Šis dokuments ir izveidots vienīgi dokumentācijas nolūkos, un iestādes neuzņemas nekādu atbildību par tā saturu

►**B**

PADOMES LĒMUMS

(2001. gada 19. maijs),

ar ko pieņem Padomes drošības reglamentu

(2001/264/EK)

(OV L 11, 11.4.2001, lpp. 1)

Grozīts ar:

		Oficiālais Vēstnesis		
		Nr.	Lappuse	Datums
►**M1**	Padomes Lēmums 2004/194/EK (2004. gada 10. februāris)	L 63	48	28.2.2004
►**M2**	Padomes Lēmums 2005/571/EK (2005. gada 12. jūlijs)	L 193	31	23.7.2005
►**M3**	Padomes Lēmums 2005/952/EK (2005. gada 20. decembris)	L 346	18	29.12.2005

▼B

PADOMES LĒMUMS

(2001. gada 19. maijs),

ar ko pieņem Padomes drošības reglamentu

(2001/264/EK)

EIROPAS SAVIENĪBAS PADOME,

ņemot vērā Eiropas Kopienas dibināšanas līgumu, un jo īpaši tā 207. panta 3. punktu,

ņemot vērā Padomes Lēmumu 2000/396/EK, EOTK, *Euratom* (2000. gada 5. jūnijs), ar ko pieņem Padomes reglamentu ([1]), un jo īpaši tā 24. pantu,

tā kā:

(1) Lai attīstītu Padomes darbības jomās, kurās nepieciešama konfidencialitāte, ir lietderīgi izveidot visaptverošu drošības sistēmu, kas attiektos uz Padomi, tās Ģenerālsekretariātu un dalībvalstīm.

(2) Šāda sistēma ir jāapvieno vienā dokumentā, kura priekšmets aptvertu visus iepriekšējos lēmumus un noteikumus tajā pašā jomā.

(3) Praksē lielākā daļa ES informācijas, kas klasificēta kā ES konfidenciālā (*CONFIDENTIEL UE*) informācija, attiecas uz Kopējo drošības un aizsardzības politiku.

(4) Lai nodrošinātu šādi izveidotās drošības sistēmas efektivitāti, dalībvalstis jāiesaista tās darbībā, veicot valstu pasākumus, kas nepieciešami šā lēmuma noteikumu ievērošanai, ja to kompetentās iestādes un darbinieki rīkojas ar ES klasificēto informāciju.

(5) Padome atbalsta Komisijas nodomu līdz šā lēmuma piemērošanas dienai ieviest visaptverošu sistēmu, kas atbilst tā pielikumiem, lai nodrošinātu vienmērīgu Savienības lēmumu pieņemšanas procesu darbību.

(6) Padome uzsver, ka ir svarīgi attiecīgā gadījumā sasaistīt Eiropas Parlamentu un Komisiju ar konfidencialitātes noteikumiem un standartiem, kuri ir nepieciešami, lai aizstāvētu Savienības un tās dalībvalstu intereses.

(7) Šis lēmums ir pieņemts, neierobežojot Līguma 255. pantu un tā īstenošanas dokumentus.

(8) Šis lēmums ir pieņemts, neierobežojot dalībvalstīs pastāvošo praksi attiecībā uz attiecīgo valstu parlamentu informēšanu par Savienības darbībām,

IR PIEŅĒMUSI ŠO LĒMUMU.

1. pants

Ar šo apstiprina pielikumā ietverto Padomes drošības reglamentu.

2. pants

1. Ģenerālsekretārs/Augstais pārstāvis veic nepieciešamos pasākumus, lai nodrošinātu to, ka, rīkojoties ar ES klasificēto informāciju, Padomes Ģenerālsekretariāta ierēdņi un citi darbinieki, Padomes Ģenerālsekretariāta līgumdarbinieki un darbam Padomes Ģenerālsekretariātā norīkots personāls Padomes Ģenerālsekretariātā, kā arī Padomes telpās un ES decentralizētajās aģentūrās ([2]) ievēro 1. pantā minēto reglamentu.

([1]) OV L 149, 23.6.2000., 21. lpp.
([2]) Sk. Padomes 2000. gada 10. novembra Slēdzienu.

▼B

2. Dalībvalstis saskaņā ar valstu noteikumiem veic attiecīgus pasākumus, lai nodrošinātu to, ka, rīkojoties ar ES klasificēto informāciju, savos dienestos un telpās 1. pantā minēto reglamentu ievēro:

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

b) citi dalībvalstu valsts pārvaldes iestāžu locekļi, kas rīkojas ar ES klasificēto informāciju neatkarīgi no tā, vai tie strādā dalībvalstu teritorijās vai ārzemēs, un

c) dalībvalstu ārējie līgumslēdzēji un norīkotais personāls, kas rīkojas ar ES klasificēto informāciju.

Dalībvalstis tūlīt informē Padomes Ģenerālsekretariātu par veiktajiem pasākumiem.

3. Pasākumus, kas minēti 1. un 2. punktā, veic līdz 2001. gada 30. novembrim.

3. pants

Lai ievērotu drošības pamatprincipus un minimālos standartus, kas ietverti pielikuma I daļā, ģenerālsekretārs/Augstais pārstāvis var veikt pasākumus saskaņā ar pielikuma II daļas I iedaļas 1. un 2. punktu.

4. pants

No šā lēmuma piemērošanas dienas ar šo lēmumu aizstāj:

a) Padomes Lēmumu (1998. gada 27. aprīlis) par kārtību, kādā Padomes Ģenerālsekretariāta ierēdņiem un darbiniekiem var atļaut piekļuvi Padomes rīcībā esošai klasificētai informācijai ([1]);

b) ģenerālsekretāra/augstā pārstāvja Lēmumu (2000. gada 27. jūlijs) par pasākumiem klasificētas informācijas aizsardzībai, kas piemērojami Padomes Ģenerālsekretariātam ([2]);

c) Padomes ģenerālsekretāra Lēmumu 433/97 (1997. gada 22. maijs) par drošības pārbaudes procedūru ierēdņiem, kas atbild par *Cortesy* tīkla darbību.

5. pants

1. Šis lēmums stājas spēkā tā publicēšanas dienā.

2. To piemēro no 2001. gada 1. decembra.

([1]) OV L 140, 12.5.1998., 12. lpp.
([2]) OV C 239, 23.8.2000., 1. lpp.

▼B

PIELIKUMS

EIROPAS SAVIENĪBAS PADOMES DROŠĪBAS REGLAMENTS

▼B

SATURS

I DAĻA

Drošības pamatprincipi un minimālie standarti

II DAĻA

I IEDAĻA

Drošības organizācija Eiropas Savienības Padomē

II IEDAĻA

Klasifikācijas un marķējumi

III IEDAĻA

Klasifikācijas vadība

IV IEDAĻA

Fiziskā drošība

V IEDAĻA

Vispārīgie noteikumi par vajadzības pēc informācijas principu un drošības pārbaudi

VI IEDAĻA

Drošības pārbaudes procedūra Padomes Ģenerālsekretariāta ierēdņiem un citiem darbiniekiem

VII IEDAĻA

ES klasificētā materiāla sagatavošana, izplatīšana, nosūtīšana, uzglabāšana un iznīcināšana

VIII IEDAĻA

Très secret UE/ES sevišķi slepenās informācijas reģistri
IX IEDAĻA

Drošības pasākumi, kas piemērojami īpašu sanāksmju laikā, ko rīko ārpus Padomes telpām un kur izskata augsta riska jautājumus

X IEDAĻA

Drošības pārkāpumi un ES klasificētās informācijas apdraudēšana

XI IEDAĻA

Informācijas tehnoloģijas un komunikācijas sistēmās apstrādātās informācijas aizsardzība

XII IEDAĻA

ES klasificētās informācijas nodošana trešām valstīm un starptautiskām organizācijām

Papildinājumi

1. papildinājums

Valsts drošības iestāžu saraksts

2. papildinājums

Valstu drošības klasifikāciju salīdzinājums

3. papildinājums

Praktiskās klasifikācijas metodiskais līdzeklis

4. papildinājums

Pamatnostādnes ES klasificētās informācijas nodošanai trešām valstīm un starptautiskām organizācijām

▼B

— 1. līmeņa sadarbība

5. papildinājums

Pamatnostādnes ES klasificētās informācijas nodošanai trešām valstīm un starptautiskām organizācijām

— 2. līmeņa sadarbība

6. papildinājums

Pamatnostādnes ES klasificētās informācijas nodošanai trešām valstīm un starptautiskām organizācijām

— 3. līmeņa sadarbība

▼B

I DAĻA

DROŠĪBAS PAMATPRINCIPI UN MINIMĀLIE STANDARTI

IEVADS

1. Šajos noteikumos ir paredzēti drošības pamatprincipi un minimālie standarti, kas attiecīgā veidā jāievēro Padomei, Padomes Ģenerālsekretariātam, dalībvalstīm un Eiropas Savienības decentralizētajām aģentūrām (še turpmāk "ES decentralizētās aģentūras"), lai nodrošinātu drošību un katram būtu garantija, ka ir izveidots kopējs aizsardzības standarts.

