

ņemot vērā Padomes Lēmumu 2009/937/ES (2009. gada 1. decembris), ar ko pieņem Padomes reglamentu ([1]), un jo īpaši tā 24. pantu,

tā kā:

(1) Lai attīstītu Padomes darbības visās jomās, kurās jārīkojas ar klasificētu informāciju, ir lietderīgi izveidot vispusīgu drošības sistēmu klasificētas informācijas aizsardzībai, kas attiektos uz Padomi, tās Ģenerālsekretariātu un dalībvalstīm.

(2) Šis lēmums būtu jāpiemēro gadījumos, kad Padome, tās darba sagatavošanas struktūras un Padomes Ģenerālsekretariāts (PĢS) rīkojas ar ES klasificēto informāciju (ESKI).

(3) Saskaņā ar saviem normatīvajiem aktiem un tiktāl, ciktāl tas vajadzīgs Padomes darbībai, dalībvalstīm būtu jāievēro šis lēmums gadījumos, kad to kompetentās iestādes, personāls vai līgumslēdzēji rīkojas ar ESKI, lai ikvienam būtu garantija, ka ESKI tiek aizsargāta līdzvērtīgā līmenī.

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

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

(6) Padomei būtu jānosaka piemērota sistēma, kas paredzētu, kā attiecīgā gadījumā saskaņā ar šo lēmumu un starp iestādēm spēkā esošo kārtību dalīties ar ESKI, kas ir Padomes rīcībā, ar citām ES iestādēm, struktūrām, birojiem un aģentūrām.

(7) Savienības struktūrām un aģentūrām, kas izveidotas saskaņā ar Līguma par Eiropas Savienību (LES) V sadaļas 2. nodaļu, kā arī Eiropolam un *Eurojust* saistībā ar iekšējām darbībām būtu jāpiemēro ar šo lēmumu noteiktie pamatprincipi un minimālie standarti ESKI aizsardzībai, ja tā ir paredzēts aktā, ar ko tās izveido.

([1]) OV L 325, 11.12.2009., 35. lpp.

▼B

(8) Krīzes pārvarēšanas operācijām, kas izveidotas saskaņā ar LES V sadaļas 2. nodaļu, un to personālam būtu jāpiemēro Padomes pieņemtie drošības noteikumi ESKI aizsardzībai, ja tā ir paredzēts Padomes aktā, ar ko tās izveido.

(9) ES īpašajiem pārstāvjiem un to komandas locekļiem būtu jāpiemēro Padomes pieņemtie drošības noteikumi ESKI aizsardzībai, ja tā ir paredzēts attiecīgajā Padomes aktā.

(10) Šis lēmums ir pieņemts, neskarot Līguma par Eiropas Savienības darbību (LESD) 15. un 16. pantu un to īstenošanas instrumentus.

(11) Šis lēmums ir pieņemts, neskarot dalībvalstīs pastāvošo praksi attiecībā uz attiecīgo valstu parlamentu informēšanu par Savienības darbībām.

(12) Lai nodrošinātu ESKI aizsardzībai paredzēto drošības noteikumu savlaicīgu piemērošanu attiecībā uz Horvātijas Republikas pievienošanos Eiropas Savienībai, šim lēmumam būtu jāstājas spēkā tā publicēšanas dienā,

IR PIEŅĒMUSI ŠO LĒMUMU.

1. pants

Mērķis, darbības joma un definīcijas

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

2. Minētie pamatprincipi un minimālie standarti attiecas uz Padomi un PĢS, un tos ievēro dalībvalstis saskaņā ar saviem attiecīgajiem normatīvajiem aktiem, lai ikvienam būtu garantija, ka ir nodrošināts līdzvērtīgs ESKI aizsardzības līmenis.

3. Šajā lēmumā piemēro definīcijas, kas izklāstītas A papildinājumā.

2. pants

ESKI, drošības klasifikāciju un marķējumu definīcijas

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

2. ESKI piešķir kādu no šādiem klasifikācijas līmeņiem:

a) *TRÈS 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;

▼B

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 varētu būt nevēlama Eiropas Savienības vai vienas vai vairāku dalībvalstu interesēm.

3. ESKI piemēro drošības klasifikācijas marķējumu saskaņā ar 2. punktu. Papildus var piemērot marķējumus, norādot ar dokumentu saistīto darbības jomu, autoru, izplatīšanas ierobežojumus, ierobežojot izmantošanu vai norādot izpaušanu.

3. pants

Klasifikācijas pārvaldība

1. Kompetentās iestādes nodrošina, ka ESKI ir pienācīgi klasificēta, skaidri apzināta kā klasificēta informācija un saglabā klasifikācijas līmeni vienīgi tik ilgi, cik tas nepieciešams.

2. ESKI neklasificē zemākā kategorijā vai nedeklasificē un 2. panta 3. punktā minētos marķējumus nemaina vai nesvītro bez autora iepriekšējas rakstiskas piekrišanas.

3. Padome apstiprina drošības politiku attiecībā uz ESKI izstrādi, kurā ir ietverta praktiskā klasifikācijas rokasgrāmata.

4. pants

Klasificētas informācijas aizsardzība

1. ESKI aizsargā saskaņā ar šo lēmumu.

2. Jebkādas ESKI turētājs ir atbildīgs par tās aizsardzību saskaņā ar šo lēmumu.

3. Ja dalībvalstis Savienības iestādēs vai tīklos ievieš klasificētu informāciju, kam piemērots valsts drošības klasifikācijas marķējums, Padome un PĢS aizsargā šo informāciju saskaņā ar prasībām, kas attiecas uz līdzvērtīgas kategorijas ESKI, kā tas izklāstīts B papildinājumā paredzētajā drošības klasifikāciju atbilsmju tabulā.

4. ESKI kopumam var ļaut piešķirt tāda līmeņa aizsardzību, kas atbilst augstākai klasifikācijas kategorijai nekā tās atsevišķajiem komponentiem piešķirtā klasifikācijas kategorija.

▼B

5. pants

Drošības riska pārvaldība

1. ESKI risku pārvalda kā procesu. Šā procesa mērķis ir noteikt zināmos drošības riskus, definēt drošības pasākumus, lai mazinātu šādus riskus līdz pieņemamam līmenim saskaņā ar šajā lēmumā izklāstītajiem pamatprincipiem un minimālajiem standartiem, un piemērot šos pasākumus saskaņā ar pastiprinātas aizsardzības koncepciju, kā definēts A papildinājumā. Minēto pasākumu efektivitāti nepārtraukti izvērtē.

2. Drošības pasākumi ESKI aizsardzībai visā tās aprites laikā jo īpaši atbilst drošības klasifikācijai, informācijas vai materiāla veidam un apjomam, to iekārtu atrašanās vietai un uzbūvei, kurās ESKI atrodas, un vietēji izvērtētam vardarbīgu un/vai noziedzīgu nodarījumu apdraudējumam, tostarp spiegošanai, sabotāžai un terorismam.

3. Ārkārtas rīcības plānos ņem vērā vajadzību aizsargāt ESKI ārkārtas situācijās, lai novērstu neatļautu piekļuvi, izpaušanu, integritātes vai piekļuves zaudējumu.

4. Darbības nepārtrauktības plānos iekļauj preventīvus un atgūšanas pasākumus, lai mazinātu ietekmi, ko rada nozīmīgi starpgadījumi saistībā ar rīkošanos ar ESKI un tās glabāšanu.

6. pants

Šā lēmuma īstenošana

1. Vajadzības gadījumā Padome pēc Drošības komitejas ieteikuma apstiprina drošības politiku, kurā izklāstīti pasākumi šā lēmuma īstenošanai.

2. Drošības komiteja savā līmenī var pieņemt drošības pamatnostādnes, lai papildinātu vai atbalstītu šo lēmumu un Padomes apstiprināto drošības politiku.

7. pants

Personāla drošība

1. Personāla drošība nozīmē tādu pasākumu piemērošanu, lai nodrošinātu, ka piekļuvi ESKI piešķir tikai tādām personām:

— kurām ir vajadzība pēc informācijas,

— kurām attiecīgā gadījumā ir attiecīga līmeņa drošības pielaide un

— kuras ir informētas par viņu pienākumiem.

2. Personāla drošības pielaides procedūras izstrādā tā, lai noteiktu, vai konkrētai personai var nodrošināt piekļuvi ESKI, ņemot vērā attiecīgās personas lojalitāti un uzticamību.

▼B

3. Visas personas, kuras strādā PĢS un kuru pienākumos ietilpst vajadzība piekļūt vai rīkoties ar ESKI, kas klasificēta kā *CONFIDENTIEL UE/EU CONFIDENTIAL* vai augstāk, iziet attiecīga līmeņa drošības pārbaudi, pirms tām piešķir piekļuvi šādai ESKI. Šādām personām jāsaņem PĢS iecēlējinstitūcijas atļauja, lai piekļūtu ESKI līdz konkrētam līmenim un līdz konkrētam datumam.

4. Šā lēmuma 15. panta 3. punktā minētais dalībvalstu personāls, kura pienākumos var ietilpt vajadzība piekļūt ESKI, kas klasificēta kā *CONFIDENTIEL UE/EU CONFIDENTIAL* vai augstāk, iziet attiecīga līmeņa drošības pārbaudi vai ieņemamā amata dēļ viņiem sniedz pienācīgu atļauju saskaņā ar attiecīgās valsts normatīvajiem aktiem, pirms viņiem piešķir piekļuvi šādai ESKI.

5. Visas personas, pirms tām piešķir piekļuvi ESKI un pēc tam – regulāri, tiek informētas par pienākumu aizsargāt ESKI saskaņā ar šo lēmumu, un tās atzīst šo pienākumu.

6. Šā panta īstenošanas noteikumi ir izklāstīti I pielikumā.

8. pants

Fiziskā drošība

1. Fiziskā drošība ir fizisku un tehnisku aizsardzības pasākumu piemērošana, lai novērstu neatļautu piekļuvi ESKI.

2. Fiziskās drošības pasākumu mērķis ir nepieļaut slepenu vai vardarbīgu ielaušanos, novērst, kavēt un atklāt neatļautas darbības un pieļaut personāla nošķirumu attiecībā uz pielaidi ESKI, ņemot vērā vajadzības pēc informācijas principu. Šādus pasākumus nosaka, pamatojoties uz riska pārvaldības procesu.

3. Fiziskās drošības pasākumus īsteno visās telpās, ēkās, birojos un citās zonās, kur rīkojas ar ESKI vai to glabā, tostarp zonās, kur atrodas 10. panta 2. punktā definētās komunikāciju un informācijas sistēmas.

4. Zonas, kurās glabā ESKI, kas klasificēta kā *CONFIDENTIEL UE/EU CONFIDENTIAL* vai augstāk, izveido par drošības zonām saskaņā ar II pielikumu, un tās apstiprina kompetentā drošības iestāde.

5. Lai aizsargātu ESKI, kas klasificēta kā *CONFIDENTIEL UE/EU CONFIDENTIAL* vai augstāk, izmanto vienīgi apstiprinātas iekārtas vai ierīces.

6. Šā panta īstenošanas noteikumi ir izklāstīti II pielikumā.

▼B

9. pants

Klasificētas informācijas pārvaldība

1. Klasificētas informācijas pārvaldība ir administratīvu pasākumu piemērošana ESKI kontrolei tās aprites cikla laikā, lai papildinātu 7., 8. un 10. pantā minētos pasākumus un tādējādi palīdzētu novērst un atklāt tīšu vai netīšu šādas informācijas apdraudējumu vai tās zaudējumu. Šādi pasākumi jo īpaši ir saistīti ar ESKI izstrādi, reģistrāciju, kopēšanu, tulkošanu, klasifikācijas līmeņa pazemināšanu, deklasifikāciju, pārvietošanu un iznīcināšanu.

2. Informāciju, kas klasificēta kā *CONFIDENTIEL UE/EU CONFIDENTIAL* vai augstāk, drošības nolūkā reģistrē, pirms to izplata un to saņemot. PĢS un dalībvalstu kompetentās iestādes šim nolūkam izveido reģistrācijas sistēmu. Informāciju, kas klasificēta kā *TRÈS SECRET UE/EU TOP SECRET*, reģistrē īpašos reģistros.

3. Dienestus un telpas, kur rīkojas ar ESKI vai to glabā, regulāri pārbauda kompetentā drošības iestāde.

4. 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 saskaņā ar 10. panta 6. punktu;

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

   i) izmantojot elektroniskus informācijas nesējus (piemēram, zibatmiņas, kompaktdiskus, cietos diskus), kurus aizsargā ar kriptogrāfijas produktiem, kas apstiprināti saskaņā ar 10. panta 6. punktu; vai

   ii) visos citos gadījumos – kā to nosaka kompetentā drošības iestāde saskaņā ar III pielikumā izklāstītajiem attiecīgajiem aizsardzības pasākumiem.

5. Šā panta īstenošanas noteikumi ir izklāstīti III un IV pielikumā.

10. pants

ESKI aizsardzība, ar to rīkojoties komunikāciju un informācijas sistēmās

1. Informācijas aizsardzība (IA) ir pārliecība, ka komunikāciju un informācijas sistēmas jomā šīs sistēmas aizsargās informāciju, ar ko tās rīkojas, un darbosies, kā tas ir paredzēts, kad paredzēts un likumīgu lietotāju kontrolē. Ar efektīvu IA nodrošina atbilstīga līmeņa konfidencialitāti, integritāti, pieejamību, nenoliedzamību un autentiskumu. IA pamatā ir riska pārvaldības process.

▼B

2. “Komunikāciju un informācijas sistēma” (KIS) ir jebkura sistēma, kurā ar informāciju var rīkoties elektroniski. KIS ietver visus vajadzīgos resursus, lai sistēma darbotos, tostarp infrastruktūru, organizāciju, personālu un informācijas resursus. Šo lēmumu piemēro KIS, kurās rīkojas ar ESKI.

3. KIS rīkojas ar ESKI saskaņā ar IA koncepciju.

4. Visas KIS tiek akreditētas. Akreditācijas mērķis ir saņemt garantiju, ka ir īstenotas visas attiecīgās drošības procedūras un ka ir sasniegts pietiekams ESKI un KIS aizsardzības līmenis saskaņā ar šo lēmumu. Ar akreditācijas paziņojumu nosaka augstāko klasifikācijas līmeni informācijai, ar kādu atļauts rīkoties KIS, kā arī atbilstīgos noteikumus.

5. Drošības pasākumus īsteno, lai aizsargātu KIS, kurās rīkojas ar informāciju, kas klasificēta kā *CONFIDENTIEL UE/EU CONFIDENTIAL* un augstāk, pret šādas informācijas apdraudējumu, ko izraisa netīšas elektromagnētiskas emisijas (“*TEMPEST* drošības pasākumi”). Šādi drošības pasākumi ir samērīgi ar ekspluatācijas risku un informācijas klasifikācijas līmeni.

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

a) tās informācijas konfidencialitāti, kas klasificēta kā *SECRET UE/EU SECRET* un augstāk, aizsargā ar kriptogrāfijas produktiem, ko pēc Drošības komitejas ieteikuma ir apstiprinājusi Padome kā kriptogrāfijas apstiprinājuma iestāde (KAI);

b) tās informācijas konfidencialitāti, kas klasificēta kā *CONFIDENTIEL UE/EU CONFIDENTIAL* vai *RESTREINT UE/EU RESTRICTED*, aizsargā ar kriptogrāfijas produktiem, ko pēc Drošības komitejas ieteikuma apstiprinājis Padomes ģenerālsekretārs (“ģenerālsekretārs”) kā KAI.

Neatkarīgi no šā punkta b) apakšpunkta dalībvalstu sistēmās tās ESKI konfidencialitāti, kas klasificēta kā *CONFIDENTIEL UE/EU CONFIDENTIAL* vai *RESTREINT UE/EU RESTRICTED*, var aizsargāt ar kriptogrāfijas produktiem, ko apstiprinājusi dalībvalsts KAI.

7. Pārsūtot ESKI elektroniski, izmanto apstiprinātus kriptogrāfijas produktus. Neatkarīgi no šīs prasības ārkārtas apstākļos vai īpašās tehniskās konfigurācijās var piemērot īpašas procedūras, kā noteikts IV pielikumā.

▼B

8. PĢS un dalībvalstu kompetentās iestādes attiecīgi sadala šādus IA pienākumus:

a) IA iestāde (IAI);

b) *TEMPEST* iestāde (TI);

c) kriptogrāfijas apstiprinājuma iestāde (KAI);

d) kriptogrāfijas izplatīšanas iestāde (KII).

9. Katrai sistēmai PĢS un dalībvalstu kompetentās iestādes attiecīgi izveido:

a) drošības akreditācijas iestādi (DAI);

b) IA operatīvo iestādi.

10. Šā panta īstenošanas noteikumi ir izklāstīti IV pielikumā.

11. pants

Industriālā drošība

1. Industriālā drošība ir pasākumu piemērošana nolūkā nodrošināt, ka līgumslēdzējs vai apakšlīgumslēdzējs aizsargā ESKI sarunu laikā pirms klasificēta līguma slēgšanas un klasificēto līgumu darbības laikā. Tādi līgumi nav saistīti ar piekļuvi informācijai, kas klasificēta kā *TRÈS SECRET UE/EU TOP SECRET*.

2. PĢS līgumā var uzticēt uzdevumus, kas ietver vai ir saistīti ar piekļuvi ESKI vai rīkošanos ar to, vai tās glabāšanu, kuru veic rūpniecības vai citas vienības, kas reģistrētas dalībvalstī vai trešā valstī, kura noslēgusi nolīgumu vai administratīvu vienošanos saskaņā ar 13. panta 2. punkta a) vai b) apakšpunktu.

3. PĢS kā līgumslēdzēja iestāde nodrošina, ka, piešķirot klasificētu līgumu rūpniecības vai citām vienībām, tiek ievēroti šajā lēmumā izklāstītie un attiecīgajā līgumā minētie industriālās drošības minimālie standarti.

4. Katras dalībvalsts valsts drošības iestāde (VDI), izraudzītā drošības iestāde (IDI) vai cita kompetenta iestāde tiktāl, cik tas iespējams saskaņā ar attiecīgās valsts normatīvajiem aktiem, nodrošina, ka līgumslēdzēji un apakšlīgumslēdzēji, kas reģistrēti tās teritorijā, veic visus piemērotos pasākumus, lai aizsargātu šādu ESKI sarunās pirms klasificēta līguma slēgšanas un klasificēto līgumu darbības laikā.

5. Katras dalībvalsts VDI, IDI vai cita kompetenta iestāde atbilstīgi valsts normatīvajiem aktiem nodrošina, ka tās teritorijā reģistrētajiem līgumslēdzējiem un apakšlīgumslēdzējiem, kas iesaistīti klasificētos līgumos vai apakšlīgumos un kam savās telpās vajadzīga piekļuve informācijai, kura klasificēta kā *CONFIDENTIEL UE/EU CONFIDENTIAL* vai *SECRET UE/EU SECRET*, izpildot minētos līgumus vai pirms to parakstīšanas, vajadzīga atbilstīga klasifikācijas līmeņa iestādes drošības pielaide (IDP).

▼B

6. Līgumslēdzēja vai apakšlīgumslēdzēja personālam, kam klasificēta līguma darbības laikā jāpiekļūst informācijai, kura klasificēta kā *CONFIDENTIEL UE/EU CONFIDENTIAL* vai *SECRET UE/EU SECRET*, personāla drošības pielaidi (PDP) piešķir attiecīgā VDI/IDI vai kāda cita kompetenta drošības iestāde saskaņā ar valsts normatīvajiem aktiem un minimālajiem drošības standartiem, kas izklāstīti I pielikumā.

7. Šā panta īstenošanas noteikumi ir izklāstīti V pielikumā.

12. pants

Dalīšanās ar ESKI

1. Padome paredz nosacījumus, ar kādiem tā var dalīties tās rīcībā esošajā ESKI ar citām ES iestādēm, struktūrām, birojiem vai aģentūrām. Šajā sakarā var izveidot piemērotu sistēmu, tostarp vajadzības gadījumā šajā nolūkā var slēgt iestāžu nolīgumus vai izstrādāt citu kārtību.

2. Jebkura šāda sistēma nodrošina, ka ESKI tiek aizsargāta atbilstīgi tās klasifikācijas līmenim un saskaņā ar pamatprincipiem un minimālajiem standartiem, kas ir līdzvērtīgi šajā lēmumā noteiktajiem.

13. pants

Klasificētas informācijas apmaiņa ar trešām valstīm un starptautiskām organizācijām

1. Ja Padome nosaka, ka vajadzīga ESKI apmaiņa ar trešo valsti vai starptautisku organizāciju, šādas apmaiņas veikšanai izveido piemērotu sistēmu.

2. Lai izveidotu šādu sistēmu un definētu savstarpējus noteikumus par tās klasificētās informācijas aizsardzību, ar kuru apmainās:

a) Savienība noslēdz nolīgumus ar trešām valstīm vai starptautiskām organizācijām par drošības procedūrām klasificētas informācijas apmaiņai un aizsardzībai (“informācijas drošības nolīgumi”); vai

b) ģenerālsekretārs var noslēgt administratīvu vienošanos PĢS vārdā saskaņā ar VI pielikuma 17. punktu, ja tās ESKI klasifikācijas līmenis, kuru izplatīs, parasti nav augstāks par *RESTREINT UE/EU RESTRICTED*.

3. Šā panta 2. punktā minētajos informācijas drošības nolīgumos un administratīvajās vienošanās iekļauj noteikumus, lai nodrošinātu, ka gadījumos, kad trešās valstis vai starptautiskās organizācijas saņem ESKI, šai informācijai nodrošina tādu aizsardzību, kas atbilst tās klasifikācijas līmenim un saskaņā ar minimālajiem standartiem, kuri ir ne mazāk stingri kā šajā lēmumā paredzētie.