2. Termins "ES klasificētā informācija" nozīmē jebkādu informāciju un materiālu, kura neatļauta izpaušana varētu dažādās pakāpēs izraisīt traucējumu ES interesēm vai vienai vai vairākām tās dalībvalstīm neatkarīgi no tā, vai šādas informācijas izcelsme ir ES vai tā saņemta no dalībvalstīm, trešām valstīm vai starptautiskām organizācijām.

3. Šajā reglamentā:

   a) "dokuments" nozīmē jebkuru vēstuli, piezīmi, protokolu, ziņojumu, memorandu, signālu/ziņojumu, skici, fotoattēlu, diapozitīvu, filmu, karti, shēmu, plānu, piezīmju grāmatiņu, matricu, rakstāmmašīnas vai printera lentu, lentu, datora disku, lasāmatmiņas kompaktdisku vai jebkādu citu fizisko nesēju, uz kura ir ierakstīta informācija;

   b) "materiāls" nozīmē "dokumentu", kas definēts iepriekš a) apakšpunktā, kā arī jebkuru iekārtas vai ieroču sastāvdaļu, kas ir ražota vai atrodas ražošanas procesā.

4. Drošībai ir šādi galvenie mērķi:

   a) nodrošināt ES klasificēto informāciju pret spiegošanu, apdraudējumu vai neatļautu izpaušanu;

   b) nodrošināt komunikāciju un informācijas sistēmās un tīklos apstrādāto ES informāciju pret draudiem tās integritātei un pieejamībai;

   c) nodrošināt ierīces, kurās izvietota ES informācija, pret sabotāžu un ļaunprātīgu apzinātu kaitējumu;

   d) kļūmes gadījumā novērtēt izraisīto kaitējumu, ierobežot tā sekas un veikt vajadzīgos pasākumus stāvokļa izlabošanai.

5. Pareizas drošības pamati ir:

   a) katrā dalībvalstī — valsts drošības organizācija, kas atbild par:

      i) ziņu savākšanu un reģistrēšanu par spiegošanu, sabotāžu, terorismu un citām graujošām darbībām, un

      ii) attiecīgās valdības un līdz ar to Padomes informēšanu un konsultēšanu par drošības apdraudējuma raksturu un aizsardzības līdzekļiem pret to;

   b) katrā dalībvalstī un Padomes Ģenerālsekretariātā — tehniska informācijas drošības (INFOSEC) iestāde, kas atbild par darbu ar attiecīgo drošības iestādi, lai sniegtu informāciju un konsultācijas par tehniskiem draudiem drošībai un aizsardzības līdzekļiem pret to;

   c) regulāra sadarbība valdības struktūrvienību, aģentūru un attiecīgu Padomes Ģenerālsekretariāta dienestu starpā, lai pēc vajadzības konstatētu un ieteiktu:

      i) kādu informāciju, resursus un ierīces nepieciešams aizsargāt un

      ii) kopējus aizsardzības standartus.

6. Ja tas attiecas uz konfidencialitāti, ir nepieciešama rūpība un pieredze, lai izvēlētos aizsargājamo informāciju un materiālus un novērtētu tam nepieciešamo aizsardzības pakāpi. Ir būtiski, lai aizsardzības pakāpe atbilstu atsevišķās aizsargājamās informācijas un materiāla drošības nozīmībai. Lai nodrošinātu vienmērīgu informācijas plūsmu, veic pasākumus, lai izvairītos no pārklasifikācijas. Klasifikācijas sistēma ir šo principu īstenošanas instru-

▼B

ments; līdzīga klasifikācijas sistēma jāievēro, plānojot un organizējot veidus, kā novērst spiegošanu, sabotāžu, terorismu un citus draudus, lai lielākie drošības pasākumi tiktu piemēroti vissvarīgākajām telpām, kurās atrodas klasificēta informācija, un visaugstākā riska punktiem tajās.

PAMATPRINCIPI

7. Drošības pasākumi:

a) ir attiecināmi uz visām personām, kurām ir pieeja klasificētai informācijai, klasificētas informācijas nesējiem, visām telpām, kurās atrodas šāda informācija un svarīgas ierīces;

b) ir izstrādāti, lai noteiktu personas, kuru postenis var apdraudēt klasificētās informācijas un svarīgu ierīču, kurās atrodas klasificēta informācija, drošību, un paredzētu to izslēgšanu vai pārvietošanu;

c) aizkavē visu nepiederošu personu piekļuvi klasificētai informācijai vai ierīcēm, kuras to satur;

d) nodrošina, ka klasificētu informāciju izplata vienīgi, pamatojoties uz vajadzības pēc informācijas principu, kas ir būtisks visiem drošības aspektiem;

e) nodrošina visas informācijas neatkarīgi no tā, vai tā ir vai nav klasificēta, un jo īpaši tādas informācijas, ko uzglabā, apstrādā vai pārraida elektromagnētiskā veidā, integritāti (proti, novēršot sabojāšanu vai neatļautas izmaiņas, vai neatļautu izdzēšanu) un pieejamību (proti, netiek liegta piekļuve tiem, kuriem nepieciešama un ir atļauta piekļuve).

DROŠĪBAS ORGANIZĒŠANA

Kopējie minimālie standarti

8. Padome un dalībvalstis nodrošina, lai tiktu ievēroti kopējie minimālie drošības standarti visas administratīvās un/vai valdības struktūrvienības, citas ES iestādes, aģentūras un līgumslēdzēji, lai ES informāciju varētu nodot tālāk, uzticoties, ka tā tiks apstrādāta ar līdzvērtīgu rūpību. Šādi minimālie standarti ietver personāla pārbaudes kritērijus un ES klasificētās informācijas aizsardzības procedūras. ►**M3** Šādi minimālie standarti ietver arī minimālos standartus, ko piemēro, ja Padomes Ģenerālsekretariāts rūpnieciskiem līgumslēdzējiem vai citām struktūrām uztic uzdevumus, kas saistīti ar ES klasificēto informāciju un/vai kuros tā ietverta; šie kopējie minimālie standarti ir ietverti II daļas XIII iedaļā. ◄

PERSONĀLA DROŠĪBA

Personāla pārbaude

9. Visas personas, kuras pieprasa piekļuvi informācijai, kas klasificēta kā ES konfidenciālā (*CONFIDENTIEL UE*) informācija vai stingrāk, pirms šādas atļaujas piešķiršanas pienācīgi pārbauda. Līdzīga pārbaude ir nepieciešama tādām personām, kuru pienākumi ietver sakaru un informācijas sistēmu, kas satur klasificētu informāciju, tehnisku ekspluatēšanu vai uzturēšanu. Šo pārbaudi izstrādā, lai noteiktu, vai šādi indivīdi:

a) ir neapšaubāmi uzticami;

b) ir ar tādu raksturu un atbildību, kas nerada šaubas par viņu godīgumu, rīkojoties ar klasificēto informāciju, vai

c) var būt neaizsargāti pret ārvalstu vai citu avotu spiedienu, piemēram, iepriekšējās dzīvesvietas vai pagātnes saistību dēļ, kas var ietvert draudus drošībai;

Īpaša rūpība pārbaudes procedūrās jāpievērš personām:

d) kam jāpiešķir pieeja ES sevišķi slepenajai (*TRÈS SECRET UE/EU TOP SECRET*) informācijai;

e) kas ieņem amatus, kuri paredz regulāru piekļuvi ievērojamam ES slepenās (*SECRET UE*) informācijas apjomam;

▼B

f) kuru pienākumi piešķir viņiem īpašu piekļuvi komunikāciju un informācijas sistēmām, kas būtiskas uzdevumam, un līdz ar to — iespēju neatļauti piekļūt lieliem ES klasificētās informācijas apjomiem vai radīt nopietnu kaitējumu misijai ar tehniskās sabotāžas darbībām.