▼B

4. Lēmumu ESKI, kas nāk no Padomes, nodot trešai valstij vai starptautiskai organizācijai pieņem Padome, izskatot katru gadījumu atsevišķi un atbilstīgi šādas informācijas būtībai un saturam, vajadzības pēc informācijas principam attiecībā uz saņēmēju un tam, ko no nodošanas gūst Savienība. Ja Padome nav tās klasificētās informācijas autors, kuras nodošana ir vajadzīga, PĢS vispirms lūdz rakstisku autora piekrišanu nodošanai. Ja autoru nevar noteikt, Padome uzņemas autora atbildību.

5. Lai pārliecinātos par to drošības pasākumu efektivitāti, kurus piemēro trešā valsts vai starptautiska organizācija ar mērķi aizsargāt sniegto ESKI vai to ESKI, ar kuru notiek apmaiņa, organizē izvērtējuma apmeklējumus.

6. Šā panta īstenošanas noteikumi ir izklāstīti VI pielikumā.

14. pants

Drošības prasību pārkāpumi un ESKI apdraudējums

1. Drošības prasību pārkāpums rodas tādas personas darbības vai bezdarbības rezultātā, kas ir pretrunā šajā lēmumā noteiktajiem drošības noteikumiem.

2. ESKI ir apdraudēta, ja drošības prasību pārkāpuma gadījumā tā ir pilnībā vai daļēji nonākusi nesankcionētu personu rīcībā.

3. Par jebkuriem drošības pārkāpumiem vai iespējamiem drošības pārkāpumiem nekavējoties ziņo kompetentajai drošības iestādei.

4. Ja ir zināms vai pastāv pamatotas aizdomas, ka ESKI ir apdraudēta vai zudusi, VDI vai cita kompetentā iestāde veic visus vajadzīgos pasākumus saskaņā ar attiecīgajiem normatīvajiem aktiem, lai:

a) informētu informācijas autoru;

b) nodrošinātu, ka faktu apzināšanas nolūkā lietu izmeklē personāls, kas nav tieši saistīts ar drošības apdraudējumu;

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

d) veiktu attiecīgus pasākumus atkārtošanās novēršanai; un

e) ziņotu attiecīgajām iestādēm par veiktajiem pasākumiem.

5. Jebkurai personai, kura ir atbildīga par šajā lēmumā izklāstīto drošības noteikumu tīšu pārkāpšanu, piemēro disciplināratbildību saskaņā ar spēkā esošajiem noteikumiem. Jebkurai personai, kura ir atbildīga par ESKI apdraudējumu vai zudumu, piemēro disciplināratbildību un/vai kriminālatbildību saskaņā ar spēkā esošajiem normatīvajiem aktiem.

▼B

15. pants

Atbildība par īstenošanu

1. Padome veic visus vajadzīgos pasākumus, lai nodrošinātu vispārēju saskaņotību šā lēmuma piemērošanā.

2. Ģenerālsekretārs veic visus vajadzīgos pasākumus, lai nodrošinātu, ka, strādājot ar ESKI vai citu klasificētu informāciju vai to glabājot, šo lēmumu piemēro Padomes izmantotajās telpās un visā PĢS tā ierēdņi un pārējie darbinieki, kā arī personāls, kas norīkots darbā uz PĢS, un PĢS līgumslēdzēji.

3. Dalībvalstis saskaņā ar saviem attiecīgajiem normatīvajiem aktiem veic atbilstīgus pasākumus, lai nodrošinātu, ka, rīkojoties ar ESKI vai to glabājot, šo lēmumu ievēro:

a) dalībvalstu pastāvīgo pārstāvniecību Eiropas Savienībā personāls, kā arī valstu delegāciju locekļi, kas apmeklē Padomes vai tās sagatavošanas struktūru sanāksmes vai piedalās citās Padomes darbībās;

b) citi dalībvalstu valsts pārvaldes locekļi, tostarp personāls, kas norīkots darbam šajā pārvaldē, neatkarīgi no tā, vai tie strādā dalībvalsts teritorijā vai ārzemēs;

c) citas personas dalībvalstīs, kam ieņemamā amata dēļ ar pienācīgām atļaujām ir piekļuve ESKI; un

d) dalībvalstu līgumslēdzēji neatkarīgi no tā, vai tie strādā dalībvalsts teritorijā vai ārzemēs.

16. pants

Padomes drošības organizācija

1. Kā daļu no pienākuma nodrošināt vispārēju saskaņotību šā lēmuma piemērošanā Padome apstiprina:

a) līgumus, kas minēti 13. panta 2. punkta a) apakšpunktā;

b) lēmumus, ar ko atļauj vai piekrīt nodot ESKI, kas nāk no Padomes vai ir Padomes rīcībā, trešām valstīm un starptautiskām organizācijām saskaņā ar informācijas autora piekrišanas principu;

c) ikgadēju izvērtējuma apmeklējumu programmu, ko iesaka Drošības komiteja attiecībā uz apmeklējumiem, lai izvērtētu dalībvalstu dienestus un telpas, Savienības struktūras, aģentūras un vienības, kuras piemēro šo lēmumu vai tā principus, kā arī attiecībā uz trešo valstu un starptautisku organizāciju izvērtējuma apmeklējumiem, lai pārliecinātos par īstenoto ESKI aizsardzības pasākumu efektivitāti; un

▼B

d) drošības politikas jomas, kā paredzēts 6. panta 1. punktā.

2. Ģenerālsekretārs ir PĢS drošības iestāde. Veicot šīs funkcijas, ģenerālsekretārs:

a) īsteno Padomes drošības politiku un to regulāri pārskata;

b) sazinās ar dalībvalstu VDI saistībā ar drošības jautājumiem, kas attiecas uz tādas klasificētas informācijas aizsardzību, kura ir atbilstīga Padomes darbībām;

c) saskaņā ar 7. panta 3. punktu PĢS ierēdņiem, pārējiem darbiniekiem un norīkotiem valsts ekspertiem piešķir atļauju piekļūt informācijai, kas klasificēta kā *CONFIDENTIEL UE/EU CONFIDENTIAL* vai augstāk;

d) attiecīgā gadījumā uzdod veikt izmeklēšanu par notikušu vai iespējamu tādas ESKI neatļautu izpaušanu vai pazušanu, kas ir Padomes rīcībā vai kas nāk no Padomes, un lūdz attiecīgu drošības iestāžu palīdzību šādas izmeklēšanas veikšanā;

e) veic klasificētās informācijas aizsardzībai paredzēto drošības pasākumu periodiskas pārbaudes PĢS telpās;

f) veic periodiskus apmeklējumus, lai izvērtētu ESKI aizsardzībai paredzētos drošības pasākumus, ko veic Savienības struktūrās, aģentūrās un vienībās, kuras piemēro šo lēmumu vai tā principus;

g) periodiski, kopīgi un vienojoties ar attiecīgo VDI, veic to drošības pasākumu izvērtējumus, kuru mērķis ir aizsargāt ESKI dalībvalstu dienestos un telpās;

h) nodrošina, lai drošības pasākumi vajadzības gadījumā tiktu saskaņoti ar dalībvalstu kompetentajām iestādēm, kuras ir atbildīgas par klasificētas informācijas aizsardzību, un attiecīgā gadījumā – ar trešām valstīm vai starptautiskām organizācijām, tostarp attiecībā uz ESKI drošības apdraudējuma būtību un ar to saistītiem aizsardzības pasākumiem; un

i) slēdz administratīvas vienošanās, kas minētas 13. panta 2. punkta b) apakšpunktā.

PĢS Drošības birojs ir ģenerālsekretāra rīcībā, lai palīdzētu pildīt minētos pienākumus.

3. Īstenojot 15. panta 3. punktu, dalībvalstīm būtu:

a) jāizraugās VDI, kā uzskaitīts C papildinājumā, kas ir atbildīga par drošības pasākumiem ESKI aizsardzībai, lai:

   i) attiecīgajā dalībvalstī vai ārvalstīs jebkāda valsts dienesta, valsts vai privātas struktūras vai aģentūras glabātā ESKI būtu aizsargāta saskaņā ar šo lēmumu;

   ii) regulāri pārbaudītu vai izvērtētu ESKI aizsardzībai paredzētos drošības pasākumus;

▼B

iii) visas personas, kas strādā valsts pārvaldē vai pie līgumslēdzēja un kam var tikt piešķirta atļauja piekļūt klasificētai informācijai, kura klasificēta kā *CONFIDENTIEL UE/EU CONFIDENTIAL* vai augstāk, attiecīgi saņemtu drošības pielaidi vai saņemtu citu pienācīgu atļauju saskaņā ar valsts normatīvajiem aktiem;

iv) vajadzības gadījumā izstrādātu drošības programmas, lai līdz minimumam samazinātu ESKI apdraudējuma vai zuduma risku;

v) ar citām kompetentām valsts iestādēm saskaņotu drošības pasākumus, kas saistīti ar ESKI aizsardzību, tostarp šajā lēmumā minētos; un

vi) atbildētu uz atbilstīgiem drošības pielaides lūgumiem, jo īpaši tiem, ko iesniedz jebkuras Savienības struktūras, aģentūras, vienības, operācijas, kas izveidotas saskaņā ar LES V sadaļas 2. nodaļu, un ES īpašie pārstāvji (ESĪP) un to komandas, kuri piemēro šo lēmumu vai tā principus;

b) jānodrošina, ka to kompetentās iestādes sniedz informāciju un padomus valdībām un līdz ar to Padomei par ESKI drošības apdraudējuma raksturu un aizsardzības līdzekļiem pret to.

17. pants

Drošības komiteja

1. Ar šo izveido Drošības komiteju. Tā izskata un izvērtē jebkurus drošības jautājumus šā lēmuma darbības jomā un attiecīgos gadījumos sniedz ieteikumus Padomei.

2. Drošības komitejas sastāvā ir dalībvalstu VDI pārstāvji, un tās sanāksmēs piedalās Komisijas un EĀDD pārstāvis. Tās priekšsēdētājs ir ģenerālsekretārs vai viņa izraudzīts pārstāvis. Drošības komitejas sanāksmes notiek saskaņā ar Padomes norādījumiem pēc ģenerālsekretāra vai kādas VDI pieprasījuma.

Var uzaicināt piedalīties pārstāvjus no Savienības struktūrām, aģentūrām un vienībām, kuras piemēro šo lēmumu vai tā principus, ja tiek izskatīti jautājumi, kas attiecas uz tām.

3. Drošības komiteja organizē savas darbības tā, lai varētu sniegt ieteikumus par konkrētām drošības jomām. Vajadzības gadījumā tā izveido apakšgrupu IA jautājumiem un citas ekspertu apakšgrupas. Tā izstrādā mandātus šādām ekspertu apakšgrupām un saņem ziņojumus par to darbību, tostarp attiecīgā gadījumā – jebkādus ieteikumus Padomei.

▼B

18. pants

Iepriekšējā lēmuma aizstāšana

1. Ar šo lēmumu atceļ un aizstāj Padomes Lēmumu 2011/292/ES ([1]).

2. Visu ESKI, kas klasificēta saskaņā ar Padomes Lēmumu 2001/264/EK ([2]) un Lēmumu 2011/292/ES, turpina aizsargāt saskaņā ar šā lēmuma attiecīgajiem noteikumiem.

19. pants

Stāšanās spēkā

Šis lēmums stājas spēkā dienā, kad to publicē *Eiropas Savienības Oficiālajā Vēstnesī*.

([1]) Padomes Lēmums 2011/292/ES (2011. gada 31. marts) par drošības noteikumiem ES klasificētas informācijas aizsardzībai (OV L 141, 27.5.2011., 17. lpp.).

([2]) Padomes Lēmums 2001/264/EK (2001. gada 19. marts), ar ko pieņem Padomes drošības reglamentu (OV L 101, 11.4.2001., 1. lpp.).

▼B

PIELIKUMI

I PIELIKUMS

Personāla drošība

II PIELIKUMS

Fiziskā drošība

III PIELIKUMS

Klasificētas informācijas pārvaldība

IV PIELIKUMS

ESKI aizsardzība, rīkojoties ar to komunikāciju un informācijas sistēmās

V PIELIKUMS

Industriālā drošība

VI PIELIKUMS

Klasificētas informācijas apmaiņa ar trešām valstīm un starptautiskām organizācijām

▼B

I PIELIKUMS

PERSONĀLA DROŠĪBA

I. IEVADS

1. Šajā pielikumā izklāstīti 7. panta īstenošanas noteikumi. Tajā izklāstīti kritēriji, lai, ņemot vērā personas lojalitāti un uzticamību, noteiktu, vai tai var dot atļauju piekļūt ESKI, un izmeklēšanas un administratīvās procedūras, kas vajadzīgas šim nolūkam.

II. PIEKĻUVES ESKI PIEŠĶIRŠANA

2. Personai piešķir piekļuvi klasificētai informācijai vienīgi pēc tam, kad:

a) noskaidrota personas vajadzība pēc informācijas;

b) persona ir iepazīstināta ar ESKI aizsardzībai paredzētiem drošības noteikumiem un procedūrām un ir atzinusi savus pienākumus saistībā ar šādas informācijas aizsargāšanu; un

c) attiecībā uz informāciju, kas klasificēta kā *CONFIDENTIEL UE/EU CONFIDENTIAL* vai augstāk:

— tai piešķirta attiecīgā līmeņa PDP vai saņemta cita pienācīga atļauja ieņemamā amata dēļ saskaņā ar valsts normatīvajiem aktiem vai

— attiecībā uz PĢS ierēdņiem, pārējiem darbiniekiem un norīkotajiem valsts ekspertiem – personai atļauju piekļūt ESKI līdz konkrētam līmenim un konkrētam datumam piešķīrusi PĢS iecēlējiestāde saskaņā ar 16. līdz 25. punktu.

3. Katra dalībvalsts un PĢS apzina tos amatus savās struktūrās, kuriem vajadzīga piekļuve informācijai, kas klasificēta kā *CONFIDENTIEL UE/EU CONFIDENTIAL* vai augstāk, un tādēļ vajadzīga attiecīga līmeņa drošības pielaide.

III. PERSONĀLA DROŠĪBAS PIELAIDES PRASĪBAS

4. Pēc tam, kad saņemts pienācīgi atļauts pieprasījums, VDI vai cita kompetentā valsts iestāde ir atbildīga par to, lai nodrošinātu, ka tiek veiktas drošības izmeklēšanas attiecībā uz valstspiederīgajiem, kam vajadzīga piekļuve informācijai, kura klasificēta kā *CONFIDENTIEL UE/EU CONFIDENTIAL* vai augstāk. Izmeklēšanas standarti atbilst valsts normatīvajiem aktiem, lai izsniegtu PDP vai lai attiecīgā gadījumā sniegtu apliecinājumu attiecībā uz personu, kurai piešķirama atļauja piekļūt ESKI.

5. Ja attiecīgā persona dzīvo citas dalībvalsts vai trešās valsts teritorijā, kompetentās valsts iestādes lūdz dzīvesvietas dalībvalsts iestādes palīdzību saskaņā ar valsts normatīvajiem aktiem. Dalībvalstis palīdz cita citai veikt drošības izmeklēšanu saskaņā ar saviem normatīvajiem aktiem.

6. Ja to atļauj valsts normatīvie akti, VDI vai cita kompetenta valsts iestāde var veikt drošības izmeklēšanu attiecībā uz personām, kas nav valstspiederīgie un lūdz piekļuvi informācijai, kura klasificēta kā *CONFIDENTIEL UE/EU CONFIDENTIAL* vai augstāk. Izmeklēšanas standarti ir saskaņā ar valsts normatīvajiem aktiem.

▼B

Drošības izmeklēšanas kritēriji

7. Ar drošības izmeklēšanas palīdzību nosaka personas lojalitāti un uzticamību, lai šai personai varētu piešķirt drošības pielaidi ar mērķi piekļūt informācijai, kas klasificēta kā *CONFIDENTIEL UE/EU CONFIDENTIAL* vai augstāk. Kompetentā valsts iestāde veic vispārēju izvērtējumu, pamatojoties uz drošības izmeklēšanas rezultātiem. Šajā sakarā izmantotajos galvenajos kritērijos ietilpst, ciktāl to atļauj valsts normatīvie akti, izskatīt, vai persona:

a) ir veikusi vai ir mēģinājusi veikt, ir bijusi līdzzinātāja vai ir palīdzējusi kādam citam un atbalstījusi kādu citu izdarīt jebkādu spiegošanas, terorisma, sabotāžas, nodevības vai musināšanas aktu;

b) ir vai ir bijusi spiegu, teroristu, sabotieru vai arī tādu personu sabiedrotā, par kurām ir pamatotas aizdomas, ka viņi tādi ir, vai ārvalstu organizāciju pārstāvju, arī ārvalstu izlūkošanas dienestu, sabiedrotā, kas var apdraudēt Savienības un/vai kādas dalībvalsts drošību, ja vien tādas saistības nav bijušas atļautas oficiālo darba pienākumu pildīšanas laikā;

c) ir vai ir bijusi tādas organizācijas locekle, kas ar vardarbīgiem, graujošiem vai citiem nelikumīgiem līdzekļiem, *inter alia*, tiecas gāzt kādas dalībvalsts valdību, mainīt kādas dalībvalsts konstitucionālo kārtību vai mainīt tās valdības formu vai politiku;

d) atbalsta vai ir atbalstījusi kādu c) apakšpunktā minētu organizāciju vai ir vai ir bijusi cieši saistīta ar tādu organizāciju biedriem;

e) ir tīši noklusējusi, sagrozījusi vai viltojusi nozīmīgu informāciju, jo īpaši attiecībā uz drošības jautājumiem, vai ir tīši melojusi, aizpildot personāla drošības anketu, vai melojusi drošības intervijas laikā;

f) ir notiesāta par noziedzīgu nodarījumu vai nodarījumiem;

g) ir atzīta par atkarīgu no alkohola, nelikumīgu narkotisku vielu lietotāju un/vai likumīgu narkotisku vielu pārmērīgu lietotāju;

h) ir vai ir bijusi iesaistīta tādās darbībās, kas iespējami var būt par iemeslu šantāžai vai izspiešanai;

i) darbos vai runās ir izrādījusi negodīgumu, nelojalitāti un apliecinājusi, ka uz to nevar paļauties vai tai uzticēties;

j) ir nopietni vai atkārtoti pārkāpusi drošības noteikumus vai ir mēģinājusi veikt vai ir veikusi neatļautu darbību attiecībā uz komunikāciju un informācijas sistēmām; un

k) var būt pakļauta spiedienam (piemēram, ja tai ir vienas vai vairāku trešo valstu valstspiederība vai tai ir tādi radinieki vai tuvi sabiedrotie, kurus varētu iespaidot ārvalstu izmeklēšanas dienesti, teroristu grupējumi vai citas graujošas vai noziedzīgas organizācijas, vai personas, kuru nodomi var apdraudēt Savienības un/vai dalībvalstu drošību).

▼B

8. Attiecīgos gadījumos un saskaņā ar attiecīgās valsts normatīvajiem aktiem drošības izmeklēšanā var izskatīt arī personas finanšu un medicīnisko vēsturi.

9. Attiecīgos gadījumos un saskaņā ar attiecīgās valsts normatīvajiem aktiem drošības izmeklēšanā par nozīmīgu var uzskatīt arī laulātā, kopdzīves partnera vai tuva ģimenes locekļa uzvedību un apstākļus.

Izmeklēšanas prasības, lai iegūtu piekļuvi ESKI

Drošības pielaides sākotnēja piešķiršana

10. Sākotnējā drošības pielaide, lai piekļūtu informācijai, kas klasificēta kā *CONFIDENTIEL UE/EU CONFIDENTIAL* un *SECRET UE/EU SECRET*, pamatojas uz drošības izmeklēšanu, kura aptver vismaz pēdējos piecus gadus vai laiku no 18 gadu vecuma līdz pašreizējam brīdim, izvēloties īsāko no abiem, un tā ietver šādus elementus:

a) valsts personāla drošības anketas aizpildīšana attiecībā uz to ESKI līmeni, kuram personai var būt vajadzība piekļūt; pēc aizpildīšanas minēto anketu nosūta kompetentajai drošības iestādei;

b) identitātes/pilsonības/valstspiederības statusa pārbaude – pārbauda personas dzimšanas datumu un vietu un identitāti. Nosaka personas pašreizējo vai iepriekšējo pilsonības statusu un/vai valstspiederību; tostarp izvērtē, vai personu var jebkā ietekmēt ārvalstu avoti, piemēram, sakarā ar iepriekšēju dzīvesvietu vai agrākiem sakariem; un

c) attiecīgās valsts un vietējā mēroga datu pārbaude – pārbauda valsts drošības un centrālos sodāmības reģistrus, ja tādi ir, un/vai citus salīdzināmus valdības un policijas reģistrus. Pārbauda tādu policijas aģentūru reģistrus, kuru jurisdikcijā ir vieta, kur persona ir uzturējusies vai strādājusi.

11. Sākotnējā drošības pielaide, lai piekļūtu informācijai, kas klasificēta kā *TRÈS SECRET UE/EU TOP SECRET*, pamatojas uz drošības izmeklēšanu, kura aptver vismaz pēdējos desmit gadus vai laiku no 18 gadu vecuma līdz pašreizējam brīdim, izvēloties īsāko no abiem. Ja atbilstīgi e) apakšpunktam rīko intervijas, informāciju iegūst vismaz par pēdējiem septiņiem gadiem vai par laiku no 18 gadu vecuma līdz pašreizējam brīdim, izvēloties īsāko no abiem. Papildus 7. punktā minētajiem rādītājiem, pirms piešķirt *TRÈS SECRET UE/EU TOP SECRET* personāla drošības pielaidi, ciktāl to atļauj valsts normatīvie akti, izmeklē turpmāk norādītos elementus; tos var izmeklēt arī, pirms piešķir *CONFIDENTIEL UE/EU CONFIDENTIAL* vai *SECRET UE/EU SECRET* personāla drošības pielaidi, ja tas prasīts valsts normatīvajos aktos:

a) finansiālais statuss – meklē informāciju par personas finansēm, lai izvērtētu, vai viņu var ietekmēt ārvalstu vai pašmāju spiediens nopietnu finanšu grūtību dēļ, vai lai konstatētu neizskaidrojamu personas pārticību;

▼B

b) izglītība – meklē informāciju, lai pārbaudītu personas gūto izglītību skolās, universitātēs un citās mācību iestādēs, ko persona apmeklējusi pēc 18. dzimšanas dienas vai laikposmā, ko izmeklētāja iestāde uzskata par atbilstīgu;

c) nodarbinātība – meklē informāciju par pašreizējo un agrāko nodarbinātību, atsaucoties uz tādiem avotiem kā nodarbinātības reģistri, darba izpildes vai efektivitātes ziņojumi, kā arī uz darba devējiem vai vadītājiem;

d) militārais dienests – attiecīgos gadījumos pārbauda, vai persona dienējusi bruņotajos spēkos un kā demobilizēta; un

e) intervijas – kad tas paredzēts un atļauts attiecīgās valsts tiesību aktos, attiecīgo personu intervē (vienu vai vairākas reizes). Tāpat intervē citas personas, kas spēj objektīvi novērtēt attiecīgās personas pagātni, agrāk veiktās darbības, lojalitāti un uzticamību. Ja attiecīgajā valstī pastāv prakse, ka personai, kuras lietu izskata, prasa uzrādīt atsauksmes devējus, intervē arī viņus, ja vien nav pamatotu iemeslu to nedarīt.

12. Vajadzības gadījumā un saskaņā ar valsts normatīvajiem aktiem var veikt papildu izmeklēšanu, lai apkopotu visu atbilstīgo pieejamo informāciju par personu un pamatotu vai atspēkotu nelabvēlīgu informāciju.

Drošības pielaides atjaunošana

13. Kad sākotnēji piešķirta drošības pielaide un ar noteikumu, ka persona nepārtraukti darbojusies valsts pārvaldē vai PĢS un tai joprojām ir vajadzīga piekļuve ESKI, drošības pielaidi pārskata, lai to atjaunotu, ik pēc laikposma, kas nepārsniedz piecus gadus *TRÈS SECRET UE/EU TOP SECRET* līmeņa pielaidei un desmit gadus *SECRET UE/EU SECRET* un *CONFIDENTIEL UE/EU CONFIDENTIAL* līmeņa pielaidei, sākot no dienas, kad paziņots par pēdējās drošības pārbaudes rezultātiem, ar kuru attiecīgā pielaide pamatota. Visas drošības izmeklēšanas, lai atjaunotu drošības pielaidi, veic attiecībā uz laiku kopš iepriekšējās izmeklēšanas.

14. Drošības pielaides atjaunošanai attiecīgi izmeklē 10. un 11. punktā izklāstītos elementus.

15. Atjaunošanas pieteikumu iesniedz laikus, ņemot vērā laiku, kas vajadzīgs drošības izmeklēšanai. Tomēr, ja atbildīgā VDI vai cita kompetentā valsts iestāde ir saņēmusi attiecīgo atjaunošanas pieteikumu un personāla drošības anketu pirms drošības pielaides derīguma termiņa beigām, bet vajadzīgā drošības izmeklēšana vēl nav pabeigta, kompetentā valsts iestāde var pagarināt esošās drošības pielaides derīguma termiņu līdz 12 mēnešiem, ja tas atļauts saskaņā ar valsts normatīvajiem aktiem. Ja pēc šā papildu 12 mēnešu termiņa beigām drošības izmeklēšana joprojām nav pabeigta, personai nosaka tādus pienākumus, kuru pildīšanai drošības pielaide nav vajadzīga.

Atļaujas piešķiršanas procedūras PĢS

16. Attiecībā uz PĢS ierēdņiem un pārējiem darbiniekiem PĢS drošības iestāde nosūta aizpildītās personāla drošības anketas tās dalībvalsts VDI, kuras valstspiederīgā ir šī persona, un lūdz veikt drošības izmeklēšanu saistībā ar ESKI līmeni, kuram šai personai vajadzēs piekļūt.

▼B

17. Ja PĢS uzzina informāciju, kas attiecas uz personu, kura ir iesniegusi pieteikumu drošības pielaides saņemšanai, lai piekļūtu ESKI, un kas ir nozīmīga drošības izmeklēšanā, tas rīkojas atbilstīgi attiecīgiem noteikumiem un paziņo attiecīgajai VDI par šo informāciju.

18. Pēc drošības izmeklēšanas beigām attiecīgā VDI sniedz PĢS drošības iestādei izmeklēšanas rezultātus Drošības komitejas noteiktajā standarta saziņas formātā.

a) Ja drošības izmeklēšanas rezultātā apstiprinās, ka nav zināms nekas negatīvs, kā dēļ varētu apšaubīt personas lojalitāti un uzticamību, PĢS iecēlējinstitūcija var attiecīgajai personai piešķirt atļauju līdz konkrētam datumam piekļūt ESKI līdz konkrētam līmenim.

b) Ja drošības izmeklēšanas rezultātā nerodas šāda pārliecība, PĢS iecēlējinstitūcija dara to zināmu attiecīgajai personai, kura var lūgt, lai iecēlējinstitūcija viņu uzklausītu. Iecēlējinstitūcija var lūgt kompetento VDI sniegt papildu skaidrojumus, ko tā var sniegt saskaņā ar saviem valsts normatīvajiem aktiem. Ja negatīvo atzinumu apstiprina, atļauju piekļūt ESKI nepiešķir.

19. Uz drošības izmeklēšanu kopā ar iegūtajiem rezultātiem attiecas atbilstīgi normatīvie akti, kas ir spēkā attiecīgajā dalībvalstī, tostarp tiesību akti par pārsūdzēšanu. Uz PĢS iecēlējinstitūcijas lēmumiem attiecas pārsūdzēšanas iespēja saskaņā ar Eiropas Savienības Civildienesta noteikumiem un Eiropas Savienības Pārējo darbinieku nodarbināšanas kārtību, kā izklāstīts Padomes Regulā (EEK, Euratom, EOTK) Nr. 259/68 ([1]) (“Civildienesta noteikumi un Nodarbināšanas kārtība”).

20. Valsts eksperti, kas ir norīkoti darbam PĢS tādā amatā, kur vajadzīga piekļuve ESKI, kas klasificēta kā *CONFIDENTIEL UE/EU CONFIDENTIAL* un augstāk, pirms stāšanās amatā iesniedz PĢS drošības iestādei derīgu valsts personāla drošības pielaides apliecību (PDPA), lai nodrošinātu piekļuvi ESKI, uz ko pamatojoties PĢS iecēlējinstitūcija izdod atļauju piekļuvei ESKI.

21. PĢS akceptēs atļauju piekļūt ESKI, kuru piešķīrusi jebkura cita Savienības iestāde, struktūra vai aģentūra, ar noteikumu, ka tā joprojām ir spēkā. Atļauja būs spēkā attiecībā uz visiem attiecīgās personas uzdevumiem PĢS. Savienības iestāde, struktūra vai aģentūra, kurā persona stājas darbā, paziņos attiecīgajai VDI par darba devēja maiņu.

22. Ja personas darbs nesākas 12 mēnešos pēc tam, kad PĢS iecēlējinstitūcijai ziņots par drošības izmeklēšanas rezultātiem, vai ja personas darbā iestājas pārtraukums uz 12 mēnešiem un tā šajā laikā neieņem amatu dalībvalsts valsts pārvaldē vai PĢS, izmeklēšanas rezultātus pārsūta attiecīgajai VDI, lai apstiprinātu, ka tie joprojām ir derīgi un izmantojami.

23. Ja PĢS saņem informāciju, kas attiecas uz drošības risku, kuru izraisa persona, kam ir atļauja piekļūt ESKI, tas rīkojas saskaņā ar attiecīgajiem noteikumiem un paziņo šo informāciju attiecīgajai VDI, un var apturēt piekļuvi ESKI vai atcelt atļauju piekļūt ESKI.

([1]) Padomes Regula (EEK, Euratom, EOTK) Nr. 259/68 (1968. gada 29. februāris), ar ko nosaka Eiropas Kopienu Civildienesta noteikumus un Pārējo darbinieku nodarbināšanas kārtību (Civildienesta noteikumi) (OV L 56, 4.3.1968., 1. lpp.; Īpašais izdevums latviešu valodā, 1. nodaļa, 2. sējums, 5. lpp.).

▼B

24. Ja VDI informē PĢS par apstiprinājuma atsaukšanu saskaņā ar 18. punkta a) apakšpunktu attiecībā uz personu, kurai ir atļauja piekļūt ESKI, PĢS iecēlējinstitūcija var lūgt jebkuru paskaidrojumu, ko VDI var sniegt saskaņā ar savas valsts normatīvajiem aktiem. Ja negatīvā informācija tiek apstiprināta, atļauju atsauc, un personai liedz piekļuvi ESKI un amatiem, kuros šāda piekļuve ir iespējama vai kuros minētā persona varētu apdraudēt drošību.

25. Par jebkuru lēmumu atsaukt vai apturēt PĢS ierēdņa vai cita darbinieka atļauju piekļūt ESKI un attiecīgā gadījumā par tā iemesliem paziņo attiecīgajai personai, kura var lūgt, lai viņu uzklausītu iecēlējinstitūcija. Uz VDI sniegto informāciju attiecas atbilstīgi normatīvie akti, kas ir spēkā attiecīgajā dalībvalstī, tostarp tiesību normas par pārsūdzēšanu. Uz PĢS iecēlējinstitūcijas lēmumiem attiecas pārsūdzēšanas iespēja saskaņā ar Civildienesta noteikumiem un Nodarbināšanas kārtību.

Drošības pielaižu un atļauju reģistri

26. Visas dalībvalstis un PĢS uztur reģistrus attiecīgi par PDP un atļaujām, kas piešķirtas, lai piekļūtu informācijai, kas klasificēta kā *CONFIDENTIEL UE/EU CONFIDENTIAL* vai augstāk. Šajos reģistros iekļauj vismaz to ESKI klasifikācijas līmeni, kuram personai ir piešķirta piekļuve, drošības pielaides izsniegšanas datumu un derīguma termiņu.

27. Kompetentā drošības iestāde var izsniegt PDPA, norādot ESKI klasifikācijas līmeni, kuram personai var piešķirt piekļuvi (*CONFIDENTIEL UE/EU CONFIDENTIAL* vai augstāk), attiecīgās PDP, kas nodrošina piekļuvi ESKI, vai atļaujas, kas nodrošina piekļuvi ESKI, derīguma termiņu un apliecības derīguma beigu datumu.

Atbrīvojums no prasības par PDP

28. Tādu personu piekļuvi ESKI, kuras dalībvalstīs saņēmušas pienācīgu atļauju ieņemamā amata dēļ, nosaka saskaņā ar valsts normatīvajiem aktiem; šādas personas informē par drošības pienākumiem saistībā ar ESKI aizsardzību.

IV. IZGLĪTOŠANA UN INFORMĒŠANA PAR DROŠĪBU

29. Visas personas, kam piešķirta drošības pielaide, rakstiski apliecina, ka ir sapratušas savus pienākumus attiecībā uz ESKI aizsargāšanu un iespējamās sekas, ja ESKI ir apdraudēta. Šādu rakstisku apliecinājumu reģistrus attiecīgi glabā dalībvalsts un PĢS.

30. Visas personas, kas ir pilnvarotas piekļūt ESKI vai kam jārīkojas ar to, jau sākumā tiek informētas un vēlāk saņem regulāru atgādinājumu par drošības apdraudējumu, un tām ir nekavējoties jāinformē attiecīgās drošības iestādes par jebkuru tuvošanās mēģinājumu vai citu darbību, kas šķiet aizdomīga vai neparasta.

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

V. ĀRKĀRTĒJI APSTĀKĻI

32. Ja tas atļauts valsts normatīvajos aktos, tad, gaidot PDP izsniegšanu piekļuvei ESKI, valsts ierēdņiem var piešķirt piekļuvi līdzvērtīga līmeņa ESKI, kurš noteikts atbilstības tabulās B papildinājumā, – dalībvalsts kompetentās iestādes piešķir drošības pielaidi piekļūšanai valsts klasificētajai

▼B

informācijai uz noteiktu laiku, ja šāda pagaidu piekļuve ir Savienības interesēs. VDI informē Drošības komiteju, ja attiecīgās valsts normatīvajos aktos šāda pagaidu piekļuve ESKI nav atļauta.

33. Ārkārtas apstākļos, ja tas ir dienesta interesēs, un gaidot pilnīgas drošības izmeklēšanas beigas, PĢS iecēlējinstitūcija pēc konsultēšanās ar tās dalībvalsts VDI, kuras valstspiederīgais ir minētā persona, un ievērojot iepriekšējo pārbaužu rezultātus, kas apliecina, ka nav zināma nekāda negatīva informācija, var piešķirt PĢS ierēdņiem un pārējiem darbiniekiem pagaidu atļauju konkrētā darba uzdevumā piekļūt ESKI. Šādas pagaidu atļaujas ir derīgas uz laikposmu, kas nepārsniedz sešus mēnešus, un nesniedz piekļuvi informācijai, kas klasificēta kā *TRÈS SECRET UE/EU TOP SECRET*. Visas personas, kam piešķirta pagaidu piekļuve, rakstiski apliecina, ka ir sapratušas savus pienākumus attiecībā uz ESKI aizsargāšanu un iespējamās sekas, ja ESKI ir apdraudēta. Šādu rakstisku apliecinājumu reģistrus glabā PĢS.

34. Ja personu ieceļ amatā, kam vajadzīga augstāka līmeņa drošības pielaide nekā tā, kas tai ir, tad šo personu var iecelt amatā uz laiku ar noteikumu, ka:

a) personas tiešais priekšnieks rakstiski pamato obligāto vajadzību piekļūt augstāka līmeņa ESKI;

b) piekļuve attiecas tikai uz konkrētām ESKI daļām, kas vajadzīgas uzdevumam;

c) personai jau ir derīga PDP vai atļauja piekļūt ESKI;

d) ir sāktas darbības, lai iegūtu attiecīgajam amatam vajadzīgā līmeņa atļauju;

e) kompetentā iestāde veikusi pietiekamas pārbaudes un pārliecinājusies, ka persona nav nopietni vai atkārtoti pārkāpusi drošības noteikumus;

f) personas iecelšanu apstiprinājusi kompetentā iestāde; un

g) attiecīgā reģistrā vai pakārtotā reģistrā fiksē datus par izņēmuma gadījumu, ietverot tās informācijas aprakstu, kurai ir apstiprināta piekļuve.

35. Minētās procedūras izmanto vienreizējai piekļuvei ESKI, kas ir klasificēta par vienu līmeni augstāk nekā tā, kuras piekļuvei persona ir izturējusi drošības pārbaudi. Minēto procedūru neizmanto atkārtoti.

36. Ārkārtas izņēmuma gadījumos, piemēram, misijās naidīgā vidē vai laikā, kad pieaug starptautiskais saspīlējums, ja to prasa ārkārtas pasākumi, jo īpaši – lai glābtu dzīvības, dalībvalstis un ģenerālsekretārs var attiecīgā gadījumā rakstiski piešķirt piekļuvi *CONFIDENTIEL UE/EU CONFIDENTIAL* vai *SECRET UE/EU SECRET* līmenī klasificētai informācijai personām, kam nav vajadzīgās drošības pielaides, ja tāda atļauja ir obligāti vajadzīga un nav pamatotu šaubu par attiecīgās personas lojalitāti un uzticamību. Tiek fiksēti dati par piešķirto atļauju, norādot arī tās informācijas aprakstu, kurai ir sniegta piekļuve.

▼B

37. Ja informācija ir klasificēta kā *TRÈS SECRET UE*/EU TOP SECRET, ārkārtas piekļuvi piešķir tikai Savienības pilsoņiem, kam ir piešķirta piekļuve vai nu *TRÈS SECRET UE*/*EU TOP SECRET* līdzvērtīgai valsts klasifikācijai, vai informācijai, kas klasificēta kā *SECRET UE/EU SECRET*.

38. Drošības komiteju informē par gadījumiem, kad tiek izmantota 36. un 37. punktā izklāstītā procedūra.

39. Ja dalībvalsts normatīvajos aktos paredzēti stingrāki noteikumi par pagaidu atļaujām, pagaidu uzdevumiem, vienreizēju piekļuvi vai ārkārtas piekļuvi klasificētai informācijai, šajā iedaļā paredzētās procedūras īsteno tikai tiktāl, ciktāl tas atļauts attiecīgajos valsts normatīvajos aktos.

40. Drošības komiteja katru gadu saņem ziņojumu par šajā iedaļā izklāstīto procedūru izmantojumu.

VI. PADOMES SANĀKSMJU APMEKLĒŠANA

41. Saskaņā ar 28. punktu personas, kas nosūtītas piedalīties Padomes darba sagatavošanas struktūru sanāksmēs, kurās apspriež informāciju, kas klasificēta kā *CONFIDENTIEL UE/EU CONFIDENTIAL* vai augstāk, var tajās piedalīties tikai tad, ja ir apstiprināts viņu drošības pielaides statuss. Attiecībā uz delegātiem PDP apliecību vai citus drošības pielaides pierādījumus PĢS Drošības birojam nosūta attiecīgās iestādes vai – izņēmuma gadījumā – iesniedz attiecīgais delegāts. Attiecīgā gadījumā var izmantot konsolidētu sarakstu ar personu vārdiem, sniedzot vajadzīgo drošības pielaides pierādījumu.

42. Kompetentā iestāde informē PĢS, ja drošības apsvērumu dēļ ir atcelta PDP, lai piekļūtu ESKI, personai, kuras pienākumos ietilpst apmeklēt Padomes vai Padomes darba sagatavošanas struktūru sanāksmes.

VII. IESPĒJAMA PIEKĻUVE ESKI

43. Kurjeri, apsargi un eskortētāji iziet attiecīga līmeņa drošības pārbaudes, vai attiecībā uz viņiem saskaņā ar valsts normatīvajiem aktiem veic atbilstīgu izmeklēšanu, viņus instruē par ESKI aizsardzības drošības procedūrām un dara viņiem zināmu pienākumu sargāt uzticēto informāciju.

▼B

II PIELIKUMS

FIZISKĀ DROŠĪBA

I. IEVADS

1. Šajā pielikumā izklāstīti 8. panta īstenošanas noteikumi. Ar šo pielikumu nosaka fiziskās aizsardzības minimuma standartus telpās, ēkās, birojos un citās zonās, kur rīkojas ar ESKI un to glabā, tostarp zonās, kur atrodas KIS.

2. Fiziskās drošības pasākumi ir paredzēti, lai novērstu neatļautu piekļuvi ESKI:

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

b) pieļaujot personāla nošķīrumu atbilstīgi tā pielaidei ESKI, ņemot vērā principu par vajadzību pēc informācijas un – attiecīgā gadījumā – viņu drošības pielaidi;

c) novēršot, aizkavējot un atklājot neatļautas darbības; un

d) neatļaujot vai aizkavējot iekļūšanu slepus vai ar spēku.

II. FIZISKĀS DROŠĪBAS PRASĪBAS UN PASĀKUMI

3. Fiziskās drošības pasākumus izvēlas, pamatojoties uz kompetento iestāžu veiktu apdraudējuma izvērtējumu. PĢS un dalībvalsts savās telpās ESKI aizsargāšanai piemēro riska pārvaldības procesu, lai nodrošinātu, ka piemēro tāda līmeņa fizisko aizsardzību, kas ir samērīga novērtētajam riskam. 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) novērtēto apdraudējumu, ko rada izlūkošanas dienesti, kuri vēršas pret Savienību vai dalībvalstīm, un sabotāža, terorisms un citas graujošas vai kriminālas darbības.

4. Piemērojot pastiprinātas aizsardzības koncepciju, kompetentā drošības iestāde nosaka piemērotu īstenojamo fiziskās drošības pasākumu kopumu. Šajā kopumā var tikt iekļauts viens vai vairāki šādi pasākumi:

a) perimetra barjera – fiziska barjera, ar kuru nosaka aizsargājamās zonas robežas;

b) ielaušanās konstatācijas sistēma (IKS) – IKS var izmantot uz perimetra, lai pastiprinātu barjeras sniegto drošību, vai arī to var izmantot telpās un ēkās drošības personāla vietā vai tā atbalstam;

▼B

c) piekļuves kontrole – piekļuves kontroli veic vietā, ēkā vai ēkās, kuras atrodas vietā, vai zonās vai telpās ēkas iekšienē. Kontrole var būt elektroniska vai elektromehāniska, to var veikt drošības personāls un/vai sekretārs, vai ar citiem fiziskiem līdzekļiem;

d) drošības personāls – var pieņemt darbā drošības personālu, kas ir apmācīts, uzraudzīts un vajadzības gadījumā ar atbilstīgu pielaidi, *inter alia*, lai novērstu iespējamu ielaušanos;

e) videonovērošanas sistēma (*CCTV*) – drošības personāls var izmantot *CCTV*, lai pārbaudītu starpgadījumus un IKS trauksmes signālus plašās vietās vai uz perimetra;

f) drošības apgaismojums – var izmantot drošības apgaismojumu, lai novērstu iespējamu ielaušanos, kā arī nodrošina apgaismojumu, kas vajadzīgs efektīvai uzraudzībai, ko drošības personāls veic vai nu tieši, vai arī netieši, izmantojot *CCTV* sistēmu; un

g) citi atbilstīgi fiziski pasākumi, kas paredzēti neatļautas piekļuves novēršanai un atklāšanai vai ESKI zuduma vai bojājuma novēršanai.