Apstākļos, kas uzsvērti d), e) un f) apakšpunktā, iespējami pilnīgi izmanto iepriekšējas darbības izmeklēšanas metodi.

10. Ja darbā jāpieņem personas, kurām nav pamatotas vajadzības pēc informācijas, apstākļos, kad tām var būt pieeja ES klasificētajai informācijai (piemēram, kurjeri, drošības aģenti, tehniskās apkopes personāls u.c.), tām vispirms veic pienācīgu drošības pārbaudi.

Personāla pārbaudes uzskaite

11. Visi dienesti, institūcijas vai iestādes, kas rīkojas ar ES klasificēto informāciju vai glabā misijai svarīgas komunikācijas vai informācijas sistēmas, uztur šajās iestādēs norīkotajam personālam piešķirto atļauju reģistru. Katru atļauju pēc vajadzības pārbauda, lai nodrošinātu, ka tā ir atbilstoša attiecīgās personas pašreizējam uzdevumam; to prioritāri pārbauda atkārtoti, ja tiek saņemta jauna informācija, kas norāda, ka šīs personas darbs ar klasificēto informāciju vairs neatbilst drošības interesēm. Atļauju reģistru glabā attiecīgā dienesta, institūcijas vai iestādes atbildīgais par drošību.

Personāla sagatavošana drošības jautājumos

12. Visu personālu, kas ieņem amatus, kuros tam var būt piekļuve klasificētai informācijai, rūpīgi sagatavo, stājoties amatā un pēc regulāriem starplaikiem, lai ievērotu drošību un tās nodrošināšanas procedūras. Ir lietderīgi pieprasīt, lai viss šāds personāls rakstveidā apliecinātu, ka tas pilnībā saprot amatiem atbilstošo drošības reglamentu.

Vadības pienākumi

13. Vadītāju pienākums ir zināt tos darbiniekus, kuri ir iesaistīti darbā ar klasificētu informāciju vai kuriem ir piekļuve uzdevumam būtiskām komunikācijas vai informācijas sistēmām, kā arī reģistrēt jebkādus starpgadījumus vai acīmredzamus ietekmējamības gadījumus, kas var iespaidot drošību, un ziņot par tiem.

Personāla drošības statuss

14. Izveido procedūras, lai nodrošinātu, ka gadījumos, kad par kādu indivīdu kļūst zināma negatīva informācija, tiek konstatēts, vai indivīds strādā ar klasificētu informāciju, vai viņam ir piekļuve uzdevumam būtiskām komunikācijas vai informācijas sistēmām, un tiek informēta attiecīgā iestāde. Ja konstatē, ka šāds indivīds rada drošības apdraudējuma iespējamību, viņu norobežo vai pārceļ no amata, kurā viņš var apdraudēt drošību.

FIZISKĀ DROŠĪBA

Vajadzība pēc aizsardzības

15. ES klasificētās informācijas aizsardzības nodrošināšanai piemēroto fiziskās drošības pasākumu pakāpe ir proporcionāla uzglabātās informācijas un materiāla klasifikācijai, apjomam un apdraudējumam. Tādēļ jāraugās, lai tiktu novērsta pārāk augsta un pārāk zema klasifikācija, un klasifikācija regulāri jāpārskata. Visi ES klasificētās informācijas turētāji ievēro vienotu praksi attiecībā uz šīs informācijas klasifikāciju, kā arī ievēro kopējus aizsardzības standartus attiecībā uz informācijas un materiāla, kam nepieciešama aizsardzība, glabāšanu, nosūtīšanu un nodošanu.

Pārbaudes

16. Pirms iziet no zonām, kurās atrodas ES klasificētā informācija, atbildīgās personas nodrošina to, ka tā tiek droši uzglabāta un darbojas visas drošības ierīces (slēdzenes, trauksmes signāli u.c.). Turpmākas neatkarīgas pārbaudes veic pēc darba dienas beigām.

Ēku drošība

▼B

17. Ēkas, kurās atrodas ES klasificētā informācija vai uzdevumam būtiskas komunikācijas un informācijas sistēmas, aizsargā pret nesankcionētu piekļuvi. ES klasificētās informācijas aizsardzības raksturs, piemēram, logu aizrestošana, durvju slēdzenes, durvju apsardze, automatizētas iekļūšanas kontroles sistēmas, drošības pārbaudes un patruļas, signalizācijas sistēmas, iekļūšanas noteikšanas sistēmas un sargsuņi, ir atkarīgs no:

    a) aizsargājamās informācijas un materiāla klasifikācijas, apjoma un atrašanās vietas ēkā;

    b) šai informācijai un materiālam paredzēto seifu kvalitātes;

    c) ēkas fiziskajām īpašībām un atrašanās vietas.

18. Komunikācijas un informācijas sistēmām piemērotās aizsardzības raksturs līdzīgi ir atkarīgs no riskam pakļauto aktīvu vērtības un iespējamā kaitējuma novērtējuma drošības apdraudējuma gadījumā, no ēkas, kurā glabājas sistēma, fiziskajām īpašībām un atrašanās vietas, kā arī no sistēmas atrašanās vietas ēkā.

Ārkārtas rīcības plāni

19. Iepriekš sagatavo sīki izstrādātus plānus klasificētas informācijas aizsardzībai vietējas vai valsts mēroga ārkārtējas situācijas gadījumā.

INFORMĀCIJAS DROŠĪBA (*INFOSEC*)

20. *INFOSEC* ir saistīta ar drošības pasākumu identificēšanu un piemērošanu, lai aizsargātu informāciju, kuru apstrādā, uzglabā vai pārraida sakaru, informācijas un citās elektroniskajās sistēmās, pret konfidencialitātes, integritātes vai pieejamības zaudēšanu nejauši vai ar nolūku. Veic attiecīgus pretpasākumus, lai novērstu piekļuvi ES informācijai nesankcionētiem lietotājiem, lai novērstu piekļuves ES informācijai atteikumu sankcionētiem lietotājiem un novērstu ES informācijas sabojāšanu, neatļautu izmainīšanu, vai izdzēšanu.

AIZSARDZĪBA PRET SABOTĀŽU UN CITIEM ĻAUNPRĀTĪGIEM APZINĀTIEM KAITĒJUMIEM

21. Fiziska piesardzība, lai aizsargātu svarīgas iekārtas, kurās atrodas klasificēta informācija, ir vislabākais drošības nodrošinājums pret sabotāžu un ļaunprātīgu apzinātu kaitējumu, un tā nav efektīvi aizstājama tikai ar personāla pārbaudi. Kompetentā valsts institūcija ievāc ziņas par spiegošanu, sabotāžu, terorismu un citām graujošām darbībām.

ES KLASIFICĒTĀS INFORMĀCIJAS NODOŠANA TREŠĀM VALSTĪM UN STARPTAUTISKĀM ORGANIZĀCIJĀM

22. Lēmumu nodot ES klasificēto informāciju, kuras izcelsme ir Padomē, trešai valstij vai starptautiskai organizācijai, pieņem Padome. Ja informācijas, kuras nodošana ir vajadzīga, autors nav Padome, Padome vispirms saņem autora piekrišanu nodošanai. Ja autoru nevar noteikt, Padome uzņemas tā atbildību.

23. Ja Padome saņem klasificētu informāciju no trešām valstīm, no starptautiskām organizācijām vai no citām trešām pusēm, šai informācijai nodrošina aizsardzību, kas atbilst tās klasifikācijai un ir līdzvērtīga šajā reglamentā noteiktajiem ES klasificētās informācijas standartiem vai augstākiem standartiem, kādus var pieprasīt trešā puse, kas nodod informāciju. Var rīkot savstarpējas pārbaudes.