5. Kompetentā drošības iestāde var būt pilnvarota pārmeklēt personas pie ieejas vai izejas, lai novērstu materiālu neatļautu ievešanu vai ESKI neatļautu izvešanu no telpām vai ēkām.

6. Ja pastāv risks, ka ESKI varētu slepus novērot (pat nejauši), veic atbilstīgus pasākumus, lai novērstu šo risku.

7. Attiecībā uz jaunām iekārtām fiziskās drošības prasības un to darbības specifikācijas pēc iespējas iekļauj iekārtu plānošanā un izveidē. Jau esošās iekārtās fiziskās drošības prasības īsteno pēc iespējas lielākā apjomā.

III. IEKĀRTAS FIZISKAI ESKI AIZSARDZĪBAI

8. Iegādājoties iekārtas (piemēram, seifus, smalcinātājus, durvju slēdzenes, elektroniskas piekļuves kontroles sistēmas, IKS, signalizācijas sistēmas) fiziskai ESKI aizsargāšanai, kompetentā drošības iestāde nodrošina, ka iekārtas atbilst apstiprinātiem tehniskiem standartiem un minimuma prasībām.

9. Fiziskai ESKI aizsardzībai izmantojamo iekārtu tehniskās specifikācijas ir izklāstītas drošības pamatnostādnēs, kas jāapstiprina Drošības komitejai.

10. Drošības sistēmas periodiski pārbauda un veic iekārtu regulāru apkopi. Apkopes darbā ņem vērā pārbaužu rezultātus, lai nodrošinātu, ka iekārtas turpina maksimāli efektīvi darboties.

11. Katrā pārbaudē pārskata atsevišķu drošības pasākumu un visas drošības sistēmas efektivitāti.

IV. FIZISKI AIZSARGĀTAS ZONAS

12. Fiziskai ESKI aizsardzībai izveido divu veidu fiziski aizsargātas zonas vai tām līdzvērtīgas valsts zonas:

▼B

a) administratīvās zonas; un

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

Šajā lēmumā visas atsauces uz administratīvām zonām un drošības zonām, tostarp tehniski drošām drošības zonām, attiecas arī uz valsts zonām, kas tām līdzvērtīgas.

13. Kompetentā drošības iestāde nosaka, vai zona atbilst prasībām, lai to varētu kvalificēt kā administratīvo zonu, drošības zonu un tehniski drošu drošības zonu.

14. Attiecībā uz administratīvām zonām:

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

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

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

15. 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 var piešķirt tikai personām, kurām ir drošības pielaide un īpaša atļauja iekļūt zonā, pamatojoties uz principu par vajadzību pēc informācijas; un

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

16. Gadījumos, kad praktiskā nolūkā piekļuve drošības zonām ir saistīta ar 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 nav iespējama jebkāda veida piekļuve ESKI.

17. Drošības zonas, kuras ir aizsargātas pret slepenu noklausīšanos ar skaņas pārtveršanu, raksturo kā tehniski drošas drošības zonas. Piemēro šādas papildu prasības:

a) šādas zonas ir aprīkotas ar IKS, aizslēgtas, kad tajās neviena nav, vai apsargātas, kad tajās kāds uzturas. Visas atslēgas pārbauda saskaņā ar VI iedaļu;

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

▼B

c) šādās zonās veic regulāras fiziskas un/vai tehniskas pārbaudes, kā to nosaka kompetentā drošības iestāde. Minētās pārbaudes veic arī katru reizi pēc jebkādas neatļautas iekļuves vai aizdomām par šādu iekļuvi; un

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

18. Neatkarīgi no 17. 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 kā *SECRET UE/EU SECRET* un augstāk, un apstākļos, kad ESKI apdraudējumu vērtē kā augstu, tās pārbauda kompetentā drošības iestāde, lai nodrošinātu, ka ārpus drošības zonas perimetra ar šādām ierīcēm netīšām vai nelikumīgi nepārraidītu nekādu saprotamu informāciju.

19. 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 tur nav IKS.

20. Administratīvā zonā uz laiku var izveidot drošības zonas un tehniski drošas drošības zonas, lai organizētu slepenu sanāksmi vai citiem līdzīgiem mērķiem.

21. Katrai drošības zonai izstrādā drošības darba procedūras, kurās paredz:

a) klasifikācijas līmeni ESKI, 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 pielaidi;

d) attiecīgā gadījumā – eskortēšanas vai ESKI aizsardzības procedūras, sniedzot jebkuriem citiem apmeklētājiem piekļuvi zonai; un

e) citus attiecīgus pasākumus un procedūras.

22. Drošības zonās izveido glabātavas. Sienas, grīdas, griestus, logus un aizslēdzamas durvis apstiprina kompetentā drošības iestāde, un tās sniedz aizsardzību, kas ir līdzvērtīga tāda seifa sniegtajai aizsardzībai, kurš apstiprināts tās pašas klasifikācijas līmeņa ESKI glabāšanai.

V. FIZISKĀS AIZSARDZĪBAS PASĀKUMI, RĪKOJOTIES AR ESKI UN TO GLABĀJOT

23. Ar ESKI, kas klasificēta kā *RESTREINT UE/EU RESTRICTED*, var rīkoties:

a) drošības zonā;

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

▼B

c) ārpus drošības vai administratīvās zonas, ja informācijas turētājs pārvieto ESKI saskaņā ar III pielikuma 28. līdz 41. punktu un ja viņš veic kompensācijas pasākumus, kas izklāstīti kompetentās drošības iestādes izdotās drošības instrukcijās, lai nodrošinātu, ka ESKI ir aizsargāta pret nesankcionētu personu piekļuvi.

24. ESKI, kas klasificēta kā *RESTREINT UE/EU RESTRICTED*, glabā piemērotās aizslēdzamās biroja mēbelēs administratīvā zonā vai drošības zonā. To uz laiku var glabāt ārpus drošības vai administratīvās zonas, ja informācijas turētājs veic kompensācijas pasākumus, kas izklāstīti kompetentās drošības iestādes izdotās drošības instrukcijās.

25. Ar ESKI, kas klasificēta kā *CONFIDENTIEL UE/EU CONFIDENTIAL* vai *SECRET UE/EU SECRET*, 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) pārvieto ESKI saskaņā ar III pielikuma 28. līdz 41. punktu;

ii) veic kompensācijas pasākumus, kas izklāstīti kompetentās drošības iestādes izdotās drošības instrukcijās, lai nodrošinātu, ka ESKI ir aizsargāta pret nesankcionētu personu piekļuvi;

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

iv) gadījumā, ja dokumenti ir papīra formā, par šo faktu ir informējis atbilstīgo reģistru.

26. ESKI, kas klasificēta kā *CONFIDENTIEL UE/EU CONFIDENTIAL* un *SECRET UE/EU SECRET*, glabā drošības zonā vai nu seifā, vai glabātavā.

27. Ar ESKI, kas klasificēta kā *TRÈS SECRET UE/EU TOP SECRET*, rīkojas drošības zonā.

28. ESKI, kas klasificēta kā *TRÈS SECRET UE/EU TOP SECRET*, glabā drošības zonā saskaņā ar vienu no šiem nosacījumiem:

a) saskaņā ar 8. punktu seifā ar vismaz vienu no papildu kontroles pasākumiem:

i) drošības pārbaudi izturējuša drošības personāla vai dienesta personāla veikta nepārtraukta aizsardzība vai pārbaudes;

ii) apstiprināta IKS kopā ar drošības darbiniekiem;

b) glabātavā, kas aprīkota ar IKS, kopā ar drošības darbiniekiem.

▼B

29. Noteikumi attiecībā uz ESKI pārvietošanu ārpus fiziski aizsargātām zonām ir izklāstīti III pielikumā.

VI. ESKI AIZSARDZĪBAI IZMANTOTO ATSLĒGU UN KODU KOMBINĀCIJU KONTROLE

30. Kompetentā drošības iestāde nosaka procedūras biroju, telpu, glabātavu un seifu atslēgu un kodu kombināciju parametru pārzināšanai. Šādas procedūras aizsargā pret neatļautu piekļuvi.

31. Seifu kombinācijas jāiegaumē pēc iespējas mazākam to personu skaitam, kas atbilst vajadzības pēc informācijas principam. To seifu un glabātavu kodu kombinācijas, kuros glabājas ESKI, maina:

a) saņemot jaunu seifu;

b) ja ir mainījies personāls, kas zina šo kodu kombināciju;

c) ja ir īstenojies apdraudējums vai ir aizdomas, ka tas ir īstenojies;

d) veicot slēdzenes apkopi vai remontu; un

e) vismaz reizi 12 mēnešos.

▼B

III PIELIKUMS

KLASIFICĒTAS INFORMĀCIJAS PĀRVALDĪBA

I. IEVADS

1. Šajā pielikumā izklāstīti 9. panta īstenošanas noteikumi. Tajā paredz administratīvus pasākumus ESKI kontrolei visā tās aprites cikla laikā, lai palīdzētu novērst un atklāt tīšu vai netīšu šādas informācijas apdraudējumu vai nozaudēšanu.

II. KLASIFIKĀCIJAS PĀRVALDĪBA

Klasifikācijas un marķējumi

2. Informāciju klasificē, ja tā ir jāaizsargā, lai nodrošinātu tās konfidencialitāti.

3. ESKI autors atbild par to, lai noteiktu drošības klasifikācijas līmeni saskaņā ar attiecīgajām pamatnostādnēm, un par sākotnējo informācijas izplatīšanu.

4. ESKI klasifikācijas līmeni nosaka saskaņā ar 2. panta 2. punktu un atsaucoties uz drošības politiku, kas jāapstiprina saskaņā ar 3. panta 3. punktu.

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

6. 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.

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

8. Dokumenti, kas ietver daļas ar dažādiem klasifikācijas līmeņiem, pēc iespējas jāveido tā, lai daļas ar dažādiem klasifikācijas līmeņiem varētu viegli identificēt un vajadzības gadījumā atdalīt.

9. Pavadvēstules vai piezīmes klasifikācija ir tikpat augsta kā tai pievienoto dokumentu visaugstākā klasifikācija. 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*

Marķējums

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

a) identifikatori, ar ko nosaka informācijas autoru;

b) brīdinājumi, kodu vārdi vai akronīmi, ar ko precizē darbības jomu, uz kuru attiecas dokuments, vai lai norādītu konkrētu izplatīšanu, pamatojoties uz vajadzību pēc informācijas, vai lietošanas ierobežojumus;

c) marķējumi attiecībā uz nodošanu; vai

▼B

d) attiecīgā gadījumā datums vai konkrēts notikums, pēc kura informāciju var klasificēt zemākā kategorijā vai deklasificēt.

Klasifikācijas marķējumu saīsinājumi

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

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

TRÈS 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*

ESKI gatavošana

13. Gatavojot ES klasificētu dokumentu:

a) katru lappusi skaidri marķē atbilstīgi klasifikācijas līmenim;

b) katru lappusi numurē;

c) uz dokumenta raksta atsauces numuru un tematu, kurš pats par sevi nav klasificēta informācija, ja vien tas nav marķēts kā klasificēta informācija;

d) dokumentu datē; un

e) dokumentiem, kas klasificēti kā *SECRET UE/EU SECRET* vai augstāk, katrā lappusē norāda kopijas numuru, ja tie jāizplata vairākos eksemplāros.

14. Ja ESKI nav iespējams piemērot 13. punktu, veic citus piemērotus pasākumus saskaņā ar drošības pamatnostādnēm, kuras jāizstrādā, ievērojot 6. panta 2. punktu.

ESKI klasifikācijas līmeņa pazemināšana un deklasifikācija

15. Gatavojot informāciju, tās autors, ja iespējams, un īpaši informācijai, kas klasificēta kā *RESTREINT UE/EU RESTRICTED*, norāda, vai var pazemināt ESKI slepenības pakāpi vai to deklasificēt konkrētā dienā vai pēc konkrēta notikuma.

16. PĢS regulāri pārskata ESKI, kas atrodas tā rīcībā, lai pārliecinātos, vai attiecīgais klasifikācijas līmenis joprojām ir piemērots. PĢS izveido sistēmu, lai ne retāk kā ik pēc pieciem gadiem pārskatītu klasifikācijas līmeni ESKI, kas nāk no Padomes Ģenerālsekretariāta. Šādu pārskatu neveic, ja autors jau no sākuma ir norādījis, ka informācijas slepenības pakāpi automātiski pazemina vai deklasificē, un uz informācijas ir attiecīgs marķējums.

III. ESKI REĢISTRĀCIJA DROŠĪBAS NOLŪKĀ

17. Katru PĢS un dalībvalstu valsts pārvaldes organizatorisko vienību, kurā rīkojas ar ESKI, pievieno atbildīgajam reģistram, lai nodrošinātu, ka ar ESKI rīkojas saskaņā ar šo lēmumu. Reģistrus veido kā II pielikumā definētās drošības zonas.

▼B

18. Šajā lēmumā reģistrācija drošības nolūkā ("reģistrācija") ir tādu procedūru piemērošana, kas reģistrē materiālu aprites ciklu, tostarp tā izplatīšanu un iznīcināšanu.

19. Visus materiālus, kas klasificēti kā *CONFIDENTIEL UE/EU CONFIDENTIAL* un augstāk, reģistrē norādītos reģistros, kad tie tiek saņemti organizatoriskā vienībā vai tiek izsūtīti no tās.

20. PĢS Centrālais reģistrs reģistrē visu klasificēto informāciju, ko Padome un PĢS nodod trešām valstīm un starptautiskām organizācijām, un visu klasificēto informāciju, ko saņem no trešām valstīm un starptautiskām organizācijām.

21. KIS gadījumā reģistrācijas procedūras var veikt ar procesiem, kas ietilpst pašās KIS.

22. Padome apstiprina drošības politiku attiecībā uz ESKI reģistrāciju drošības nolūkā.

***TRÈS SECRET UE/EU TOP SECRET* reģistri**

23. Dalībvalstīs un PĢS izveido reģistru, un tas darbojas kā galvenā *TRÈS SECRET UE/EU TOP SECRET* klasificētas informācijas saņemšanas un izplatīšanas iestāde. Vajadzības gadījumā var nozīmēt pakārtotus reģistrus, kurā rīkojas ar šādu informāciju reģistrēšanas nolūkā.

24. Pakārtoti reģistri bez centrālā *TRÈS SECRET UE/EU TOP SECRET* informācijas reģistra skaidri izteiktas rakstiskas atļaujas nedrīkst *TRÈS SECRET UE/EU TOP SECRET* dokumentus tieši nosūtīt ne citiem tā paša centrālā *TRÈS SECRET UE/EU TOP SECRET* informācijas reģistra pakārtotajiem reģistriem, ne ārējiem reģistriem.

IV. ES KLASIFICĒTU DOKUMENTU KOPĒŠANA UN TULKOŠANA

25. *TRÈS SECRET UE/EU TOP SECRET* dokumentus nedrīkst kopēt un tulkot bez autora iepriekšējas rakstiskas piekrišanas.

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

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

V. ESKI PĀRVIETOŠANA

28. Uz ESKI pārvietošanu attiecas aizsardzības pasākumi, kas izklāstīti 30. līdz 41. punktā. Ja ESKI pārvieto ar elektroniskām iekārtām un neatkarīgi no 9. panta 4. punkta turpmāk tekstā izklāstītos aizsardzības pasākumus var papildināt ar attiecīgiem tehniskiem pretpasākumiem, kā to noteikusi kompetentā drošības iestāde, lai cik vien iespējams samazinātu informācijas apdraudējuma vai zaudējuma risku.

29. PĢS un dalībvalstu kompetentās drošības iestādes dod norādes attiecībā uz ESKI pārvietošanu saskaņā ar šo lēmumu.

Pārvietošana ēkā vai noslēgtā ēku grupā

30. Ja ESKI pārvieto ēkā vai noslēgtā ēku grupā, to apsedz, lai novērstu to, ka kāds redz tās saturu.

▼B

31. Informāciju, kas klasificēta kā *TRÈS SECRET UE/EU TOP SECRET*, ēkā vai noslēgtā ēku grupā pārnēsā nodrošinātā aploksnē, uz kuras ir norādīts tikai adresāta vārds.

Savienībā

32. ESKI, ko Savienībā pārvieto no vienas ēkas vai telpas uz citu, iepako, lai tā būtu aizsargāta no neatļautas izpaušanas.

33. Informāciju, kuras klasifikācijas līmenis ir *CONFIDENTIEL UE/EU CONFIDENTIAL* vai *SECRET UE/EU SECRET*, Savienībā pārvieto, izmantojot vienu no šādiem veidiem:

a) attiecīgā gadījumā izmantojot militāro, valdības vai diplomātisko kurjeru;

b) rokas bagāžā ar noteikumu, ka:

i) ESKI visu laiku atrodas pārnēsātāja valdījumā, ja vien tā netiek glabāta saskaņā ar prasībām, kas noteiktas II pielikumā;

ii) ESKI neatver pārnēsāšanas laikā vai nelasa publiskās vietās;

iii) personas tiek informētas par to pienākumiem saistībā ar drošību; un

iv) vajadzības gadījumā personām izsniedz kurjera apliecību;

c) izmantojot pasta pakalpojumus vai komerciālus kurjeru pakalpojumus ar noteikumu, ka:

i) valsts drošības iestādes tos ir apstiprinājušas saskaņā ar attiecīgās valsts normatīvajiem aktiem; un

ii) tiem piemēro piemērotus aizsargpasākumus saskaņā ar minimālajām prasībām, kas jānosaka drošības pamatnostādnēs, ievērojot 6. panta 2. punktu.

Gadījumā, ja veic pārvietošanu no vienas dalībvalsts uz citu dalībvalsti, c) apakšpunkta noteikumus attiecina vienīgi uz informāciju, kas klasificēta līmenī līdz *CONFIDENTIEL UE/EU CONFIDENTIAL*.

34. Informāciju, kas klasificēta kā *RESTREINT UE/EU RESTRICTED*, var pārvietot, arī izmantojot pasta pakalpojumus vai komerciālus kurjeru pakalpojumus. Šādas informācijas parvietošanai kurjera apliecība nav nepieciešama.

35. Materiālus, kas klasificēti kā *CONFIDENTIEL UE/EU CONFIDENTIAL* un *SECRET UE/EU SECRET* (piemēram, iekārtas un mašīnas) un ko nevar pārvietot ar 33. punktā minētajiem līdzekļiem, nogādā, izmantojot kravu pārvadājumus, ko veic komercpārvadātāji saskaņā ar V pielikumu.

36. Informāciju, kas klasificēta kā *TRÈS SECRET UE/EU TOP SECRET*, no vienas ēkas vai telpas uz citu Savienībā pārvieto, attiecīgā gadījumā izmantojot militāro, valdības vai diplomātisko kurjeru.

Pārvietošana no Savienības uz kādas trešās valsts teritoriju

37. ESKI, ko no Savienības pārvieto uz kādas trešās valsts teritoriju, iepako, lai tā būtu aizsargāta no neatļautas izpaušanas.

▼B

38. Informāciju, kas klasificēta kā *CONFIDENTIEL UE/EU CONFIDENTIAL* un *SECRET UE/EU SECRET*, no Savienības uz kādas trešās valsts teritoriju pārvieto šādi:

a) izmantojot militāro vai diplomātisko kurjeru;

b) rokas bagāžā ar noteikumu, ka:

i) uz iepakojuma ir oficiāls zīmogs vai informācija ir iepakota tā, lai norādītu, ka tas ir oficiāls sūtījums un tam nebūtu jāpiemēro muitas vai drošības pārbaudes;

ii) personām ir kurjera apliecība, ar ko identificē sūtījumu un ļauj šai personai to pārvietot;

iii) ESKI visu laiku atrodas pārnēsātāja valdījumā, ja vien tā netiek glabāta saskaņā ar prasībām, kas noteiktas II pielikumā;

iv) ESKI neatver pārnēsāšanas laikā vai nelasa publiskās vietās; un

v) personas tiek informētas par to pienākumiem saistībā ar drošību.

39. Informāciju, kas ir klasificēta kā *CONFIDENTIEL UE/EU CONFIDENTIAL* un *SECRET UE/EU SECRET* un ko Savienība ir sniegusi trešām valstīm vai starptautiskām organizācijām, pārvieto saskaņā informācijas drošības nolīguma vai administratīvas vienošanās attiecīgajiem noteikumiem, kā noteikts 13. panta 2. punkta a) vai b) apakšpunktā.

40. Informāciju, kas klasificēta kā *RESTREINT UE/EU RESTRICTED*, var pārvietot, arī izmantojot pasta pakalpojumus vai komerciālus kurjeru pakalpojumus.

41. Informāciju, kas klasificēta kā *TRÈS SECRET UE/EU TOP SECRET*, no Savienības uz kādas trešās valsts teritoriju pārvieto, izmantojot militāro vai diplomātisko kurjeru.

VI. ESKI IZNĪCINĀŠANA

42. ES klasificētos dokumentus, kas vairs nav vajadzīgi, var iznīcināt, neskarot attiecīgos arhivēšanas noteikumus.

43. Dokumentus, kurus reģistrē saskaņā ar 9. panta 2. punktu, pēc to turētāja vai kompetentās iestādes rīkojuma iznīcina reģistrs, kas atbild par šiem dokumentiem. Reģistrācijas žurnālus un pārējo reģistrācijas informāciju atbilstīgi atjaunina.

44. Kā *SECRET UE/EU SECRET* vai *TRÈS SECRET UE/EU TOP SECRET* klasificētus dokumentus iznīcina liecinieka klātbūtnē – lieciniekam jābūt vismaz tāda līmeņa pielaidei, kas atbilst iznīcināmā dokumenta klasifikācijas līmenim.

45. Reģistrētājs un liecinieks, ja ir vajadzīga viņa klātbūtne, paraksta iznīcināšanas sertifikātu, ko iekļauj reģistrā. *TRÈS SECRET UE/EU TOP SECRET* dokumentu iznīcināšanas sertifikātus reģistrā saglabā vismaz desmit gadus un *CONFIDENTIEL UE/EU CONFIDENTIAL* un *SECRET UE/EU SECRET* dokumentu iznīcināšanas sertifikātus – vismaz piecus gadus.

46. Klasificētos dokumentus, tostarp tos, kas klasificēti kā *RESTREINT UE/EU RESTRICTED*, iznīcina ar tādām metodēm, kuras atbilst attiecīgiem

▼B

Savienības vai līdzvērtīgiem standartiem vai kuras apstiprinājusi dalībvalsts saskaņā ar valsts tehniskajiem standartiem, lai novērstu pilnīgu vai daļēju dokumentu atjaunošanu.

47. ESKI izmantotu elektronisko informācijas nesēju iznīcināšana notiek saskaņā ar IV pielikuma 37. punktu.

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

VII. IZVĒRTĒJUMA APMEKLĒJUMI

49. Ar terminu "izvērtējuma apmeklējums" turpmāk apzīmē jebkuru:

a) pārbaudi vai izvērtējuma apmeklējumu saskaņā ar 9. panta 3. punktu un 16. panta 2. punkta e), f) un g) apakšpunktu; vai

b) izvērtējuma apmeklējumu saskaņā ar 13. panta 5. punktu,

lai izvērtētu ESKI aizsardzībai īstenoto pasākumu efektivitāti.

50. Izvērtējuma apmeklējumus veic, lai *inter alia*:

a) nodrošinātu, ka tiek ievēroti šajā lēmumā minētie ESKI aizsardzībai noteiktie minimālie standarti;

b) uzsvērtu, cik svarīga ir drošība un iedarbīga riska pārvaldība pārbaudāmajās vienībās;

c) konkrētos gadījumos ieteiktu pretpasākumus, lai samazinātu kaitējumu, ko rada klasificētas informācijas konfidencialitātes, integritātes vai piekļuves režīma neievērošana; un

d) stiprinātu pašreizējās programmas, ko drošības iestādes īsteno, izglītojot un informējot par dažādiem jautājumiem drošības jomā.

51. Pirms katra kalendārā gada beigām Padome pieņem 16. panta 1. punkta c) apakšpunktā noteikto nākamajam gadam paredzēto izvērtējuma apmeklējumu programmu. Faktiskos datumus katram izvērtējuma apmeklējumam nosaka, vienojoties ar attiecīgo Savienības struktūru vai aģentūru, dalībvalsti, trešo valsti vai starptautisko organizāciju.

Izvērtējuma apmeklējumu veikšana

52. Izvērtējuma apmeklējumus veic, lai pārbaudītu attiecīgos apmeklētās vienības noteikumus un procedūras un pārliecinātos, vai tās prakse atbilst pamatprincipiem un minimālajiem standartiem, kas paredzēti šajā lēmumā, un noteikumiem, ar ko reglamentē klasificētas informācijas apmaiņu ar šo iestādi.

53. Izvērtējuma apmeklējumus veic divos posmos. Vajadzības gadījumā pirms paša izvērtējuma apmeklējuma ar konkrēto vienību rīko izvērtējuma sagatavošanas sanāksmi. Pēc šādas sagatavošanas sanāksmes vērtētāju grupa saziņā ar attiecīgo vienību sīki izstrādā izvērtējuma apmeklējuma programmu, aptverot visas drošības jomas. Izvērtējuma apmeklējumu grupai vajadzētu būt piekļuvei visām vietām, jo īpaši reģistriem un KIS punktiem, kur rīkojas ar ESKI.

54. Izvērtējuma apmeklējumus dalībvalstu valsts pārvaldes iestādēs, trešās valstīs un starptautiskās organizācijās veic pilnīgā sadarbībā ar tās vienības, trešās valsts vai starptautiskās organizācijas ierēdņiem, kuru apmeklē.

▼B

55. Izvērtējuma apmeklējumus Savienības struktūrās, aģentūrās un vienībās, kuras piemēro šo lēmumu vai tā principus, veic ar tās VDI speciālistu palīdzību, kuras teritorijā šī struktūra vai aģentūra atrodas.

56. Kad veic izvērtējuma apmeklējumus Savienības struktūrās, aģentūrās un vienībās, kuras piemēro šo lēmumu vai tā principus, kā arī trešās valstīs un starptautiskās organizācijās, VDI ekspertu palīdzību un ieguldījumu var lūgt saskaņā ar sīki izstrādātiem noteikumiem, par kuriem jāvienojas Drošības komitejai.

Ziņojumi

57. Izvērtējuma apmeklējuma beigās galvenos secinājumus un ieteikumus iesniedz apmeklētajai vienībai. Pēc tam izstrādā izvērtējuma apmeklējuma ziņojumu. Ja ziņojumā ir ierosinātas darbības un ieteikumi trūkumu novēršanai, tajā ietver arī pietiekami sīku aprakstu, lai pamatotu gūtos secinājumus. Ziņojumu nosūta attiecīgajai apmeklētās vienības iestādei.

58. Attiecībā uz dalībvalstu valsts pārvaldes iestādēs veiktiem izvērtējuma apmeklējumiem:

a) izvērtējuma ziņojuma projektu nosūtīs attiecīgajai VDI, lai pārliecinātos, ka tajā uzskaitītie fakti ir pareizi un ka tajā nav informācijas, kas klasificēta ar augstāku slepenības pakāpi nekā *RESTREINT UE/EU RESTRICTED*; un

b) ja vien attiecīgās dalībvalsts VDI nav lūgusi atturēties no vispārējas izplatīšanas, izvērtējuma ziņojumus nosūta Drošības komitejai. Ziņojumam piešķir klasifikāciju *RESTREINT UE/EU RESTRICTED*.

PĢS drošības iestādes (Drošības biroja) atbildībā regulāri sagatavo ziņojumu, lai izceltu pieredzi, kas gūta konkrētā laikposmā dalībvalstīs veiktajos izvērtējuma apmeklējumos un ko izskatījusi Drošības komiteja.

59. Trešo valstu un starptautisko organizāciju izvērtējuma apmeklējumu vajadzībām ziņojumu nosūta Drošības komitejai. Ziņojumam piešķir klasifikāciju, kas nav zemāka par *RESTREINT UE/EU RESTRICTED*. Nākamajos apmeklējumos pārbauda, vai ir veiktas koriģējošas darbības, un par to ziņo Drošības komitejai.

60. Attiecībā uz to Savienības struktūru, aģentūru un vienību izvērtējuma apmeklējumiem, kuras piemēro šo lēmumu vai tā principus, izvērtējuma apmeklējumu ziņojumus nosūta Drošības komitejai. Izvērtējuma apmeklējuma ziņojuma projektu nosūta attiecīgajai aģentūrai vai struktūrai, lai pārliecinātos, ka tajā uzskaitītie fakti ir pareizi un ka tajā nav informācijas, kas klasificēta ar augstāku slepenības pakāpi nekā *RESTREINT UE/EU RESTRICTED*. Nākamajos apmeklējumos pārbauda, vai ir veiktas koriģējošas darbības, un par to ziņo Drošības komitejai.

61. PĢS drošības iestāde PĢS organizatoriskajās vienībās veic regulāras pārbaudes 50. punktā paredzētajos nolūkos.

Kontrolsaraksts

62. PĢS drošības iestāde (Drošības birojs) izstrādā un atjaunina tādu priekšmetu kontrolsarakstu, kuri jāpārbauda izvērtējuma apmeklējuma laikā. Šo kontrolsarakstu nosūta Drošības komitejai.

63. Informāciju, kas vajadzīga kontrolsaraksta aizpildīšanai, iegūst jo īpaši apmeklējuma laikā no pārbaudāmo vienību drošības pārvaldības. Pēc kontrolsaraksta papildināšanas ar detalizētām atbildēm tam, vienojoties ar pārbaudīto vienību, piešķir klasifikāciju. Tas neveido daļu no pārbaudes ziņojuma.

▼B

IV PIELIKUMS

ESKI AIZSARDZĪBA, RĪKOJOTIES AR TO KOMUNIKĀCIJU UN INFORMĀCIJAS SISTĒMĀS

I. IEVADS

1. Šajā pielikumā izklāstīti 10. panta īstenošanas noteikumi.

2. Lai darbības KIS notiktu droši un pareizi, būtiskas ir šādas IA īpašības un koncepcijas:

Autentiskums:	garantija, ka informācija ir īsta un saņemta no *bona fide* avotiem.
Pieejamība:	tai var piekļūt un to var izmantot pēc pilnvarotas vienības pieprasījuma.
Konfidencialitāte:	informāciju neatklāj nesankcionētām personām, vienībām un procesiem.
Integritāte:	spēja nosargāt informācijas un materiālu precizitāti un pilnīgumu.
Nenoliedzamība:	spēja pierādīt, ka darbība vai notikums ir noticis, lai vēlāk nevarētu noliegt, ka šāds notikums vai darbība ir notikusi.

II. INFORMĀCIJAS AIZSARDZĪBAS PRINCIPI

3. Turpmāk izklāstītie noteikumi veido jebkuras tādas KIS drošības pamatus, kurā rīkojas ar ESKI. IA drošības politikā un drošības pamatnostādnēs nosaka sīki izstrādātas minēto noteikumu īstenošanas prasības.

Drošības riska pārvaldība

4. Drošības riska pārvaldība ir neatņemama daļa KIS definēšanā, izstrādē, darbībā un uzturēšanā. Riska pārvaldību (izvērtējums, risinājums, pieņemšana, paziņošana) veic kā atkārtotu procesu kopīgi ar sistēmu īpašnieku pārstāvjiem, projekta iestādēm, darbības iestādēm un drošības apstiprināšanas iestādēm, izmantojot apliecinātu, pārskatāmu un pilnīgi izprotamu riska izvērtējuma procesu. KIS darbības jomu un tās materiālus skaidri definē riska pārvaldības procesa sākumā.

5. Kompetentās iestādes pārskata iespējamos KIS apdraudējumus un uztur aktuālus un precīzus apdraudējumu izvērtējumus, kas atspoguļo pašreizējo darbības vidi. Tās pastāvīgi atjaunina informāciju par ietekmējamību un periodiski pārskata ietekmējamības izvērtējumu, lai atbilstu mainīgajai informāciju tehnoloģiju (IT) videi.

6. Drošības riska risinājuma mērķis ir piemērot drošības pasākumu kopumu, kuru rezultātā panāk apmierinošu līdzsvaru starp lietotāja vajadzībām, izmaksām un atlikušo drošības risku.

7. Atbilstīgās DAI noteiktās detalizācijas īpašās prasības, darbības mērogs un pakāpe atbilst novērtētajam riskam, ņemot vērā visus atbilstīgos faktorus, tostarp klasifikācijas līmeni ESKI, ar ko rīkojas KIS. Akreditācijā ietver oficiālu paziņojumu par atlikušo risku un to, ka atbildīgā iestāde pieņem atlikušo risku.

▼B

Drošība visā KIS aprites cikla laikā

8. Drošība ir būtiska prasība, kas ir aktuāla visā KIS aprites ciklā no sākuma līdz izņemšanai no aprites.

9. Katram aprites cikla posmam nosaka katra dalībnieka, kas saistīts ar KIS saistībā ar tās drošību, lomu un sadarbības veidu.

10. Jebkurā KIS, tostarp tās tehniskajos drošības pasākumos un pasākumos, kas nav tehniski drošības pasākumi, akreditācijas laikā veic drošības pārbaudes, lai pārliecinātos, ka panākts piemērots aizsardzības līmenis, un pārbaudītu, ka tie ir pareizi īstenoti, integrēti un konfigurēti.

11. KIS darbības posmā un uzturēšanas laikā periodiski, kā arī ja rodas ārkārtas apstākļi, veic drošības izvērtējumus, pārbaudes un pārskatīšanu.

12. Drošības informācija KIS vajadzībām tās aprites ciklā mainās kā neatņemama pārmaiņu procesa un konfigurācijas vadības daļa.

Paraugprakse

13. PĢS un dalībvalstis sadarbojas, lai izveidotu kopīgu aizsardzības paraugpraksi attiecībā uz ESKI, ar kuru rīkojas KIS. Paraugprakses pamatnostādnēs iekļauj KIS tehniskus, fiziskus, organizatoriskus un procedūras drošības pasākumus, kuru iedarbība cīņā pret konkrētiem apdraudējumiem un ietekmējamību ir pierādīta.

14. ESKI, ar kuru rīkojas KIS, aizsardzībā izmanto pieredzi, ko guvušas IA iesaistītās vienības gan Savienībā, gan ārpus tās.

15. Paraugprakses izplatīšana un turpmāka īstenošana palīdz panākt līdzvērtīgu aizsardzības līmeni dažādās PĢS un dalībvalstu vadītās KIS, kurās rīkojas ar ESKI.

Padziļināta aizsardzība

16. Lai mazinātu risku komunikāciju un informācijas sistēmai, īsteno plaša spektra tehniskus drošības pasākumus un pasākumus, kas nav tehniski drošības pasākumi, izveidojot daudzslāņainu aizsardzību. Minētie slāņi ir:

a) *atturēšana:* drošības pasākumi, lai atturētu no jebkādiem kaitnieciskiem plāniem, kas vērsti pret KIS;

b) *preventīva rīcība:* drošības pasākumi, kuru mērķis ir traucēt vai novērst pret KIS vērstu uzbrukumu;

c) *atklāšana:* drošības pasākumi, kuru mērķis ir atklāt pret KIS vērstu uzbrukumu;

d) *izturība:* drošības pasākumi, kuru mērķis ir maksimāli ierobežot uzbrukuma ietekmi uz informācijas kopumu vai KIS materiāliem un pasargāt tos no turpmākiem bojājumiem; un

e) *reģenerācija:* drošības pasākumi, kuru mērķis ir atjaunot drošu KIS stāvokli.

Minēto drošības pasākumu stingrību nosaka pēc riska izvērtējuma.

17. VDI vai cita kompetentā iestāde nodrošina, ka:

a) tiek īstenotas kiberaizsardzības spējas, lai reaģētu uz apdraudējumiem, kas var sniegties pāri organizācijas un valsts robežām; un

▼B

b) tiek koordinēta reakcija uz šiem apdraudējumiem, incidentiem un saistīto risku (ārkārtas reaģēšanas spējas datordrošības jomā) un notiek dalīšanās ar informāciju par tiem.

Ierobežojumu un mazākās konfidencialitātes pielaides princips

18. Lai izvairītos no lieka riska, ievieš tikai būtiskās darbībai vajadzīgās funkcijas, iekārtas un dienestus.

19. KIS lietotājiem un automatizētiem procesiem nodrošina tikai tādu piekļuvi, privilēģijas vai pilnvaras, kas vajadzīgas to pienākumu veikšanai, lai tādējādi ierobežotu negadījumu, kļūdu vai neatļautas KIS resursu izmantošanas rezultātā radušos bojājumus.

20. Reģistrācijas procedūras, kuras veic KIS, vajadzības gadījumā pārbauda akreditācijas procesa laikā.

Informētība par informācijas aizsardzību

21. Informētība par risku un pieejamiem drošības pasākumiem ir KIS drošības aizsardzības pirmais priekšnoteikums. Visas personas, kas iesaistītas KIS aprites ciklā, tostarp tās lietotāji, saprot:

a) ka trūkumi drošības sistēmā var būtiski kaitēt KIS;

b) ka savstarpējās savienojamības un atkarības dēļ kaitējums var tikt nodarīts arī citiem; un

c) ka tās personiski atbild un atskaitās par KIS drošību saskaņā ar saviem pienākumiem sistēmās un procesos.

22. Lai nodrošinātu, ka atbildība par drošības garantēšanu ir izprasta, viss iesaistītais personāls, tostarp augstākā līmeņa vadība un KIS lietotāji, obligāti saņem izglītību un apmācību par IA.

IT drošības produktu izvērtēšana un apstiprināšana

23. Vajadzīgo uzticamības līmeni drošības pasākumos, ko definē kā aizsardzības līmeni, nosaka atbilstīgi riska pārvaldības procesā gūtajiem rezultātiem un saskaņā ar attiecīgo drošības politiku un drošības pamatnostādnēm.

24. Aizsardzības līmeni pārbauda, lietojot starptautiski plaši izmantotus vai valstī apstiprinātus procesus un metodoloģijas. Tas ietver sākotnējo izvērtēšanu, kontroli un revīziju.

25. ESKI aizsardzībai paredzētos kriptogrāfijas produktus izvērtē un apstiprina dalībvalsts valsts KAI.

26. Pirms ieteikt Padomei vai ģenerālsekretāram šādus kriptogrāfijas produktus apstiprināt saskaņā ar 10. panta 6. punktu, tos otru reizi veiksmīgi izvērtē tās dalībvalsts atbilstīgi apstiprināta iestāde (*AQUA*), kas nepiedalās aprīkojuma projektēšanā un ražošanā. Otrās izvērtēšanas detalizācijas pakāpe ir atkarīga no paredzētā maksimālā tādas ESKI klasifikācijas līmeņa, kas jāsargā, izmantojot šos produktus. Padome apstiprina drošības politiku attiecībā uz kriptogrāfijas produktu izvērtēšanu un apstiprināšanu.

27. Ja tas pamatots ar īpašiem operatīviem apsvērumiem, Padome vai ģenerālsekretārs pēc Drošības komitejas ieteikuma var attiecīgi atteikties no šā pielikuma 25. vai 26. punktā noteiktajām prasībām un saskaņā ar 10. panta 6. punktā noteikto procedūru piešķirt pagaidu apstiprinājumu uz konkrētu laikposmu.

▼B

28. Padome pēc Drošības komitejas ieteikuma var akceptēt trešās valsts vai starptautiskas organizācijas kriptogrāfijas produktu izvērtēšanas, atlases un apstiprināšanas procesu un attiecīgi uzskatīt šādus kriptogrāfijas produktus par apstiprinātiem, lai aizsargātu ESKI, kas nodota minētajai trešai valstij vai starptautiskai organizācijai.

29. *AQUA* ir tās dalībvalsts KAI, kas ir akreditēta, pamatojoties uz Padomes noteiktiem kritērijiem, lai uzņemtos tādu kriptogrāfijas produktu otrreizēju izvērtēšanu, ar ko paredzēts aizsargāt ESKI.

30. Padome apstiprina drošības politiku attiecībā uz tādu IT produktu kvalificēšanu un apstiprināšanu, kas nav saistīti ar kriptogrāfiju.

Pārsūtīšana drošās un administratīvās zonās

31. Neatkarīgi no šā lēmuma noteikumiem, ja ESKI nosūta tikai drošās zonās vai administratīvās zonās, nešifrētu nosūtīšanu vai zemāka līmeņa šifrēšanu var izmantot, pamatojoties uz riska pārvaldības procesa rezultātiem un ar drošības akreditācijas iestādes apstiprinājumu.

Drošs KIS savstarpējs savienojums

32. Šajā lēmumā sistēmu savstarpējs savienojums ir tieši savienotas divas vai vairākas IT sistēmas, lai dalītos ar datiem un citiem informācijas resursiem (piemēram, saziņu) vienā vai vairākos virzienos.

33. KIS jebkuru pieslēgtu IT sistēmu uzskata par neuzticamu un ievieš aizsargpasākumus, lai kontrolētu informācijas apmaiņu.

34. Visi KIS un citas IT sistēmas savstarpēji savienojumi atbilst šādām pamatprasībām:

a) kompetentās iestādes nosaka un apstiprina šādu savienojumu darbības vai operatīvās prasības;

b) savstarpējam savienojumam piemēro riska pārvaldības un akreditācijas procesu, un to apstiprina kompetentās DAI; un

c) visu KIS perimetrā izvieto robežu aizsardzības dienestus (*BPS*).

35. Nedrīkst savstarpēji savienot akreditētu KIS un neaizsargātu vai publiski pieejamu tīklu, izņemot gadījumus, ja KIS apstiprinājusi šādiem mērķiem ieviesto *BPS* starp KIS un neaizsargāto vai publiski pieejamo tīklu. Šādu savstarpēju savienojumu drošības pasākumus pārskata kompetentā IAI un apstiprina kompetentā DAI.

Ja neaizsargāto vai publiski pieejamo tīklu izmanto vienīgi tādas informācijas transportēšanai, kura ir šifrēta ar kriptogrāfijas produktu, kas apstiprināts saskaņā ar 10. pantu, šādu savienojumu neuzskata par savstarpēju savienojumu.

36. Ir aizliegts tādas KIS, kas ir akreditēta rīkoties ar *TRÈS SECRET UE/EU TOP SECRET* informāciju, tiešs vai pakāpenisks savstarpējs savienojams ar neaizsargātu vai publiski pieejamu tīklu.