24. Iepriekš minētos principus īsteno saskaņā ar sīki izstrādātiem noteikumiem, kas norādīti II daļā.

▼B

II DAĻA

1. IEDAĻA

EIROPAS SAVIENĪBAS PADOMES DROŠĪBAS ORGANIZĀCIJA

Ģenerālsekretārs/augstais pārstāvis

1. Ģenerālsekretārs/augstais pārstāvis:

   a) īsteno Padomes drošības politiku;

   b) izskata drošības jautājumus, ko viņam iesniedz Padome vai tās kompetentās iestādes;

   c) ciešā sadarbībā ar dalībvalstu valsts drošības iestādēm pārbauda jautājumus, kas saistīti ar Padomes drošības politiku. 1. papildinājumā ir ietverts šo iestāžu saraksts.

2. Ģenerālsekretārs/augstais pārstāvis jo īpaši atbild par:

   a) visu ar Padomes darbībām saistīto drošības jautājumu koordinēšanu;

   b) pieprasījumu katrai dalībvalstij izveidot centrālo ES sevišķi slepenās (*TRÈS SECRET UE/EU TOP SECRET*) informācijas reģistru un pieprasījumu pēc vajadzības izveidot šādu reģistru ES decentralizētajās aģentūrās;

   c) pieprasījumu nosūtīšanu dalībvalstu atbildīgajām iestādēm, lai Valsts drošības iestādes nodrošinātu Padomes Ģenerālsekretariātā nodarbinātā personāla drošības pārbaudes saskaņā ar VI iedaļu;

   d) visu ES klasificētās informācijas noplūžu, kas saskaņā ar pirmā acumirkļa pierādījumiem ir notikušas Padomes Ģenerālsekretariātā vai jebkurā no ES decentralizētajām aģentūrām, izmeklēšanu vai izmeklēšanas pasūtīšanu;

   e) pieprasījumu attiecīgajām drošības iestādēm uzsākt izmeklēšanu, ja šķiet, ka notikusi ES klasificētās informācijas noplūde ārpus Padomes Ģenerālsekretariāta vai ES decentralizētajām aģentūrām, un izmeklēšanas koordinēšanu, ja ir iesaistīta vairāk nekā viena drošības iestāde;

   f) periodisku drošības pasākumu pārbaužu veikšanu kopīgi un vienojoties ar attiecīgo Valsts drošības iestādi, lai aizsargātu ES klasificēto informāciju dalībvalstīs;

   g) ciešas sadarbības uzturēšanu ar visām attiecīgajām drošības iestādēm, lai panāktu vispārēju drošības koordinēšanu;

   h) pastāvīgu Padomes drošības politikas un procedūru pārskatīšanu un attiecīgu ieteikumu sagatavošanu vajadzības gadījumā. Šajā sakarā viņš iepazīstina Padomi ar ikgadējo pārbaudes plānu, ko sagatavo Padomes Ģenerālsekretariāta Drošības birojs.

Padomes drošības komiteja

3. Izveido Drošības komiteju. Tās sastāvā ir pa vienam pārstāvim no katras dalībvalsts Valsts drošības iestādes. To vada ģenerālsekretārs/augstais pārstāvis vai viņa deleģēts pārstāvis. Var uzaicināt piedalīties arī ES decentralizēto aģentūru pārstāvjus, ja tiek izskatīti jautājumi, kas attiecas uz viņiem.

4. Drošības komitejas sanāksmes notiek saskaņā ar Padomes norādījumiem, pēc ģenerālsekretāra/augstā pārstāvja, vai kādas Valsts drošības iestādes pieprasījuma. Komiteja ir pilnvarota pārbaudīt un izvērtēt visus drošības jautājumus, kas saistīti ar Padomes darbu, un pēc vajadzības sniegt Padomei ieteikumus. Attiecībā uz Padomes Ģenerālsekretariāta darbību komiteja ir pilnvarota sniegt ieteikumus par drošības jautājumiem ģenerālsekretāram/augstajam pārstāvim.

▼B

Padomes Ģenerālsekretariāta Drošības birojs

5. Lai izpildītu 1. un 2. punktā minētos pienākumus, ģenerālsekretāra/augstā pārstāvja rīcībā ir Padomes Ģenerālsekretariāta Drošības birojs, lai koordinētu, uzraudzītu un īstenotu drošības pasākumus.

6. Padomes Ģenerālsekretariāta Drošības biroja vadītājs ir ģenerālsekretāra/augstā pārstāvja galvenais padomdevējs drošības jautājumos un darbojas kā Drošības komitejas sekretārs. Šajā sakarā viņš vada drošības reglamenta atjaunināšanu un koordinē drošības pasākumus ar dalībvalstu kompetentām iestādēm un, pēc vajadzības, ar starptautiskām organizācijām, kas saistītas ar Padomi ar drošības nolīgumiem. Šajā nolūkā viņš darbojas kā sadarbības koordinators.

7. Padomes Ģenerālsekretariāta drošības dienesta vadītājs atbild par IT sistēmu un tīklu akreditāciju Padomes Ģenerālsekretariātā. Padomes Ģenerālsekretariāta drošības dienesta vadītājs un attiecīgā Valsts drošības iestāde vajadzības gadījumā kopīgi lemj par IT sistēmu un tīklu, kur iesaistīts Padomes Ģenerālsekretariāts, dalībvalstis, ES decentralizētās aģentūras un/vai trešās puses (valstis var starptautiskas organizācijas), akreditāciju.

ES decentralizētās aģentūras

8. Katrs ES decentralizētās aģentūras direktors atbild par drošības īstenošanu savā iestādē. Viņš parasti izvirzīs kādu savu darbinieku kā personu, kas šajā jomā viņam atskaitās. Šo darbinieku ieceļ par atbildīgo par drošību.

Dalībvalstis

9. Katrai dalībvalstij ir jāizraugās Valsts drošības iestāde, kas ir atbildīga par ES klasificētās informācijas drošību ([1]).

10. Katras dalībvalsts pārvaldē attiecīgajai Valsts drošības iestādei jābūt atbildīgai par:

   a) šajā dalībvalstī vai ārvalstīs jebkāda valsts dienesta, valsts vai privātas iestādes vai aģentūras glabātās ES klasificētās informācijas drošības uzturēšanu;

   b) ES sevišķi slepenās (*TRÈS SECRET UE/EU TOP SECRET*) informācijas reģistru izveides pilnvarojumu (šo pilnvarojumu var deleģēt atbildīgajam par ES sevišķi slepenās (*TRÈS SECRET UE/EU TOP SECRET*) informācijas kontroli centrālā reģistrā);

   c) ES klasificētās informācijas aizsardzībai paredzēto drošības pasākumu periodisku pārbaudi;

   d) to, lai visiem valsts pilsoņiem, kā arī ārvalstniekiem, kuri nodarbināti attiecīgās valsts struktūrvienībā, iestādē vai aģentūrā un kuriem var būt pieejama ES informācija, kas klasificēta kā ES sevišķi slepenā (*TRÈS SECRET UE/EU TOP SECRET*), ES slepenā (*SECRET UE*) un ES konfidenciālā (*CONFIDENTIEL UE*) informācija, būtu veikta drošības pārbaude;

   e) tādu drošības plānu izstrādi, ko uzskata par nepieciešamiem, lai novērstu ES klasificētās informācijas nokļūšanu nepiederošu personu rīcībā.

Savstarpējās drošības pārbaudes

11. Padomes Ģenerālsekretariāta Drošības dienests un attiecīgā Valsts drošības iestāde kopīgi un savstarpēji vienojoties veic periodiskas drošības pasākumu pārbaudes, kas paredzēti ES klasificētās informācijas aizsardzībai Padomes Ģenerālsekretariātā un dalībvalstu pastāvīgajās pārstāvniecībās Eiropas Savienībā, kā arī dalībvalstu telpās Padomes ēkās ([2]).

12. Padomes Ģenerālsekretariāta Drošības dienests vai, pēc ģenerālsekretāra pieprasījuma, uzņēmējas dalībvalsts Valsts drošības iestāde veic periodiskas

([1]) Valsts drošības iestāžu, kas atbild par ES klasificētās informācijas drošību, saraksts ir iekļauts 1. papildinājumā.

([2]) Neierobežojot Vīnes 1961. gada Konvenciju par diplomātiskiem sakariem.

▼B

pārbaudes ES klasificētās informācijas aizsardzībai paredzētajiem drošības pasākumiem ES decentralizētajās aģentūrās.

▼B

II IEDAĻA

KLASIFIKĀCIJAS UN MARĶĒJUMI

KLASIFIKĀCIJAS LĪMEŅI [1]

Informāciju klasificē šādos līmeņos:

1. ES sevišķi slepeni (*TRÈS SECRET UE/EU TOP SECRET*): šo klasifikāciju piemēro tikai informācijai un materiālam, kura neatļauta izpaušana var izraisīt ārkārtīgi nopietnu apdraudējumu Eiropas Savienības vai vienas vai vairāku tās dalībvalstu būtiskām interesēm.

2. ES slepeni (*SECRET UE*): šo klasifikāciju piemēro tikai informācijai un materiālam, kura neatļauta izpaušana varētu nopietni kaitēt Eiropas Savienības vai vienas, vai vairāku tās dalībvalstu būtiskām interesēm.

3. ES konfidenciāli (*CONFIDENTIEL UE*): šo klasifikāciju piemēro informācijai un materiālam, kura neatļauta izpaušana varētu kaitēt Eiropas Savienības vai vienas vai vairāku tās dalībvalstu būtiskām interesēm.

4. ES ierobežotas pieejamības (*RESTREINT UE*): šo klasifikāciju piemēro informācijai un materiālam, kura neatļauta izpaušana varētu būt neizdevīga Eiropas Savienības vai vienas vai vairāku tās dalībvalstu interesēm.

MARĶĒJUMI

5. Brīdinājuma marķējumu var izmantot, lai precizētu jomu, uz kuru attiecas dokuments, vai lai norādītu konkrētu izplatīšanu, pamatojoties uz vajadzību pēc informācijas.

6. Marķējumu *ESDP/PESD* izmanto dokumentiem un to kopijām, kas attiecas uz Savienības vai vienas vai vairāku tās dalībvalstu drošību un aizsardzību, vai kas attiecas uz militāru vai nemilitāru krīzes pārvarēšanu.

7. Uz dažiem dokumentiem, proti, tiem, kas saistīti ar informācijas tehnoloģiju (IT) sistēmām, var būt papildu marķējums, kas paredz papildu drošības pasākumus, kuri noteikti attiecīgā reglamentā.

KLASIFIKĀCIJAS UN MARĶĒJUMU PIESTIPRINĀŠANA

8. Klasifikāciju un marķējumus pielieto šādi:

   a) ES ierobežotas pieejamības (*RESTREINT UE*) dokumentiem — ar mehāniskiem vai elektroniskiem līdzekļiem;

   b) ES konfidenciāliem (*CONFIDENTIEL UE*) dokumentiem — ar mehāniskiem līdzekļiem un ar rokām vai iespiežot uz iepriekš apzīmogota, reģistrēta papīra;

   c) ES slepeniem (*SECRET UE*) un ES sevišķi slepeniem (*TRÈS SECRET UE/EU TOP SECRET*) dokumentiem — ar mehāniskiem līdzekļiem vai ar rokām.

([1]) Salīdzinoša ES, NATO, RES un dalībvalstu drošības pakāpju tabula ir iekļauta 2. papildinājumā.

▼B

III IEDAĻA

KLASIFIKĀCIJAS VADĪBA

1. Informāciju klasificē tikai vajadzības gadījumā. Šo klasifikāciju norāda skaidri un pareizi un saglabā tikai tik ilgi, kamēr informācijai nepieciešama aizsardzība.

2. Atbildību par informācijas klasificēšanu un jebkādu ierindošanu zemākā kategorijā vai deklasificēšanu ([1]) uzņemas vienīgi izcelsmes iestāde.

   Padomes Ģenerālsekretariāta ierēdņi un citi darbinieki klasificē, ierindo zemākā kategorijā vai deklasificē informāciju pēc to ģenerāldirektora norādījuma vai ar viņa piekrišanu.

3. Sīki izstrādātās procedūras rīcībai ar klasificētiem dokumentiem ir veidotas, lai nodrošinātu to, ka tiem piemēro aizsardzību, kas atbilstoša tajos ietvertajai informācijai.

4. To personu skaits, kam ir atļauts radīt ES sevišķi slepenus (*TRÈS SECRET UE/EU TOP SECRET*) dokumentus, ir iespējami mazs, un viņu vārdi ir iekļauti sarakstā, ko sastādījis Padomes Ģenerālsekretariāts, katra dalībvalsts un, ja vajadzīgs, katra ES decentralizētā aģentūra.

KLASIFIKĀCIJU PIEMĒROŠANA

5. Dokumenta klasifikāciju nosaka pēc tā satura konfidencialitātes līmeņa saskaņā ar definīciju II iedaļas 1. līdz 4. punktā. Svarīgi, lai klasifikāciju izmantotu pareizi un iespējami maz. Tas īpaši attiecas uz ES sevišķi slepeno (*TRÈS SECRET UE/EU TOP SECRET*) klasifikāciju.

6. Dokumenta izcelsmes iestādei, kam ir jāpiešķir klasifikācija, jāņem vērā iepriekš norādītais reglaments un jāsamazina tendence piešķirt pārāk augstu vai pārāk zemu klasifikācijas kategoriju.

   Lai gan pirmajā mirklī var šķist, ka augstāka klasifikācija garantē dokumentam lielāku aizsardzību, regulāras pārāk augstas kategorijas piešķiršanas rezultātā var zust uzticība klasifikācijas sistēmas pamatotībai.

   No otras puses, dokumentiem nepiešķir pārāk zemu kategoriju nolūkā izvairīties no ierobežojumiem saistībā ar aizsardzību.

   Klasifikācijas praktisks metodiskais līdzeklis ir ietverts 3. papildinājumā.

7. Konkrēta dokumenta atsevišķām lappusēm, punktiem, iedaļām, pielikumiem, papildinājumiem un pievienojumiem, iespējams, nepieciešamas atšķirīgas klasifikācijas, un tos attiecīgi marķē. Dokumenta klasifikācija kopumā ir tāda pati kā tā daļai ar visaugstāko klasifikāciju.

8. Uz pievienojumiem attiecināmas vēstules vai piezīmes, klasifikācija ir tikpat augsta, kā tās pievienojumu visaugstākā klasifikācija. Izcelsmes iestādei skaidri jānorāda, kādā līmenī tai jābūt klasificētai, kad to atdala no tās pievienojumiem.

IERINDOŠANA ZEMĀKĀ KATEGORIJĀ UN DEKLASIFIKĀCIJA

9. ES klasificētos dokumentus var ierindot zemākā kategorijā vai deklasificēt tikai ar izcelsmes iestādes atļauju un, nepieciešamības gadījumā, pēc apspriedes ar citām ieinteresētajām pusēm. Ierindošanu zemākā kategorijā vai deklasificēšanu apstiprina rakstveidā. Izcelsmes iestāde, dalībvalsts, birojs, tiesību pārņēmēja organizācija vai augstāka institūcija ir atbildīga par savu adresātu informēšanu par izmaiņām, un tie savukārt ir atbildīgi par jebkādu tālāku adresātu, kuriem tie ir nosūtījuši vai nokopējuši dokumentu, informēšanu par izmaiņām.

10. Ja iespējams, izcelsmes iestādes uz klasificētajiem dokumentiem norāda datumu vai laika posmu, kad tā saturu var ierindot zemākā kategorijā vai

([1]) Ierindošana zemākā kategorijā (déclassement) nozīmē klasifikācijas līmeņa pazemināšanu; deklasifikācija (*déclassification*) nozīmē jebkādas klasifikācijas noņemšanu.