Elektroniskie informācijas nesēji

37. Elektroniskus informācijas nesējus iznīcina saskaņā ar kompetentās drošības iestādes apstiprinātām procedūrām.

▼B

38. Elektroniskus informācijas nesējus var izmantot atkārtoti, klasificēt zemākā kategorijā vai deklasificēt saskaņā ar drošības pamatnostādnēm, kas ir jānosaka saskaņā ar 6. panta 2. punktu.

Ārkārtas apstākļi

39. Neatkarīgi no šā lēmuma noteikumiem ārkārtas gadījumā, piemēram, gaidāmas vai notiekošas krīzes laikā, konflikta vai kara situācijā vai ārkārtas operatīvajā situācijā, var piemērot turpmāk aprakstītās īpašās procedūras.

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

a) sūtītājam un saņēmējam nav vajadzīgo kriptogrāfijas iekārtu vai nav nekādu kriptogrāfijas iekārtu; un

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

41. Klasificētā informācijā, kas nosūtīta 39. punktā izklāstītajos apstākļos, nav atzīmju 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.

42. Ja tiek izmantota 39. punkta procedūra, kompetentajai iestādei un Drošības komitejai par to sniedz ziņojumu.

III. INFORMĀCIJAS AIZSARDZĪBAS FUNKCIJAS UN IESTĀDES

43. Dalībvalstīs un PĢS nosaka šādas IA funkcijas. Minēto funkciju pildīšanai nav vajadzīgas vienotas organizatoriskas vienības. Tām ir atsevišķas pilnvaras. Tomēr šīs funkcijas un ar tām saistītos pienākumus var apvienot vai integrēt vienā un tai pašā organizatoriskajā vienībā vai sadalīt dažādās organizatoriskās vienībās ar noteikumu, ka nerodas iekšēji interešu vai uzdevumu konflikti.

Informācijas aizsardzības iestāde

44. IAI atbildībā ir:

a) izstrādāt IA drošības politiku un drošības pamatnostādnes un pārraudzīt to efektivitāti un piemērotību;

b) nodrošināt un administrēt tehnisko informāciju, kas attiecas uz kriptogrāfijas produktiem;

c) nodrošināt, ka ESKI aizsardzībai izraudzītie IA pasākumi atbilst attiecīgajai politikai, kas nosaka to atbilstību un atlasi;

d) nodrošināt, ka kriptogrāfijas produktus izraugās saskaņā ar politiku, kas nosaka to atbilstību un atlasi;

e) koordinēt apmācību un informēšanu par IA;

f) konsultēties ar sistēmas sniedzēju, drošības dalībniekiem un lietotāju pārstāvjiem par IA drošības politiku un drošības pamatnostādnēm; un

g) nodrošināt, ka Drošības komitejas apakšgrupā ir pieejami piemēroti IA jautājumu eksperti.

▼B

***TEMPEST* iestāde**

45. *TEMPEST* iestāde (TI) atbild par to, lai nodrošinātu KIS atbilstību *TEMPEST* politikai un pamatnostādnēm. Tā apstiprina *TEMPEST* pretpasākumus iekārtām un produktiem, lai aizsargātu ESKI līdz noteiktam klasifikācijas līmenim tās ekspluatācijas vidē.

Kriptogrāfijas apstiprinājuma iestāde

46. Kriptogrāfijas apstiprinājuma iestāde (KAI) atbild par to, lai nodrošinātu, ka kriptogrāfijas produkti atbilst valsts kriptogrāfijas politikai vai Padomes kriptogrāfijas politikai. Tā apstiprina kriptogrāfijas produkta izmantošanu ESKI aizsargāšanai līdz noteiktam klasifikācijas līmenim tās ekspluatācijas vidē. Attiecībā uz dalībvalstīm KAI ir atbildīga arī par to, lai izvērtētu kriptogrāfijas produktus.

Kriptogrāfijas izplatīšanas iestāde

47. Kriptogrāfijas izplatīšanas iestāde (KII) ir atbildīga par šādiem jautājumiem:

a) ES kriptogrāfiskā materiāla pārvaldība un uzskaite;

b) nodrošināt, ka tiek īstenotas atbilstīgas procedūras un tiek izveidoti kanāli ES kriptogrāfiskā materiāla uzskaitei, drošam rīkošanās procesam, glabāšanai un izplatīšanai; un

c) nodrošināt ES kriptogrāfiskā materiāla nosūtīšanu atsevišķām personām vai dienestiem, kas tos izmanto, vai saņemt minētos materiālus no tiem.

Drošības akreditācijas iestāde

48. DAI attiecībā uz katru sistēmu atbild par šādiem uzdevumiem:

a) nodrošināt, ka KIS atbilst attiecīgajai drošības politikai un drošības pamatnostādnēm, sniegt paziņojumus par to, ka KIS ir apstiprināta savā ekspluatācijas vidē rīkoties ar ESKI līdz konkrētam klasifikācijas līmenim, norādīt akreditācijas noteikumus un kritērijus, pēc kādiem nosaka vajadzību veikt atkārtotu apstiprināšanu;

b) izstrādāt drošības akreditācijas procesu atbilstīgi attiecīgajai politikai, skaidri nosakot apstiprināšanas noteikumus KIS, par ko tā ir atbildīga;

c) noteikt drošības akreditācijas stratēģiju, paredzot akreditācijas procesa sarežģītības pakāpi, kas ir samērīga ar vajadzīgo aizsardzības līmeni;

d) izskatīt un apstiprināt ar drošību saistītu dokumentāciju, tostarp riska pārvaldību un paziņojumus par atlikušo risku, katras sistēmas drošības prasību izklāstus ("*SSRS*"), drošības īstenošanas pārbaudes dokumentus un drošības darba procedūras ("*SecOPs*"), un nodrošināt, ka tas atbilst Padomes drošības noteikumiem un politikai;

e) pārbaudīt, kā tiek īstenoti ar KIS saistīti drošības pasākumi, veicot vai atbalstot drošības novērtējumus, pārbaudes vai pārskatus;

f) noteikt ar KIS saistītas drošības prasības (piemēram, personāla pielaides līmeņus) palielināta riska amatos;

g) apstiprināt tādu kriptogrāfijas un *TEMPEST* produktu atlasi, ko izmanto, lai KIS nodrošinātu konfidencialitāti, integritāti un pieejamību;

▼B

h) apstiprināt tādas KIS savienošanu ar citām KIS vai attiecīgā gadījumā piedalīties to kopīgā apstiprināšanā; un

i) sniegt konsultācijas sistēmas sniedzējam, drošības sistēmas dalībniekiem un lietotāju pārstāvjiem attiecībā uz drošības riska pārvaldību, jo īpaši par atlikušo risku, un apstiprināšanas paziņojuma noteikumiem.

49. PĢS DAI atbild par visu to KIS akreditāciju, kuru darbība ir PĢS pārziņā.

50. Atbilstīgā dalībvalstu DAI ir atbildīga par KIS un tādu KIS sastāvdaļu akreditāciju, kuru darbība ir dalībvalsts pārziņā.

51. Kopīga drošības akreditācijas valde (*SAB*) ir atbildīga par tādu KIS akreditāciju, kuras ir gan PĢS DAI, gan dalībvalstu DAI pārziņā. Tās sastāvā ir DAI pārstāvji no katras dalībvalsts, un tās sanāksmēs piedalās Komisijas DAI pārstāvis. Citas vienības, kuras ir iesaistītas KIS, aicina piedalīties diskusijās, kad tiek apspriesta konkrētā sistēma.

SAB vada PĢS DAI pārstāvis. Tā darbojas ar to iestāžu, dalībvalstu un citu vienību pārstāvju konsensu, kuri ir iesaistīti KIS. Tā par savām darbībām periodiski iesniedz ziņojumus Drošības komitejai un informē to par visiem akreditācijas paziņojumiem.

Informācijas aizsardzības operatīvā iestāde

52. IA operatīvā iestāde attiecībā uz katru sistēmu atbild par šādiem uzdevumiem:

a) izstrādāt drošības dokumentāciju saskaņā ar drošības politiku un drošības pamatnostādnēm, jo īpaši *SSRS*, tostarp paziņojumu par atlikušo risku, *SecOPs* un kriptogrāfijas plānu saistībā ar KIS akreditācijas procesu;

b) piedalīties katrai sistēmai īpašu tehnisku drošības pasākumu, iekārtu un programmatūras izvēlē un pārbaudē, uzraudzīt to īstenošanu un nodrošināt, ka tās tiek droši instalētas, konfigurētas un uzturētas atbilstīgi attiecīgajiem drošības dokumentiem;

c) piedalīties *TEMPEST* drošības pasākumu un iekārtu izvēlē, ja tas pieprasīts *SSRS*, un sadarbībā ar TI nodrošināt, ka tās droši uzstāda un uztur;

d) uzraudzīt *SecOps* īstenošanu un piemērošanu un – attiecīgā gadījumā – atbildību par operatīvo drošību deleģēt sistēmas īpašniekam;

e) pārvaldīt un darboties ar kriptogrāfijas produktiem, nodrošinot šifrētu un kontrolētu materiālu uzraudzību, un vajadzības gadījumā nodrošināt kriptogrāfisku mainīgo veidošanu;

f) veikt drošības analīzes pārskatus un pārbaudes, jo īpaši – lai sagatavotu attiecīgos riska ziņojumus, kādus pieprasa DAI;

g) sniegt IA apmācību attiecībā uz katru KIS; un

h) īstenot un izpildīt drošības pasākumus attiecībā uz katru KIS.

▼B

V PIELIKUMS

INDUSTRIĀLĀ DROŠĪBA

I. IEVADS

1. Šajā pielikumā izklāstīti 11. panta īstenošanas noteikumi. Šajā pielikumā izklāstīti vispārēji drošības noteikumi, kas piemērojami rūpniecības vai citām vienībām pirms PĢS piešķirta klasificēta līguma slēgšanas un klasificēto līgumu aprites laikā.

2. Padome apstiprina industriālās drošības pamatnostādnes, jo īpaši uzsverot sīki izklāstītas prasības attiecībā uz iestādes drošības pielaidēm, drošības aspektu vēstulēm (DAV), apmeklējumiem, ESKI pārsūtīšanu un pārvietošanu.

II. KLASIFICĒTA LĪGUMA DROŠĪBAS ELEMENTI

Drošības klasifikācijas rokasgrāmata (DKR)

3. Pirms izsludināt konkursu vai pirms piešķirt klasificētu līgumu, PĢS kā līgumslēdzēja iestāde nosaka tās informācijas drošības klasifikāciju, kuru sniedz pretendentiem un līgumslēdzējiem, kā arī tās informācijas drošības klasifikāciju, ko sastādīs līgumslēdzējs. Šajā sakarā PĢS sagatavo drošības klasifikācijas rokasgrāmatu (DKR), kas jāizmanto līguma izpildei.

4. Lai noteiktu dažādu klasificēta līguma elementu drošības klasifikāciju, piemēro šādus principus:

a) izstrādājot DKR, PĢS ņem vērā visus attiecīgos drošības aspektus, tostarp drošības klasifikāciju, ko informācijas autors uz informāciju attiecinājis un apstiprinājis;

b) vispārējais līguma klasifikācijas līmenis nedrīkst būt zemāks par augstāko jebkura tā elementa klasifikāciju; un

c) vajadzības gadījumā PĢS sadarbojas ar dalībvalstu VDI/IDI vai kādu citu attiecīgo kompetento drošības iestādi, ja mainās tādas informācijas klasifikācija, ko līgumslēdzēji sagatavojuši vai kas tiem sniegta līguma izpildei, un ja jāveic ar to saistītas izmaiņas DKR.

Drošības aspektu vēstule (DAV)

5. Ar attiecīgo līgumu saistītās drošības prasības izklāsta drošības aspektu vēstulē (DAV). Attiecīgā gadījumā DAV iekļauj DKR, un tā ir neatņemama klasificēta līguma vai apakšlīguma daļa.

6. DAV iekļauj nosacījumus par to, ka līgumslēdzējam un/vai apakšlīgumslēdzējam ir jānodrošina atbilsme minimālajiem standartiem, kas izklāstīti šajā lēmumā. Neatbilstība šiem minimālajiem standartiem var būt pietiekams pamats līguma izbeigšanai.

Programmas/projekta drošības instrukcijas (PDI)

7. Atkarībā no to projektu vai programmu darbības jomas, kurās vajadzīga piekļuve ESKI vai kurās ar to jārīkojas vai jāglabā, līgumslēdzēja iestāde, kurai uzticēta atbildība par minētās programmas vai projekta pārvaldību,

▼B

var izstrādāt konkrētu PDI. PDI jāapstiprina dalībvalstu VDI/IDI vai kādai citai attiecīgajai kompetentajai drošības iestādei, kas piedalās PDI, un tajās var būt ietvertas papildu drošības prasības.

III. IESTĀDES DROŠĪBAS PIELAIDE (IDP)

8. IDP piešķir dalībvalsts VDI/IDI vai jebkura cita kompetentā iestāde, lai saskaņā ar valsts normatīvajiem aktiem apliecinātu, ka rūpniecības vai cita vienība savās telpās spēj nodrošināt pietiekamu ESKI aizsardzību attiecīgā klasifikācijas līmenī (*CONFIDENTIEL UE/EU CONFIDENTIAL* vai *SECRET UE/EU SECRET*). To iesniedz PĢS kā līgumslēdzējai iestādei, pirms līgumslēdzējam vai apakšlīgumslēdzējam vai iespējamam līgumslēdzējam vai apakšlīgumslēdzējam var piešķirt vai nodrošināt piekļuvi ESKI.

9. Izsniedzot IDP, attiecīgā VDI vai IDI vismaz:

a) novērtē rūpniecības vai citas vienības integritāti;

b) novērtē atbildību, kontroli vai iespējas izdarīt neatļautu ietekmi, ko var uzskatīt par drošības risku;

c) pārbauda, vai rūpniecības vai cita vienība iestādē ir izveidojusi drošības sistēmu, kurā ietverti visi atbilstīgie drošības pasākumi, kas vajadzīgi, lai aizsargātu informāciju vai materiālus, kas saskaņā ar šajā lēmumā izklāstītajām prasībām klasificēti kā *CONFIDENTIEL UE/EU CONFIDENTIAL* vai *SECRET UE/EU SECRET*;

d) pārbauda, vai to vadības, īpašnieku un darbinieku personāla drošības statuss, kuriem vajadzīga piekļuve informācijai, kas klasificēta kā *CONFIDENTIEL UE/EU CONFIDENTIAL* vai *SECRET UE/EU SECRET*, ir noteikts saskaņā ar šajā lēmumā noteiktajām prasībām; un

e) pārbauda, vai rūpniecības vai cita vienība ir iecēlusi iestādes drošības ierēdni, kurš ir atbildīgs savas vadības priekšā par drošības pienākumu īstenošanu šajā vienībā.

10. Ja vajadzīgs, PĢS kā līgumslēdzēja iestāde paziņo attiecīgajai VDI/IDI vai jebkurai citai kompetentajai drošības iestādei, ka IDP ir vajadzīga pirms līguma parakstīšanas vai līguma pildīšanas laikā. Pirms līguma parakstīšanas pieprasa IDP vai PDP, ja priekšlikuma iesniegšanas procesā ir jāsniedz ESKI, kas klasificēta kā *CONFIDENTIEL UE/EU CONFIDENTIAL* vai *SECRET UE/EU SECRET*.

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

12. VDI/IDI vai kāda cita kompetentā drošības iestāde, kas izsniegusi IDP, paziņo PĢS kā līgumslēdzējai iestādei par izmaiņām, kas ietekmē IDP.

▼B

Apakšlīguma gadījumā attiecīgi informē VDI/IDI vai citu kompetento drošības iestādi.

13. Ja attiecīgā VDI/IDI vai kāda cita kompetentā drošības iestāde atceļ IDP, tas ir pietiekams pamats PĢS kā līgumslēdzējai iestādei izbeigt klasificētu līgumu vai izslēgt attiecīgo pretendentu no konkursa.

IV. KLASIFICĒTI LĪGUMI UN APAKŠLĪGUMI

14. Ja pretendentam sniedz ESKI pirms līguma parakstīšanas, aicinājumā piedalīties iekļauj prasību, ka pretendentam, kurš neiesniedz priekšlikumu vai kuru neizvēlas, noteiktā laikposmā ir jāatdod atpakaļ visi klasificētie dokumenti.

15. Kad klasificētais līgums vai apakšlīgums ir piešķirts, PĢS kā līgumslēdzēja iestāde paziņo līgumslēdzēja vai apakšlīgumslēdzēja VDI/IDI vai jebkurai citai kompetentajai drošības iestādei klasificētā līguma drošības noteikumus.

16. Kad tāds līgums tiek izbeigts, PĢS kā līgumslēdzēja iestāde (un/vai VDI/IDI vai attiecīgi jebkura cita kompetentā drošības iestāde apakšlīguma gadījumā) nekavējoties par to paziņo tās dalībvalsts VDI/IDI vai jebkurai citai kompetentajai drošības iestādei, kurā līgumslēdzējs vai apakšlīgumslēdzējs reģistrēts.

17. Parasti līgumslēdzējam vai apakšlīgumslēdzējam jāatgriežas pie līgumslēdzējas iestādes, ja pēc klasificēta līguma vai apakšlīguma beigšanas viņu rīcībā ir ESKI.

18. Drošības aspektu vēstulē noteikti konkrēti noteikumi attiecībā uz ESKI iznīcināšanu līguma darbības laikā vai pēc tā darbības beigšanās.

19. Ja līgumslēdzējam vai apakšlīgumslēdzējam ir atļauts saglabāt ESKI pēc līguma darbības beigām, viņš turpina ievērot šajā lēmumā noteiktos minimālos standartus un sargāt ESKI konfidencialitāti.

20. Nosacījumus par kārtību, kādā līgumslēdzējs var slēgt apakšlīgumu, definē gan izsludinātajā konkursā, gan līgumā.

21. Pirms līgumslēdzējs atsevišķas klasificēta līguma daļas nodod apakšlīgumslēdzējam, tas saņem atļauju no PĢS kā līgumslēdzējas iestādes. Nedrīkst piešķirt apakšlīgumu rūpniecības vai citām vienībām, kas reģistrētas valstī, kura nav ES dalībvalsts, ja tā nav noslēgusi informācijas drošības nolīgumu ar Savienību.

22. Līgumslēdzējs ir atbildīgs par to, lai visas apakšlīgumslēdzēja darbības tiktu veiktas saskaņā ar šajā lēmumā noteiktajiem minimālajiem standartiem un lai viņš pārsūta ESKI vai citu materiālu apakšlīgumslēdzējam tikai ar iepriekšēju rakstisku līgumslēdzējas iestādes piekrišanu.

23. Attiecībā uz ESKI, ko sagatavo vai ar ko rīkojas līgumslēdzējs vai apakšlīgumslēdzējs, līgumslēdzēja iestāde piemēro informācijas autora tiesības.

▼B

V. AR KLASIFICĒTIEM LĪGUMIEM SAISTĪTI APMEKLĒJUMI

24. Ja PĢS, līgumslēdzēju vai apakšlīgumslēdzēju personāls lūdz piekļuvi informācijai, kas klasificēta kā *CONFIDENTIEL UE/EU CONFIDENTIAL* vai *SECRET UE/EU SECRET*, viens otra telpās klasificēta līguma darbības laikā, apmeklējumus organizē sadarbībā ar VDI/IDI vai jebkuru citu attiecīgo kompetento drošības iestādi. Tomēr konkrētu projektu gadījumā VDI/IDI var vienoties arī par kārtību, saskaņā ar kuru tādus apmeklējumus var organizēt tieši.

25. Visiem apmeklētājiem ir attiecīgā PDP, un tie atbilst vajadzības pēc informācijas principam attiecībā uz ESKI, kas saistīta ar PĢS līgumu.

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

VI. ESKI NOSŪTĪŠANA UN PĀRVIETOŠANA

27. Attiecībā uz ESKI elektronisku nosūtīšanu piemēro 10. panta un IV pielikuma attiecīgos noteikumus.

28. Attiecībā uz ESKI pārvietošanu piemēro III pielikuma attiecīgos noteikumus saskaņā ar valsts normatīvajiem aktiem.

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

a) drošību garantē visos posmos sūtīšanas laikā no sūtīšanas vietas līdz galamērķim;

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

c) uzņēmumiem, kas nodrošina sūtīšanu, veic piemērotā līmeņa IDP. Šajos gadījumos personālam, kas rīkojas ar sūtījumu, veic drošības pārbaudi atbilstīgi I pielikumam;

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

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

f) 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.

VII. ESKI PĀRSŪTĪŠANA LĪGUMSLĒDZĒJIEM TREŠĀS VALSTĪS

30. ESKI pārsūta līgumslēdzējiem vai apakšlīgumslēdzējiem, kas atrodas trešās valstīs, atbilstīgi drošības pasākumiem, par kuriem vienojies PĢS kā līgumslēdzēja iestāde un tās trešās valsts VDI/IDI, kurā līgumslēdzējs reģistrēts.

▼B

VIII. *RESTREINT UE/EU RESTRICTED* KLASIFICĒTA INFORMĀCIJA

31. Sadarbībā ar attiecīgā gadījumā dalībvalsts VDI/IDI PĢS kā līgumslēdzēja iestāde, pamatojoties uz līguma noteikumiem, var veikt pārbaudes līgumslēdzēja/apakšlīgumslēdzēja telpās, lai pārbaudītu, vai tiek īstenoti līgumā noteiktie vajadzīgie drošības pasākumi, lai aizsargātu ESKI, kas klasificēta kā *RESTREINT UE/EU RESTRICTED*.