▼B

deklasificēt. Citādi tās pārskata dokumentus vismaz reizi piecos gados, lai pārliecinātos, vai ir nepieciešama sākotnējā klasifikācija.

IV IEDAĻA

FIZISKĀ DROŠĪBA

VISPĀRĪGI NOTEIKUMI

1. Fiziskās drošības galvenais mērķis ir novērst nepiederošas personas piekļuvi ES klasificētajai informācijai un/vai materiālam.

DROŠĪBAS PRASĪBAS

2. Visas telpas, zonas, ēkas, biroji, istabas, sakaru un informācijas sistēmas u. c., kur tiek uzglabāta un/vai apstrādāta ES klasificētā informācija un materiāli, tiek aizsargātas ar atbilstošu fiziskās drošības pasākumu palīdzību.

3. Lemjot, kāda fiziskās drošības aizsardzības pakāpe ir nepieciešama, ņem vērā visus attiecīgos faktorus, piemēram:

   a) informācijas un/vai materiāla klasifikāciju;

   b) uzglabātās informācijas daudzumu un veidu (piemēram, cietā kopija, elektroniskie informācijas nesēji);

   c) vietēji novērtēto apdraudējumu no izlūkošanas dienestiem, kuru mērķis ir ES, dalībvalstis un/vai citas iestādes vai trešās puses, kuru rīcībā ir ES klasificētā informācija, proti, no sabotāžas, terorisma un citām graujošām un/vai kriminālām darbībām.

4. Pielietoto drošības pasākumu mērķis ir:

   a) neatļaut iekļūšanu slepus vai ar spēku;

   b) novērst, kavēt un atklāt nelojāla personāla (iekšējā spiega) darbības;

   c) nepieļaut to Padomes Ģenerālsekretariāta, dalībvalstu valdības struktūrvienību un/vai citu iestāžu vai trešo pušu, kurām nav vajadzības pēc informācijas, piekļuvi ES klasificētajai informācijai.

FIZISKĀS DROŠĪBAS PASĀKUMI

Drošības zonas

5. Zonas, kur apstrādā un uzglabā informāciju, kas klasificēta kā ES konfidenciālā (*CONFIDENTIEL UE*) vai augstāk, organizē un strukturē tā, lai tās atbilstu vienam no šiem nosacījumiem:

   a) I kategorijas drošības zona: zona, kurā apstrādā un uzglabā informāciju, kas klasificēta kā ES konfidenciālā (*CONFIDENTIEL UE*) vai augstāk, tā, lai ieiešana tajā praktiskos nolūkos ietvertu pieeju klasificētajai informācijai. Šādai zonai nepieciešams:

      i) skaidri noteikts un aizsargāts perimetrs, caur kuru ieeja un izeja vienmēr tiek kontrolēta;

      ii) ieejas kontroles sistēma, kura pieņem tikai tos, kuri ir pienācīgi pārbaudīti un kuriem ir īpaši atļauts zonā ienākt;

      iii) zonā parasti uzglabātās informācijas klasifikācijas specifikācija, proti, informācijas, kurai piekļuvi dod ieeja;

   b) II kategorijas drošības zona: zona, kurā apstrādā un uzglabā informāciju, kas klasificēta kā ES konfidenciālā (*CONFIDENTIEL UE*) vai augstāk, lai tā ar iekšēji noteiktas kontroles palīdzību būtu aizsargāta no nepiederošu personu piekļuves, piemēram, telpās, kur atrodas biroji, kuros parasti apstrādā un uzglabā informāciju, kas klasificēta kā ES konfidenciālā (*CONFIDENTIEL UE*) vai augstāk. Šādai zonai nepieciešams:

      i) skaidri noteikts un aizsargāts perimetrs, caur kuru ieeja un izeja vienmēr tiek kontrolēta;

▼B

ii) ieejas kontroles sistēma, kura brīvi pieņem tikai tos, kuri ir pienācīgi pārbaudīti un kuriem ir īpaši atļauts zonā ienākt. Visām pārējām personām paredz eskortus vai līdzvērtīgus kontroles pasākumus, lai novērstu neatļautu piekļuvi ES klasificētajai informācijai un nekontrolētai ieejai zonās, kas pakļautas tehniskās drošības pārbaudēm.

Tās zonas, kurās 24 stundas neuzturas personāls, pārbauda tūlīt pēc parastā darba laika beigām, lai pārliecinātos, ka ES klasificētā informācija ir pietiekamā drošībā.

Administratīvā zona

6. Var izveidot mazākas drošības administratīvo zonu ap un ceļā uz I kategorijas un II kategorijas drošības zonu. Šādai zonai ir nepieciešams redzami noteikts perimetrs, kas ļauj pārbaudīt personālu un transportlīdzekļus. Administratīvajās zonās apstrādā un uzglabā ES ierobežotas pieejamības (*RESTREINT UE*) informāciju.

Ieejas un izejas kontroles pasākumi

7. Ieeju I kategorijas un II kategorijas drošības zonā kontrolē ar caurlaižu vai individuālās identifikācijas sistēmu, kas piemērojama pastāvīgajam personālam. Izveido arī apmeklētāju pārbaužu sistēmu, lai nepieļautu neatļautu piekļuvi ES klasificētajai informācijai. Caurlaižu sistēmas var papildināt ar automātisku identifikāciju, ko uzskata par papildinājumu, bet ne par pilnīgu aizstājēju sargiem. Izmaiņas apdraudējuma novērtējumā var ietvert ieejas un izejas kontroles pasākumu pastiprināšanu, piemēram, prominentu personu apmeklējumu laikā.

Apsardzes apgaitas

8. Apgaitām I kategorijas un II kategorijas drošības zonās ir jānotiek ārpus parastā darba laika, lai aizsargātu ES aktīvus pret apdraudējumu, kaitējumu vai zaudējumiem. Apgaitu biežumu noteiks vietējie apstākļi, taču tās orientējoši jāveic reizi divās stundās.

Seifi un glabātuves

9. ES klasificētās informācijas uzglabāšanai izmanto triju kategoriju seifus:

— A kategorija: seifi, kas valsts līmenī apstiprināti ES sevišķi slepenās (*TRÈS SECRET UE/EU TOP SECRET*) informācijas uzglabāšanai I kategorijas un II kategorijas drošības zonā,

— B kategorija: seifi, kas valsts līmenī apstiprināti ES slepenās (*SECRET UE*) un ES konfidenciālās (*CONFIDENTIEL UE*) informācijas uzglabāšanai I kategorijas un II kategorijas drošības zonā,

— C kategorija: biroja mēbeles, kas piemērotas tikai ES ierobežotas pieejamības (*RESTREINT UE*) informācijas uzglabāšanai.

10. Glabātuvēm, kas konstruētas I kategorijas vai II kategorijas drošības zonā, un visām I kategorijas drošības zonām, kur vaļējos plauktos vai uz diagrammām vai kartēm uzglabā informāciju, kas klasificēta kā ES konfidenciālā (*CONFIDENTIEL UE*) vai augstāk, sienas, grīdas un griestus ir sertificējusi Valsts drošības iestāde kā tādas, kas piedāvā līdzvērtīgu aizsardzību, kā seifa kategorija, kas apstiprināta tās pašas klasifikācijas informācijas uzglabāšanai.

Slēdzenes

11. Seifiem un glabātuvēm, kur uzglabā ES klasificēto informāciju, izmantotās slēdzenes atbilst šādiem standartiem:

— A grupa: valsts līmenī apstiprinātas A kategorijas seifiem,

— B grupa: valsts līmenī apstiprinātas B kategorijas seifiem,

— C grupa: derīgas tikai C kategorijas biroja mēbelēm.

Atslēgu un kombināciju kontrole

▼B

12. Seifu atslēgas no biroju ēkas neiznes. Seifu kombinācijas jāiegaumē personām, kurām tās jāzina. Pielietojumam ārkārtējā situācijā attiecīgās iestādes atbildīgais par drošību atbild par rezerves atslēgu glabāšanu un katras kombinācijas pierakstīšanu; pēdējās glabā atsevišķās aizzīmogotās necaurspīdīgās aploksnēs. Darba atslēgas, rezerves drošības atslēgas un kombinācijas glabā atsevišķos seifos. Šīm atslēgām un kombinācijām jānodrošina aizsardzība, kas nav mazāk stingra kā materiāls, kuram tās dod pieeju.

13. Personu skaitu, kam zināmas seifu kombinācijas, iespējami ierobežo. Kombinācijas iestata no jauna:

    a) saņemot jaunu seifu;

    b) kad notiek personāla maiņa;

    c) kad noticis apdraudējums, vai ir aizdomas par to;

    d) ieteicams ar sešu mēnešu starplaiku un vismaz reizi 12 mēnešos.

Ierīces iekļūšanas noteikšanai

14. Izmantojot signalizācijas sistēmas, slēgtas sistēmas televīziju un citas elektriskās ierīces, lai aizsargātu klasificēto informāciju, ir pieejama elektroapgāde ārkārtējām situācijām, lai nodrošinātu nepārtrauktu sistēmas darbību, ja tiek pārtraukta galvenā elektroapgāde. Vēl viena pamatprasība ir tāda, lai šādu sistēmu darbības traucējumu vai manipulācijas rezultātā ieslēgtos trauksmes signāls vai cits drošs brīdinājums uzraudzības personālam.

Apstiprinātas iekārtas

15. Valsts drošības iestādes, pamatojoties uz saviem vai divpusējiem avotiem, uztur jaunākos drošības iekārtu sarakstus pēc tipa un modeļa, ko tās apstiprinājušas klasificētās informācijas tiešai vai netiešai aizsardzībai dažādos precizētos apstākļos un ar dažādiem nosacījumiem. Padomes Ģenerālsekretariāta Drošības birojs uztur līdzīgu sarakstu, *inter alia*, informācijai no Valstu drošības iestādēm. ES decentralizētās aģentūras pirms šādu iekārtu iegādes konsultējas ar Padomes Ģenerālsekretariāta Drošības biroju un, vajadzības gadījumā, ar uzņēmējas dalībvalsts Valsts drošības iestādi.

Kopēšanas iekārtu un telefaksa aparātu fiziskā aizsardzība

16. Kopēšanas iekārtas un telefaksa aparātus fiziski aizsargā, ciktāl nepieciešams, lai nodrošinātu, ka tos var lietot tikai pilnvarotas personas un ka visi klasificētie produkti ir pakļauti pienācīgai kontrolei.

AIZSARDZĪBA PRET SLEPUS APSKATĪŠANU UN SLEPUS NOKLAUSĪŠANOS

Slepus apskatīšana

17. Cauru diennakti veic visus vajadzīgos pasākumus, lai nodrošinātu, ka ES klasificēto informāciju neierauga, pat nejauši, neviena nepiederoša persona.

Slepus noklausīšanās

18. Birojus vai zonas, kurās regulāri apspriež informāciju, kas klasificēta kā ES slepenā (*SECRET UE*), aizsargā pret pasīviem un aktīviem slepus noklausīšanās mēģinājumiem, ja risks to prasa. Par šādu mēģinājumu riska novērtēšanu ir atbildīga attiecīgā drošības iestāde, kas vajadzības gadījumā konsultējusies ar Valsts drošības iestādēm.

19. Lai noteiktu aizsardzības pasākumus, kādi veicami telpās, kur pastāv pasīvās slepus noklausīšanās risks (piemēram, sienu, durvju, grīdu un griestu izolācija, signālu izstarojuma noteikšana) un aktīvās slepus noklausīšanās risks (piemēram, mikrofonu meklēšana), Padomes Ģenerālsekretariāta Drošības birojs var lūgt palīdzību Valstu drošības iestāžu ekspertiem. ES decentralizēto aģentūru atbildīgie par drošību var lūgt Padomes Ģenerālsekretariāta Drošības biroju veikt tehniskas pārbaudes, vai Valstu drošības iestāžu ekspertu palīdzību.

20. Līdzīgi, ja apstākļi to prasa, Valstu drošības iestāžu tehniskās drošības speciālisti pēc kompetentā atbildīgā par drošību pieprasījuma var pārbaudīt

▼B

jebkāda veida telekomunikācijas iekārtas un elektriskās vai elektroniskās biroja iekārtas, ko izmanto ES slepenā (*SECRET UE*) līmeņa sanāksmēs.

TEHNISKI DROŠAS ZONAS

21. Dažas zonas var izraudzīties kā tehniski drošas zonas. Veic īpašu ieejas pārbaudi. Šādas zonas, kad tās nav aizņemtas, tur noslēgtas ar apstiprinātu metodi, un pret visām atslēgām izturas kā pret drošības atslēgām. Šādas zonas ir pakļautas regulārām fiziskām pārbaudēm, kuras arī veic pēc jebkādas neatļautas iekļūšanas vai aizdomām par šādu iekļūšanu.

22. Veic sīku iekārtu un mēbeļu uzskaiti, lai pārraudzītu to kustību. Nevienu mēbeli vai ierīci neienes šādā zonā, kamēr īpaši apmācīts personāls tai nav veicis rūpīgu pārbaudi, lai atklātu jebkādas noklausīšanās ierīces. Kopumā jāizvairās no sakaru līniju uzstādīšanas tehniski drošās zonās.

▼B

V IEDAĻA

VISPĀRĪGIE VAJADZĪBAS PĒC INFORMĀCIJAS PRINCIPA UN DROŠĪBAS PĀRBAUDES NOTEIKUMI

1. Piekļuve ES klasificētajai informācijai tiks dota tikai personām, kurām ir "vajadzība pēc informācijas" savu pienākumu vai misiju veikšanai. Piekļuvi ES sevišķi slepenajai (*TRÈS SECRET UE/EU TOP SECRET*), ES slepenajai (*SECRET UE*) un ES konfidenciālajai (*CONFIDENTIEL UE*) informācijai dos tikai personām, kurām veikta pienācīga drošības pārbaude.

2. Atbildību par "vajadzības pēc informācijas" noteikšanu uzņemsies Padomes Ģenerālsekretariāts, ES decentralizētās aģentūras un dalībvalstu dienests vai struktūrvienība, kurā tiks nodarbināta attiecīgā persona, saskaņā ar uzdevuma prasībām.

3. Par personāla drošības pārbaudi atbildēs ierēdņa darba devējs, pamatojoties uz attiecīgām piemērojamām procedūrām. Attiecībā uz Padomes Ģenerālsekretariāta ierēdņiem un citiem darbiniekiem, drošības pārbaudes procedūra ir paredzēta VI iedaļā.

   Rezultātā piešķirs "drošības sertifikātu", kurā norādīts klasificētās informācijas līmenis, kādam pārbaudītajai personai dota piekļuve, un izbeigšanās datums.

   Drošības sertifikāts attiecīgajai klasifikācijai var piešķirt tā turētājam piekļuvi informācijai ar zemāku klasifikāciju.

4. Personām, kas nav Padomes Ģenerālsekretariāta vai dalībvalstu darbinieki, piemēram, ES iestāžu locekļiem, ierēdņiem vai darbiniekiem, ar kuriem var būt nepieciešams apspriest vai kuriem var būt nepieciešams rādīt ES klasificēto informāciju, jābūt veiktai drošības pārbaudei attiecībā uz ES klasificēto informāciju, un tām jābūt informētām par viņu atbildību par drošību. Līdzīgos apstākļos tas pats noteikums attiecas uz ārējiem līgumslēdzējiem, ekspertiem vai konsultantiem.

ĪPAŠI NOTEIKUMI PIEKĻUVEI ES SEVIŠĶI SLEPENAJAI (*TRÈS SECRET UE/EU* TOP *SECRET*) INFORMĀCIJAI

5. Visas personas, kurām ir nepieciešama piekļuve ES sevišķi slepenajai (*TRÈS SECRET UE/EU TOP SECRET*) informācijai, pirms piekļuves piešķiršanas jāpārbauda.

6. Visas personas, kurām nepieciešama piekļuve ES sevišķi slepenajai (*TRÈS SECRET UE/EU TOP SECRET*) informācijai, izraugās to struktūrvienības vadītājs, un to vārdus glabā attiecīgā ES sevišķi slepenās (*TRÈS SECRET UE/EU TOP SECRET*) informācijas reģistrā.