32. Ciktāl tas vajadzīgs saskaņā ar valsts normatīvajiem aktiem, PĢS kā līgumslēdzēja iestāde informē VDI/IDI vai jebkuru citu kompetento drošības iestādi par līgumiem vai apakšlīgumiem, kuros ir iekļauta *RESTREINT UE/EU RESTRICTED* klasificēta informācija.

33. Līgumslēdzējam vai apakšlīgumslēdzējam un viņu personālam nav vajadzīga IDP vai PDP attiecībā uz līgumiem, kurus piešķīris PĢS un kuros iekļauta informācija, kas klasificēta kā *RESTREINT UE/EU RESTRICTED*.

34. PĢS kā līgumslēdzēja iestāde izskata iesniegtos pieteikumus līgumiem, kuros vajadzīga piekļuve *RESTREINT UE/EU RESTRICTED* klasificētai informācijai, neatkarīgi no jebkuras prasības saistībā ar IDP vai PDP, kas var būt noteikta valsts normatīvajos aktos.

35. Nosacījumus par kārtību, kādā līgumslēdzējs var slēgt apakšlīgumu, definē saskaņā ar 21. punktu.

36. Ja līgumslēdzēja izmantotās komunikāciju un informācijas sistēmās ir ar līgumu saistīta informācija, kas klasificēta kā *RESTREINT UE/EU RESTRICTED*, tad PĢS kā līgumslēdzēja iestāde nodrošina, ka līgumā vai katrā apakšlīgumā ir noteiktas nepieciešamās tehniskās un administratīvās prasības attiecībā uz KIS akreditāciju, kas ir samērīgas ar novērtēto risku, ņemot vērā visus atbilstīgos faktorus. Līgumslēdzēja iestāde un attiecīgā VDI/IDI savstarpēji vienojas par tādu KIS akreditācijas darbības jomu.

▼B

VI PIELIKUMS

KLASIFICĒTAS INFORMĀCIJAS APMAIŅA AR TREŠĀM VALSTĪM UN STARPTAUTISKĀM ORGANIZĀCIJĀM

I. IEVADS

1. Šajā pielikumā izklāstīti 13. panta īstenošanas noteikumi.

II. KLASIFICĒTAS INFORMĀCIJAS APMAIŅAS SISTĒMAS

2. Ja Padome uzskata, ka pastāv ilgtermiņa vajadzība apmainīties ar klasificētu informāciju:

— noslēdz informācijas drošības nolīgumu vai

— vienojas par administratīviem pasākumiem

saskaņā ar 13. panta 2. punktu un III un IV iedaļu un pamatojoties uz Drošības komitejas ieteikumu.

3. Ja ESKI, kas izstrādāta KDAP operācijas vajadzībām, ir jānodod trešām valstīm vai starptautiskām organizācijām, kas piedalās šādā operācijā, un ja neviena no 2. punktā minētajām sistēmām nepastāv, ESKI nodošanu šādai trešai valstij vai starptautiskai organizācijai atbilstīgi V iedaļai reglamentē saskaņā ar:

— līdzdalības pamatnolīgumu,

— *ad hoc* līdzdalības nolīgumu vai

— ja nav neviena no iepriekšminētajiem – *ad hoc* administratīviem pasākumiem.

4. Ja nav 2. un 3. punktā minētās sistēmas un ja ir pieņemts lēmums nodot ESKI trešai valstij vai starptautiskai organizācijai izņēmuma *ad hoc* kārtā saskaņā ar VI iedaļu, šo trešo valsti vai starptautisko organizāciju lūdz rakstiski apliecināt, ka tā nodrošina tai nodotās ESKI aizsardzību saskaņā ar šajā lēmumā izklāstītajiem pamatprincipiem un minimālajiem standartiem.

III. INFORMĀCIJAS DROŠĪBAS NOLĪGUMI

5. Informācijas drošības nolīgumos paredz pamatprincipus un minimālos standartus, ar ko reglamentē klasificētas informācijas apmaiņu starp Savienību un trešo valsti vai starptautisku organizāciju.

6. Informācijas drošības nolīgumos 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 nolīgumos ņem vērā aizsardzības līmeni, kas noteikts trešās valsts vai attiecīgās starptautiskās organizācijas drošības noteikumos, struktūrās un procedūrās. Tos apstiprina Drošības komiteja.

7. ESKI apmaiņu saskaņā ar informācijas drošības nolīgumu neveic elektroniskā veidā, izņemot gadījumus, kad tas īpaši noteikts nolīgumā vai atbilstīgajos tehniskās īstenošanas pasākumos.

8. Ja Padome noslēdz informācijas drošības nolīgumu, katrā pusē nosaka reģistru par galveno punktu klasificētas informācijas saņemšanai un sniegšanai.

▼B

9. Lai izvērtētu attiecīgo trešās valsts vai attiecīgās starptautiskās organizācijas drošības noteikumu, struktūru un procedūru efektivitāti, veic izvērtējuma apmeklējumus, savstarpēji vienojoties ar attiecīgo trešo valsti vai starptautisko organizāciju. Minētos izvērtējuma apmeklējumus veic saskaņā ar attiecīgajiem III pielikuma noteikumiem un tajos izvērtē:

a) normatīvos aktus, 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 tāda līmeņa ESKI, kura jānodod.

10. Grupa, kas veic izvērtējuma apmeklējumu Savienības vārdā, izvērtē to, vai attiecīgie drošības noteikumi un procedūras trešā valstī vai starptautiskā organizācijā atbilst ESKI aizsardzībai dotajā līmenī.

11. Šādos apmeklējumos izdarītos secinājumus ietver ziņojumā – pamatojoties uz šo ziņojumu, Drošības komiteja nosaka maksimālo līmeni ESKI, ko attiecīgai trešai personai var izsniegt papīra veidā vai attiecīgā gadījumā elektroniskā formātā, kā arī visus pārējos īpašos noteikumus, ko piemēro informācijas apmaiņai ar minēto pusi.

12. Veic visas pūles, lai izpildītu pilnīgus drošības izvērtējuma apmeklējumus trešā valstī vai attiecīgā starptautiskā organizācijā, pirms Drošības komiteja ir apstiprinājusi īstenošanas pasākumus, lai noteiktu pastāvošās drošības sistēmas veidu un efektivitāti. Tomēr, ja tas nav iespējams, Drošības komiteja no PĢS Drošības biroja saņem pēc iespējas pilnīgāku ziņojumu, pamatojoties uz tam pieejamo informāciju, ar ko Drošības komiteja tiek informēta par piemērojamiem drošības noteikumiem un drošības pasākumu organizēšanu attiecīgajā trešā valstī vai starptautiskā organizācijā.

13. Pirms ESKI faktiskās nodošanas attiecīgajai trešai valstij vai starptautiskai organizācijai izvērtējuma apmeklējuma ziņojumu vai, ja šāda ziņojuma nav, 12. punktā minēto ziņojumu nosūta Drošības komitejai, kura to atzīst par apmierinošu.

14. Savienības iestāžu un struktūru kompetentās drošības iestādes paziņo trešai valstij vai starptautiskai organizācijai dienu, ar kuru Savienība ir tiesīga nodot ESKI saskaņā ar nolīgumu, kā arī maksimālo ESKI līmeni, ar ko var apmainīties papīra formā vai elektroniski.

15. Turpmākus izvērtējuma apmeklējumus veic vajadzības gadījumā, jo īpaši, ja:

a) ir vajadzība palielināt nodotamās ESKI līmeni;

b) Savienībai ir paziņots par būtiskām izmaiņām trešās valsts vai starptautiskas organizācijas drošības pasākumos, kas varētu ietekmēt to, kā tā aizsargā ESKI; vai

c) ir bijis nopietns incidents, kas saistīts ar neatļautu ESKI izpaušanu.

▼B

16. Pēc tam, kad informācijas drošības nolīgums ir stājies spēkā un ir notikusi klasificētas informācijas apmaiņa ar attiecīgo trešo valsti vai starptautisko organizāciju, Drošības komiteja var pieņemt lēmumu grozīt maksimālo tādas ESKI līmeni, ar ko var apmainīties izdrukātā vai elektroniskā veidā, jo īpaši – ņemot vērā turpmākus izvērtējuma apmeklējumus.

IV. ADMINISTRATĪVI PASĀKUMI

17. Ja pastāv ilgtermiņa vajadzība organizēt tādas klasificētas informācijas apmaiņu ar trešo valsti vai starptautisku organizāciju, kura parasti nav klasificēta augstāk kā *RESTREINT UE/EU RESTRICTED*, un ja Drošības komiteja konstatējusi, ka attiecīgajai pusei nav pietiekami attīstītas drošības sistēmas, lai tā varētu noslēgt informācijas drošības nolīgumu, ģenerālsekretārs ar Padomes piekrišanu var noslēgt administratīvu vienošanos PĢS vārdā ar attiecīgām trešās valsts iestādēm vai starptautisko organizāciju.

18. Taču, ja steidzamu operatīvu iemeslu dēļ klasificētas informācijas apmaiņas sistēma ir jāizveido ātri, izņēmuma kārtā Padome var nolemt noslēgt administratīvu vienošanos par augstāka klasifikācijas līmeņa informācijas apmaiņu.

19. Administratīvās vienošanās parasti noslēdz vēstuļu apmaiņas veidā.

20. Pirms ESKI faktiskās nodošanas attiecīgajai trešai valstij vai starptautiskai organizācijai veic 9. punktā minēto izvērtējuma apmeklējumu un ziņojumu par to vai, ja šāda ziņojuma nav, 12. punktā minēto ziņojumu nosūta Drošības komitejai, kura to atzīst par apmierinošu.

21. ESKI apmaiņu saskaņā ar administratīvu vienošanos neveic elektroniskā veidā, izņemot gadījumus, kad tas īpaši noteikts ar minēto vienošanos.

V. KLASIFICĒTAS INFORMĀCIJAS APMAIŅA SAISTĪBĀ AR KDAP OPERĀCIJĀM

22. Ar līdzdalības pamatnolīgumiem reglamentē trešo valstu vai starptautisku organizāciju dalību KDAP operācijās. Šādos nolīgumos iekļauj noteikumus par tādas ESKI nodošanu operācijas dalībniecēm trešām valstīm vai starptautiskām organizācijām, kura sagatavota KDAP operāciju vajadzībām. Maksimālais klasifikācijas līmenis ESKI, ar kuru var apmainīties, ir *RESTREINT UE/EU RESTRICTED* civilo KDAP operāciju vajadzībām un *CONFIDENTIEL UE/EU CONFIDENTIAL* militāro KDAP operāciju vajadzībām, ja vien lēmumā, ar ko izveido katru KDAP operāciju, nav noteikts citādi.

23. *Ad hoc* līdzdalības nolīgumos, kas noslēgti attiecībā uz konkrētu KDAP operāciju, iekļauj noteikumus par tādas ESKI nodošanu operācijas dalībniecēm trešām valstīm vai starptautiskām organizācijām, kura sagatavota attiecīgās operācijas vajadzībām. Maksimālais klasifikācijas līmenis ESKI, ar kuru var apmainīties, ir *RESTREINT UE/EU RESTRICTED* civilo KDAP operāciju vajadzībām un *CONFIDENTIEL UE/EU CONFIDENTIAL* militāro KDAP operāciju vajadzībām, ja vien lēmumā, ar ko izveido katru KDAP operāciju, nav noteikts citādi.

▼B

24. Ja nav noslēgts informācijas drošības nolīgums un kamēr nav noslēgts dalības nolīgums, tādas ESKI, kas radīta operācijas nolūkiem, nodošanu trešai valstij vai starptautiskai organizācijai, kas piedalās operācijā, reglamentē ar administratīvu vienošanos, kas jānoslēdz Augstajam pārstāvim, vai uz to attiecas lēmums par *ad hoc* nodošanu saskaņā ar VI iedaļu. ESKI saskaņā ar šādu vienošanos var nodot tikai tik ilgi, kamēr tiek paredzēta trešās valsts vai starptautiskās organizācijas dalība. Maksimālais klasifikācijas līmenis ESKI, ar kuru var apmainīties, ir *RESTREINT UE/EU RESTRICTED* civilo KDAP operāciju vajadzībām un *CONFIDENTIEL UE/EU CONFIDENTIAL* militāro KDAP operāciju vajadzībām, ja vien lēmumā, ar ko izveido katru KDAP operāciju, nav noteikts citādi.

25. Noteikumos par klasificētas informācijas ietveršanu līdzdalības pamatnolīgumos, *ad hoc* līdzdalības nolīgumos un *ad hoc* administratīvajās vienošanās, kas minētas 22. līdz 24. punktā, paredz, ka attiecīgā trešā valsts vai starptautiskā organizācija nodrošina, ka tās personāls, kas norīkots operācijas veikšanai, aizsargās ESKI saskaņā ar Padomes drošības noteikumiem un ar turpmākām kompetento iestāžu, tostarp operācijas komandķēdes, norādēm.

26. Ja attiecīgā iesaistītā trešā valsts vai starptautiskā organizācija pēc tam noslēdz informācijas drošības nolīgumu ar Savienību, šis informācijas drošības nolīgums, ciktāl tas attiecas uz apmaiņu un rīkošanos ar ESKI, aizstāj noteikumus par klasificētas informācijas apmaiņu, kas izklāstīti jebkurā līdzdalības pamatnolīgumā, *ad hoc* līdzdalības nolīgumā vai *ad hoc* administratīvajā vienošanās.

27. Saskaņā ar trešo valsti vai starptautisko organizāciju noslēgto līdzdalības pamatnolīgumu, *ad hoc* līdzdalības nolīgumu vai *ad hoc* administratīvo vienošanos nav atļauts veikt ESKI elektronisku apmaiņu, ja vien tas nav skaidri noteikts attiecīgā nolīguma vai vienošanās tekstā.

28. ESKI, kas izstrādāta KDAP operācijas vajadzībām, var atklāt personālam, ko trešās valstis vai starptautiskas organizācijas ir norīkojušas darbam minētajā operācijā, saskaņā ar 22. līdz 27. punktu. Sniedzot tādam personālam atļauju piekļūt ESKI KDAP operācijas telpās vai komunikāciju un informācijas sistēmā, ir jāpiemēro pasākumi (tostarp atklātās ESKI reģistrācija), lai mazinātu zuduma vai riska iespēju. Tādus pasākumus definē attiecīgos plānošanas vai misijas dokumentos.

29. Ja nav noslēgts informācijas drošības nolīgums, ESKI nodošanu specifiskas un tūlītējas operatīvas vajadzības gadījumā uzņēmējvalstij, kuras teritorijā veic KDAP operāciju, var reglamentēt ar administratīvu vienošanos, kas jānoslēdz Augstajam pārstāvim. Šo iespēju paredz lēmumā, ar ko izveido KDAP operāciju. Šādos apstākļos nodod tikai tādu ESKI, kura sagatavota KDAP operācijas vajadzībām un kuras klasifikācija nav augstāka kā *RESTREINT UE/EU RESTRICTED*, izņemot gadījumus, kad lēmumā, ar ko izveido KDAP operāciju, ir noteikts augstāks klasifikācijas līmenis. Saskaņā ar tādas administratīvās vienošanās tekstu uzņēmējvalsts pienākums ir apņemties aizsargāt ESKI atbilstīgi minimālajiem standartiem, kas nav vājāki par šajā lēmumā noteiktajiem.

▼B

30. Ja nav noslēgts informācijas drošības nolīgums, ESKI nodošanu attiecīgajām trešām valstīm un starptautiskajām organizācijām, kas nav tās, kuras piedalās KDAP operācijā, var reglamentēt ar administratīvu vienošanos, kas jānoslēdz Augstajam pārstāvim. Attiecīgā gadījumā šo iespēju, kā arī jebkurus citus ar to saistītos noteikumus paredz lēmumā, ar ko izveido KDAP operāciju. Šādos apstākļos nodod tikai tādu ESKI, kura sagatavota KDAP operācijas vajadzībām un kuras klasifikācija nav augstāka kā *RESTREINT UE/EU RESTRICTED*, izņemot gadījumus, kad lēmumā, ar ko izveido KDAP operāciju, ir noteikts augstāks klasifikācijas līmenis. Saskaņā ar tādas administratīvas vienošanās tekstu attiecīgās trešās valsts vai starptautiskās organizācijas pienākums ir apņemties aizsargāt ESKI atbilstīgi minimālajiem standartiem, kas nav vājāki par šajā lēmumā noteiktajiem.

31. Nav vajadzīgi īstenošanas pasākumi vai izvērtējuma apmeklējumi, pirms nav īstenoti noteikumi par ESKI nodošanu saistībā ar 22., 23. un 24. punktu.

VI. ESKI ĀRKĀRTĒJA *AD HOC* NODOŠANA

32. Ja nav nekādas sistēmas atbilstīgi III līdz V iedaļai un ja Padomei vai vienai no tās sagatavošanas struktūrām rodas ārkārtēja vajadzība nodot ESKI trešai valstij vai starptautiskai organizācijai, PĢS:

a) cik vien iespējams konsultējas ar attiecīgās trešās valsts vai starptautiskās organizācijas drošības iestādēm par to, vai tās drošības noteikumi, struktūras un procedūras garantē, ka ESKI, kas tai tiktu nodota, būtu aizsargāta pēc standartiem, kas nav mazāk stingri par šajā lēmumā norādītajiem standartiem; un

b) lūdz Drošības komiteju, pamatojoties uz pieejamo informāciju, izsniegt ieteikumu par uzticēšanos drošības regulām, struktūrām un procedūrām tajā trešā valstī vai starptautiskajā organizācijā, kurām ESKI nodos.

33. Ja Drošības komiteja pieņem ieteikumu par labu ESKI nodošanai, attiecīgo lietu nosūta Pastāvīgo pārstāvju komitejai (*Coreper*), kura pieņem lēmumu par informācijas nodošanu.

34. Ja Drošības komitejas ieteikumā nav atbalstīta ESKI nodošana:

a) ar KĀDP/KDAP saistītos jautājumos Politikas un drošības komiteja attiecīgo jautājumu pārrunā un formulē ieteikumu *Coreper* lēmumam;

b) visos pārējos jautājumos *Coreper* attiecīgo jautājumu pārrunā un pieņem lēmumu.

35. Ja to uzskata par piemērotu un ja attiecīgā gadījumā ir rakstiski piekritis autors, *Coreper* var pieņemt lēmumu, ka klasificētu informāciju var nodot tikai daļēji vai tikai tad, ja tās klasifikācijas līmenis ir pamazināts vai tā ir deklasificēta vai ja nododamo informāciju gatavo, nenorādot avotu vai sākotnējo ES klasifikācijas līmeni.

36. PĢS saskaņā ar lēmumu nodot ESKI nosūta attiecīgo dokumentu ar norādi par trešo valsti vai starptautisko organizāciju, kurai tā ir nodota. Pirms vai pēc faktiskās nodošanas attiecīgā trešā persona rakstiski apņemas aizsargāt saņemto ESKI saskaņā ar šajā lēmumā izklāstītajiem pamatprincipiem un minimālajiem standartiem.

▼B

VII. IESTĀDE, KAS NODOD ESKI TREŠĀM VALSTĪM VAI STARPTAUTISKĀM ORGANIZĀCIJĀM

37. Ja saskaņā ar 2. punktu pastāv sistēma klasificētas informācijas apmaiņai ar kādu trešo valsti vai starptautisku organizāciju, Padome pieņem lēmumu atļaut ģenerālsekretāram saskaņā ar principu par informācijas autora piekrišanu nodot ESKI attiecīgai trešai valstij vai starptautiskai organizācijai. Ģenerālsekretārs var deleģēt šādas atļaujas piešķiršanu PĢS vecākajiem ierēdņiem.

38. Ja saskaņā ar 2. punkta pirmo ievilkumu ir noslēgts informācijas drošības nolīgums, Padome var pieņemt lēmumu atļaut Augstajam pārstāvim attiecīgajai trešai valstij vai starptautiskajai organizācijai nodot no Padomes nākošu ESKI kopējās ārpolitikas un drošības politikas jomā pēc tam, kad ir iegūta jebkura tajā iekļautā materiāla autora piekrišana. Augstais pārstāvis var deleģēt šādas atļaujas piešķiršanu vecākajiem EĀDD ierēdņiem vai ESĪP.

39. Ja saskaņā ar 2. punktu vai 3. punktu pastāv sistēma klasificētas informācijas apmaiņai ar kādu trešo valsti vai starptautisku organizāciju, Augstajam pārstāvim ir atļauts nodot ESKI saskaņā ar lēmumu, ar ko izveido KDAP operāciju, un ar principu par informācijas autora piekrišanu. Augstais pārstāvis var deleģēt šādas atļaujas piešķiršanu vecākajiem EĀDD ierēdņiem, ES operācijas, spēku vai misijas komandieriem vai ES misijas vadītājiem.

▼B

Papildinājumi

A papildinājums

Definīcijas

B papildinājums

Drošības klasifikāciju atbilstība

C papildinājums

Valsts drošības iestāžu (VDI) saraksts

D papildinājums

Akronīmu saraksts

▼B

A papildinājums

DEFINĪCIJAS

Šajā lēmumā piemēro šādas definīcijas:

“akreditācija” ir process, kura rezultāts ir drošības akreditācijas iestādes (DAI) oficiāla deklarācija, ka sistēma ir apstiprināta konkrētas klasifikācijas līmeņa darbam īpašā drošības režīmā savā darbības vidē un pieņemamā riska līmenī, balstoties uz pieņēmumu, ka ir īstenots apstiprināts tehnisku, fizisku, organizatorisku un procedūras drošības pasākumu kopums;

“resursi” ir jebkas, ko organizācija uzskata par vērtīgu savās saimnieciskajās darbībās un to nepārtrauktības nodrošināšanā, tostarp informācijas resursi, kas vajadzīgi organizācijas uzdevuma pildīšanai;

“atļauja piekļūt ESKI” ir PĢS iecēlējinstitūcijas lēmums, kas pieņemts, pamatojoties uz dalībvalsts kompetentās iestādes apliecinājumu, ka ĢPS ierēdnim, citam darbiniekam vai norīkotam valsts ekspertam – ar noteikumu, ka ir apzināta viņa vajadzība pēc informācijas un viņš ir attiecīgi informēts par saviem pienākumiem, – var līdz konkrētam datumam piešķirt piekļuvi ESKI līdz konkrētam līmenim (*CONFIDENTIEL UE/EU CONFIDENTIAL* vai augstākam);

“KIS aprites cikls” ir viss KIS pastāvēšanas laiks kopā, kurā ietilpst ierosināšana, koncepcijas izstrāde, plānošana, prasību analīze, projektēšana, izstrāde, testēšana, īstenošana, darbība, uzturēšana un likvidēšana;

“klasificēts līgums” ir līgums, kuru PĢS slēdz ar līgumslēdzēju par ražojumu piegādi, darbu veikšanu vai pakalpojumu sniegšanu un kura izpilde prasa vai ir saistīta ar piekļuvi ESKI vai tās sagatavošanu;

“klasificēts apakšlīgums” ir līgums par ražojumu piegādi, darbu veikšanu vai pakalpojumu sniegšanu, kuru PĢS līgumslēdzējs slēdz ar citu līgumslēdzēju (t. i., apakšlīgumslēdzēju) un kura izpilde prasa vai ir saistīta ar piekļuvi ESKI vai tās sagatavošanu;

“komunikāciju un informācijas sistēma” (KIS) – skatīt 10. panta 2. punktu;

“līgumslēdzējs” ir fiziska vai juridiska persona, kura ir tiesīga slēgt līgumus;

“kriptogrāfijas materiāls” ir kriptogrāfijas algoritmi, kriptogrāfijas aparatūras un programmatūras moduļi un produkti, tostarp īstenošanas informācija un ar to saistītā dokumentācija un atslēgu materiāls;

“kriptogrāfijas produkts” ir produkts, kura primārā un galvenā funkcija ir nodrošināt drošības pakalpojumus (konfidencialitāti, integritāti, pieejamību, autentiskumu, pretnoliegšanu), izmantojot vienu vai vairākus kriptogrāfijas mehānismus;

▼B

“KDAP operācija” ir krīžu militāras vai civilas pārvarēšanas operācija saskaņā ar LES V sadaļas 2. nodaļu;

“deklasifikācija” ir jebkādas drošības klasifikācijas noņemšana;

“padziļināta aizsardzība” ir dažādu drošības pasākumu piemērošana, izveidojot daudzslāņainu aizsardzību;

“izraudzītā drošības iestāde” (IDI) ir iestāde, kas pakļauta dalībvalsts valsts drošības iestādei (VDI) un ir atbildīga par to, ka rūpniecības vai citas vienības 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;

“dokuments” ir jebkura ierakstīta informācija neatkarīgi no tās fiziskā veidola vai iezīmēm;

“klasifikācijas līmeņa pazemināšana” ir klasificēšana zemākā drošības pakāpē;

“ES klasificēta informācija” (ESKI) – skatīt 2. panta 1. punktu;

“iestādes drošības pielaide” (IDP) ir IDI vai VDI administratīvs konstatējums, ka no drošības viedokļa iestāde spēj nodrošināt pietiekamu ESKI aizsardzību konkrētā drošības klasifikācijas līmenī;

“rīkošanās” ar ESKI ir visu veidu darbības, ko ar ESKI veic tās aprites laikā. Tajā ietilpst izstrāde, apstrāde, pārvietošana, klasifikācijas līmeņa pazemināšana, deklasifikācija un iznīcināšana. Saistībā ar KIS tajā ietilpst arī ievākšana, uzrādīšana, pārsūtīšana un glabāšana;

“turētājs” ir pienācīgi sertificēta persona, kurai ir oficiāli pierādīta vajadzība pēc informācijas un kuras rīcībā ir ESKI, kas tādējādi dara viņu atbildīgu par aizsardzību;

“rūpniecības vai cita vienība” ir vienība, kas piegādā ražojumus, veic darbu vai sniedz pakalpojumus; tās var būt rūpniecības, komerciālas, pakalpojumu sniedzēju, zinātniskas, pētniecības, izglītības vai attīstības vienības vai pašnodarbināta persona;

“industriālā drošība” – skatīt 11. panta 1. punktu;

“informācijas aizsardzība” – skatīt 10. panta 1. punktu;

“savstarpējs savienojums” – skatīt IV pielikuma 32. punktu;

“klasificētas informācijas pārvaldība” – skatīt 9. panta 1. punktu;

▼B

“materiāli” ir jebkurš dokuments, datu nesējs vai iekārtas vai ierīces daļa, kas jau ir izstrādāta vai vēl tiek izstrādāta;

“autors” ir Savienības iestāde, struktūra vai aģentūra, dalībvalsts, trešā valsts vai starptautiska organizācija, kuras pakļautībā klasificēta informācija ir sagatavota un/vai nodota Savienības struktūrām;

“personāla drošība” – skatīt 7. panta 1. punktu;

“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 līdz konkrētam datumam var piešķirt piekļuvi ESKI līdz konkrētam līmenim (*CONFIDENTIEL UE/EU CONFIDENTIAL* vai augstāk);

“personāla drošības pielaides apliecība” (PDPA) ir kompetentās drošības iestādes izdota apliecība, ar kuru nosaka, ka persona ir saņēmusi drošības pielaidi un tai ir derīga drošības pielaides apliecība vai iecēlējinstitūcijas atļauja piekļūt ESKI, kurā norāda to ESKI klasifikācijas līmeni, līdz kuram personai var piešķirt piekļuvi (*CONFIDENTIEL UE/EU CONFIDENTIAL* vai augstāk), attiecīgās PDP derīguma termiņu un apliecības derīguma termiņu;

“fiziskā drošība” – skatīt 8. panta 1. punktu;

“programmas/projekta drošības instrukcijas” (PDI) ir to drošības procedūru saraksts, kuras piemēro konkrētai programmai/projektam, lai standartizētu drošības procedūras. To var pārskatīt visā programmas/projekta darbības laikā;

“reģistrācija” – skatīt III pielikuma 18. punktu;

“atlikušais risks” ir risks, kas pastāv pēc drošības pasākumu īstenošanas, ņemot vērā to, ka ne pret visiem apdraudējumiem var cīnīties un ne visu ietekmējamību var likvidēt;

“risks” ir iespēja, ka ar kādu apdraudējumu izmantos iekšēju vai ārēju organizācijas vai kādas tās sistēmas vājo vietu un tādējādi radīs kaitējumu organizācijai un tās materiāliem un nemateriāliem aktīviem. To izsaka kā apdraudējumu iespējamības un to ietekmes apvienojumu:

— “riska pieņemšana” ir lēmums pēc riska risinājuma vienoties par atlikušā riska turpmāko pastāvēšanu,

— “riska izvērtējums” ir apdraudējumu un ietekmējamības noteikšana un saistītu risku analīzes veikšana, t. i., varbūtību un ietekmes analīze,

— “ziņojums par risku” ir KIS lietotāju kopienu informētības veidošana, informējot apstiprināšanas iestādes par tādiem riskiem un ziņojot par tiem rīcības iestādēm,

▼B

— “riska risinājums” ir riska ietekmes pavājināšana, tā likvidēšana vai mazināšana (izmantojot atbilstīgu tehnisku, fizisku, pārvaldes vai procedūras pasākumu apvienojumu), riska pārvietošana vai pārraudzība;

“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 sagatavošanu un kurā identificē drošības prasības vai tos līguma elementus, kam vajadzīga drošības aizsardzība;

“drošības klasifikācijas rokasgrāmata” (DKR) ir dokuments, kurā aprakstīti klasificētie programmas vai līguma elementi, precizējot piemērojamos drošības klasifikācijas līmeņus. DKR var paplašināt visā programmas vai līguma darbības laikā un informācijas elementus var pārklasificēt vai klasificēt zemākā kategorijā; ja pastāv DKR, tā ietilpst DAV;

“drošības izmeklēšana” ir izmeklēšanas procedūras, ko saskaņā ar spēkā esošiem valsts normatīvajiem aktiem veic kompetentā dalībvalsts iestāde, lai pārliecinātos, ka nav nekādas nelabvēlīgas informācijas, kas varētu liegt konkrētai personai saņemt PDP vai atļauju piekļūt ESKI, lai tā varētu piekļūt ESKI līdz konkrētam līmenim (*CONFIDENTIEL UE/EU CONFIDENTIAL* vai augstāk);

“drošības darbības režīms” ir to nosacījumu definēšana, saskaņā ar kuriem darbojas KIS, pamatojoties uz informācijas, ar kuru rīkojas KIS, klasifikāciju un pielaides līmeņiem, oficiāliem piekļuves apstiprinājumiem un tās lietotāju vajadzību pēc informācijas. Rīkošanās procesam ar klasificētu informāciju un tās pārsūtīšanai ir četri darbības režīmi – paredzētais, sistēmiskais, nodalītais un daudzlīmeņu režīms:

— “paredzētais režīms” ir darbības režīms, kurā visām personām, kam ir piekļuve KIS, ir atļauja piekļūt augstākās klasifikācijas informācijai, ar kuru rīkojas KIS, kā arī kopīga nepieciešamība zināt visu informāciju, ar kuru rīkojas KIS,

— “sistēmiskais režīms” ir darbības režīms, kurā visām personām, kam ir piekļuve KIS, ir atļauja piekļūt augstākās klasifikācijas informācijai, ar kuru rīkojas KIS, bet ne visām personām, kam ir piekļuve KIS, ir kopīga nepieciešamība pēc informācijas, ar kuru rīkojas KIS; apstiprinājumu par piekļuvi informācijai var piešķirt atsevišķa persona,

— “nodalītais režīms” ir darbības režīms, kurā visām personām, kam ir piekļuve KIS, ir atļauja piekļūt augstākās klasifikācijas informācijai, ar kuru rīkojas KIS, bet ne visām personām, kam ir piekļuve KIS, ir oficiāla atļauja piekļūt visai informācijai, ar kuru rīkojas KIS; atšķirībā no piekļuves, ko var piešķirt atsevišķa persona, tam, lai piešķirtu oficiālu atļauju, ir vajadzīga oficiāla centrāla piekļuves kontroles pārvaldība,

▼B

— “daudzlīmeņu režīms” ir darbības režīms, kurā ne visām personām, kam ir piekļuve KIS, ir atļauja piekļūt augstākās klasifikācijas informācijai, ar kuru rīkojas KIS, un ne visām personām, kam ir piekļuve KIS, ir kopīga nepieciešamība pēc informācijas, ar kuru rīkojas KIS;

“drošības riska pārvaldības process” ir viss process, kurā ietilpst tādu neparedzētu notikumu apzināšana, kontrole un ietekmes samazināšana, kuri var ietekmēt drošību organizācijā vai jebkurā no sistēmām, ko tā izmanto. Tas attiecas uz visām darbībām, kas saistītas ar risku, tostarp tā izvērtēšanu, apstrādi, pieņemšanu un izziņošanu;

“*TEMPEST*” ir apdraudošu elektromagnētisku emisiju izmeklēšana, izpēte un kontrole un pasākumi to novēršanai;

“apdraudējums” ir iespējams nevēlama atgadījuma cēlonis, kura rezultātā var tikt izdarīts kaitējums organizācijai vai jebkurai sistēmai, ko tajā izmanto; tādi apdraudējumi var būt nejauši vai apzināti (ļaunprātīgi), un tiem ir raksturīgi apdraudējuma elementi, iespējami mērķi un uzbrukuma metodes;

“ietekmējamība” ir jebkura vājā vieta, ko varētu izmantot vienā vai vairākos apdraudējuma gadījumos. Ietekmējamība var būt kāda posma iztrūkums vai var būt saistīta ar vāju vietu kontrolē attiecībā uz tās stiprumu, pilnīgumu vai konsekvenci, un tai var būt tehnisks, procedūras, fizisks, organizatorisks vai operatīvs raksturs.

▼**M1**

B papildinājums

DROŠĪBAS KLASIFIKĀCIJU ATBILSTĪBA

ES | TRÈS SECRET UE/EU TOP SECRET | SECRET UE/EU SECRET | CONFIDENTIEL UE/EU CONFIDENTIAL | RESTREINT UE/EU 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 piezīme [1] |

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 piezīme [3] |

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* |

([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 sis*tēmā nelieto klasifikāciju* RESTREINT. Francija ar ESTREINT UE/EU RESTRICTED informāciju rīkojas un aizsargā to tikpat stingri, kā noteikts Eiropas Savienības Padomes drošības noteikumu standartos un procedūrās.

▼**M1**

Luksemburga | *Très Secret Lux* | *Secret Lux* | *Confidentiel Lux* | *Restreint Lux* |

Ungārija | *Szigorúan titkos!* | *Titkos!* | *Bizalmas!* | *Korlátozott terjesztésű!* |

Malta | *L-Ogħla Segretezza* | *Sigriet* | *Kunfidenzjali* | *Ristrett* |

Top Secret | *Secret* | *Confidential* | *Restricted* ([1])

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* |

Rumānija | *Strict secret de importanţă 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 ([2]) | 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 | zemsvītras piezīme ([3]) | UK OFFICIAL-SENSITIVE

([1]) Malta var pārmaiņus izmantot marķējumu gan maltiešu, gan angļu valodā.

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

([3]) Apvienotā Karaliste savā valsts sistēmā vairs neizmanto klasifikāciju UK CONFIDENTIAL. Apvienotā Karaliste ar CONFIDENTIEL UE/EU CONFIDENTIAL informāciju rīkojas un aizsargā to atbilstīgi UK SECRET aizsardzības drošības prasībām.

▼B

C papildinājums

VALSTS DROŠĪBAS IESTĀŽU (VDI) SARAKSTS

BEĻĢIJA
Autorité nationale de Sécurité
SPF Affaires étrangères, Commerce extérieur et Coopération au Développement
15, rue des Petits Carmes
1000 Bruxelles

Sekretariāta tālr.: +32 25014542
Fakss: +32 25014596
E-pasts: nvo-ans@diplobel.fed.be

BULGĀRIJA
State Commission on Information Security
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
(National Security Authority)
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
(Danish Security Intelligence Service)
Klausdalsbrovej 1
2860 Søborg

Tālr.: +45 33148888
Fakss: +45 33430190

Forsvarets Efterretningstjeneste
(Danish Defence Intelligence Service)
Kastellet 30
2100 Copenhagen Ø

Tālr.: +45 33325566
Fakss: +45 33931320

IGAUNIJA
National Security Authority Department
Estonian Ministry of Defence
Sakala 1
15094 Tallinn

Tālr.: +372 7170019, +372 7170117
Fakss: +372 7170213
E-pasts: nsa@mod.gov.ee

ĪRIJA
National Security Authority
Department of Foreign Affairs
76–78 Harcourt Street
Dublin 2

Tālr.: +353 14780822
Fakss: +353 14082959

GRIEĶIJA
Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Διεύθυνση Ασφαλείας και Αντιπληροφοριών
ΣΤΓ 1020 -Χολαργός (Αθήνα)
Ελλάδα

Τηλέφωνα:+30 2106572045 (ώρες γραφείου)
+30 2106572009 (ώρες γραφείου)
Τηλεομοιότυπο: +30 2106536279
+30 2106577612

Hellenic National Defence General Staff
(HNDGS)
Counter Intelligence and Security Directorate
(NSA)
227–231 HOLARGOS
STG 1020 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

▼B

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	**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 Croatian NSA Jurjevska 34 10000 Zagreb Croatia Tālr.: +385 14681222 Fakss: +385 14686049 Tīmekļa vietne: www.uvns.hr	**LUKSEMBURGA** Autorité nationale de Sécurité Boîte postale 2379 1023 Luxembourg Tālr.: +352 24782210 central +352 24782253 direct Fakss: +352 24782243
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	**UNGĀRIJA** Nemzeti Biztonsági Felügyelet (National Security Authority of Hungary) 1024 Budapest, Szilágyi Erzsébet fasor 11/B Tālr.: +36 17952303 Fakss: +36 17950344 Pasta adrese: 1357 Budapest, PO Box 2 E-pasts: nbf@nbf.hu Tīmekļa vietne: www.nbf.hu
KIPRA ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ Εθνική Αρχή Ασφάλειας (ΕΑΑ) Υπουργείο Άμυνας Λεωφόρος Εμμανουήλ Ροΐδη 4 1432 Λευκωσία, Κύπρος Τηλέφωνα: +357 22807569, +357 22807643, +357 22807764 Τηλεομοιότυπο: +357 22302351 Ministry of Defence Minister's Military Staff National Security Authority (NSA) 4 Emanuel Roidi street 1432 Nicosia Tālr.: +357 22807569, +357 22807643, +357 22807764 Fakss: +357 22302351 E-pasts: cynsa@mod.gov.cy	**MALTA** Ministry for Home Affairs and National Security P.O. Box 146 MT-Valletta Tālr.: +356 21249844 Fakss: +356 25695321
LATVIJA National Security Authority Constitution Protection Bureau of the Republic of Latvia P.O. Box 286 Riga, LV-1001 Tālr.: +371 67025418 Fakss: +371 67025454 E-pasts: ndi@sab.gov.lv	**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

▼B

LIETUVA Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija (The Commission for Secrets Protection Coordination of the Republic of Lithuania National Security Authority) Gedimino 40/1 LT-01110 Vilnius Tālr.: +370 70666701, +370 70666702 Fakss: +370 70666700 E-pasts: nsa@vsd.lt	**AUSTRIJA** Informationssicherheitskommission Bundeskanzleramt Ballhausplatz 2 1014 Wien Tālr.: +43 1531152594 Fakss: +43 1531152615 E-pasts: ISK@bka.gv.at
POLIJA Agencja Bezpieczeństwa Wewnętrznego – ABW (Internal Security Agency) 2A Rakowiecka St. 00-993 Warszawa Tālr.: +48 225857360 Fakss: +48 225858509 E-pasts: nsa@abw.gov.pl Tīmekļa vietne: www.abw.gov.pl	**SLOVĀKIJA** Národný bezpečnostný úrad (National Security Authority) Budatínska 30 P.O. Box 16 850 07 Bratislava Tālr.: +421 268692314 Fakss: +421 263824005 Tīmekļa vietne: www.nbusr.sk
PORTUGĀLE Presidência do Conselho de Ministros Autoridade Nacional de Segurança Rua da Junqueira, 69 1300-342 Lisboa Tālr.: +351 213031710 Fakss: +351 213031711	**SOMIJA** National Security Authority Ministry for Foreign Affairs P.O. Box 453 FI-00023 Government Tālr.: +358 16055890 Fakss: +358 916055140 E-pasts: NSA@formin.fi
RUMĀNIJA Oficiul Registrului Național al Informațiilor Secrete de Stat (Romanian NSA – ORNISS National Registry Office for Classified Information) Str. Mureş nr. 4, sector 1 012275 Bucureşti Tālr.: +40 212245830 Fakss: +40 212240714 E-pasts: nsa.romania@nsa.ro Tīmekļa vietne: www.orniss.ro	**ZVIEDRIJA** Utrikesdepartementet (Ministry for Foreign Affairs) UD-RS SE-103 39 Stockholm Tālr.: +46 84051000 Fakss: +46 87231176 E-pasts: ud-nsa@foreign.ministry.se
SLOVĒNIJA Urad Vlade RS za varovanje tajnih podatkov Gregorčičeva 27 1000 Ljubljana Tālr.: +386 14781390 Fakss: +386 14781399 E-pasts: gp.uvtp@gov.si	**APVIENOTĀ KARALISTE** UK National Security Authority Room 335, 3rd Floor 70 Whitehall London SW1A 2AS 1. tālr.: +44 2072765645 2. tālr.: +44 2072765497 Fakss: +44 2072765651 E-pasts: UK-NSA@cabinet-office.x.gsi.gov.uk

▼B

D papildinājums

AKRONĪMU SARAKSTS

Akronīms	Nozīme
AQUA	atbilstīgi kvalificēta iestāde
BPS	robežu aizsardzības dienesti
CCTV	videonovērošanas sistēma
Coreper	Pastāvīgo pārstāvju komiteja
DAI	drošības akreditācijas iestāde
DAV	drošības aspektu vēstule
DKR	drošības klasifikācijas rokasgrāmata
EKDD	Eiropas Komisijas Drošības direktorāts
ESĪP	ES īpašais pārstāvis
ESKI	ES klasificēta informācija
IA	informācijas aizsardzība
IAI	informācijas aizsardzības iestāde
IDI	izraudzītā drošības iestāde
IDP	iestādes drošības pielaide
IKS	ielaušanās konstatācijas sistēma
IT	informācijas tehnoloģija
KĀDP	kopējā ārpolitika un drošības politika
KAI	kriptogrāfijas apstiprinājuma iestāde
KDAP	kopējā drošības un aizsardzības politika
KII	kriptogrāfijas izplatīšanas iestāde
KIS	komunikāciju un informācijas sistēmas, kurās rīkojas ar ESKI
PDI	programmas/projekta drošības instrukcijas
PDP	personāla drošības pielaide
PDPA	personāla drošības pielaides apliecība
PĢS	Padomes Ģenerālsekretariāts
SAB	Drošības akreditācijas valde
SecOPs	drošības darba procedūras
SSRS	katras sistēmas drošības prasību izklāsts
TI	*TEMPEST* iestāde
VDI	valsts drošības iestāde