7. Pirms tām piešķirta piekļuve ES sevišķi slepenajai (*TRÈS SECRET UE/EU TOP SECRET*) informācijai, visas personas paraksta sertifikātu, apliecinot, ka tās ir iepazīstinātas ar Padomes drošības procedūrām un ka tās pilnībā saprot savu īpašo atbildību attiecībā uz ES sevišķi slepenās (*TRÈS SECRET UE/EU TOP SECRET*) informācijas aizsardzību un sekām, kādas paredzētas ES noteikumos un valstu tiesību aktos, vai administratīvajos noteikumos, ja klasificēta informācija tīši vai netīši nonāk nepiederošu personu rokās.

8. Ja personām ir piekļuve ES sevišķi slepenajai (*TRÈS SECRET UE/EU TOP SECRET*) informācijai sanāksmēs u.c., tā dienesta vai institūcijas, kurā šī persona ir nodarbināta, atbildīgais par kontroli paziņo institūcijai, kura organizē sanāksmi, ka attiecīgajām personām ir šāda atļauja.

9. Visu personu, kuras pārtrauc veikt darba pienākumus, kam nepieciešama piekļuve ES sevišķi slepenajai (*TRÈS SECRET UE/EU TOP SECRET*) informācijai, vārdus izslēdz no ES sevišķi slepenās (*TRÈS SECRET UE/EU TOP SECRET*) informācijas saraksta. Turklāt šādu personu uzmanība vēlreiz jāvērš uz īpašo pienākumu par ES sevišķi slepenās (*TRÈS SECRET UE/EU TOP SECRET*) informācijas aizsardzību. Tās arī paraksta deklarāciju, kurā apņemas nedz izmantot, nedz nodot tālāk to rīcībā esošo ES sevišķi slepeno (*TRÈS SECRET UE/EU TOP SECRET*) informāciju.

▼B

ĪPAŠI NOTEIKUMI PIEKĻUVEI ES SLEPENAJAI (*SECRET UE*) UN ES KONFIDENCIĀLAJAI (*CONFIDENTIEL UE*) INFORMĀCIJAI

10. Visas personas, kurām ir nepieciešama piekļuve ES slepenajai (*SECRET UE*) vai ES konfidenciālajai (*CONFIDENTIEL UE*) informācijai, vispirms jāpārbauda attiecīgajā līmenī.

11. Visas personas, kam nepieciešama piekļuve ES slepenajai (*SECRET UE*) vai ES konfidenciālajai (*CONFIDENTIEL UE*) informācijai, iepazīstina ar attiecīgo drošības reglamentu, un tās apzinās nolaidības sekas.

12. Ja personām ir piekļuve ES slepenajai (*SECRET UE*) vai ES konfidenciālajai (*CONFIDENTIEL UE*) informācijai sanāksmēs u.c., tās institūcijas, kurā šī persona ir nodarbināta, atbildīgais par drošību paziņo institūcijai, kura organizē sanāksmi, ka attiecīgajām personām ir šāda atļauja.

ĪPAŠI NOTEIKUMI PIEKĻUVEI ES IEROBEŽOTAS PIEEJAMĪBAS (RESTREINT UE) INFORMĀCIJAI

13. Personas, kurām ir piekļuve ES ierobežotas pieejamības (*RESTREINT UE*) informācijai, informē par šo drošības reglamentu un nolaidības sekām.

PĀRCELŠANA

14. Ja darbinieku pārceļ no amata, kurš saistīts ar ES klasificētā materiāla apstrādi, kanceleja pārrauga, lai ierēdnis, kas amatu atstāj, pareizi nodod šos materiālus ierēdnim, kas stājas amatā.

ĪPAŠI NORĀDĪJUMI

15. Personas, kurām jāstrādā ar ES klasificēto informāciju, stājoties amatā un turpmāk regulāri jāinformē par:

    a) drošības apdraudējumu, ko izraisa nediskrētas sarunas;

    b) drošības pasākumiem, kas viņiem veicami attiecībās ar presi;

    c) draudiem, ko rada izlūkdienestu darbības, kuru mērķis ir ES un dalībvalstis saistībā ar ES klasificēto informāciju un darbībām;

    d) pienākumu tūlīt ziņot attiecīgām drošības iestādēm par jebkādu mēģinājumu vai manevru, kas izraisa aizdomas par spiegošanas darbībām, vai jebkādiem ārkārtējiem apstākļiem saistībā ar drošību.

16. Visas personas, kas regulāri kontaktējas ar to valstu pārstāvjiem, kuru izlūkdienestu mērķis ir ES un dalībvalstis attiecībā uz ES klasificēto informāciju un darbību, iepazīstina ar metodēm, par kurām zināms, ka tās izmanto dažādi izlūkdienesti.

17. Nepastāv Padomes drošības reglaments attiecībā uz personāla, kas saņēmis piekļuvi ES klasificētajai informācijai, privātu ceļošanu uz jebkādu galamērķi. Kompetentās drošības iestādes tomēr iepazīstinās ierēdņus un citus darbiniekus, kuru atbildības jomā tie ietilpst, ar ceļošanas noteikumiem, kuri varētu attiekties uz viņiem. Atbildīgo par drošību pienākums būs rīkot sanāksmes, lai atgādinātu darbiniekiem par šiem īpašajiem norādījumiem.

▼B

VI IEDAĻA

PADOMES ĢENERĀLSEKRETARIĀTA IERĒDŅU UN PĀRĒJO DARBINIEKU DROŠĪBAS PĀRBAUDES PROCEDŪRA

1. Šāda informācija ir pieejama tikai Padomes Ģenerālsekretariāta ierēdņiem un citiem darbiniekiem, vai personām, kuras strādā Padomes Ģenerālsekretariātā un kurām darba pienākumu dienesta vajadzību dēļ vajag uzzināt vai izmantot Padomes rīcībā esošo klasificēto informāciju.

2. Lai piekļūtu informācijai, kas klasificēta kā "ES sevišķi slepena" (*TRÈS SECRET UE/EU TOP SECRET*), "ES slepena" (*SECRET UE*) un "ES konfidenciāla" (*CONFIDENTIEL UE*), 1. punktā minētajām personām jāsaņem atļauja saskaņā ar 4. un 5. punktā minēto procedūru.

3. Atļauju piešķir tikai tām personām, kurām dalībvalstu kompetentās iestādes (valsts drošības iestādes) ir veikušas drošības pārbaudi saskaņā ar 6. līdz 10. pantā minēto procedūru.

4. Iecēlējinstitūcija Civildienesta noteikumu 2. panta pirmās daļas nozīmē atbild par 1., 2. un 3. punktā minēto atļauju piešķiršanu.

   Iecēlējinstitūcija piešķir atļauju pēc tam, kad tā ieguvusi dalībvalstu kompetento iestāžu atzinumu, pamatojoties uz drošības pārbaudi, kas veikta saskaņā ar 6. līdz 12. pantu.

5. Atļauja, kas ir derīga piecus gadus, nedrīkst pārsniegt to pienākumu termiņu, uz kuru pamata to piešķīra. Iecēlējinstitūcija var atjaunot atļauju saskaņā ar 4. punktā norādīto kārtību.

   Iecēlējinstitūcija atsauc atļauju, ja tai ir pamatoti iemesli šādi rīkoties. Ikvienu lēmumu atsaukt atļauju dara zināmu attiecīgajai personai, kura var lūgt, lai to uzklausa iecēlējinstitūcija, kā arī attiecīgās valsts kompetentajai iestādei.

6. Drošības pārbaudes mērķis ir konstatēt, ka nepastāv šķēršļi atļaut personai piekļūt Padomes rīcībā esošai klasificētai informācijai.

7. Drošības pārbaudi veic tās dalībvalsts kompetentā iestāde, kuras valstspiederība ir personai, uz ko attiecas atļauja, pēc iecēlējinstitūcijas lūguma. Ja attiecīgā persona dzīvo citas dalībvalsts teritorijā, attiecīgās valsts iestādes var nodrošināt sadarbību ar dzīvesvietas dalībvalsts iestādēm.

8. Veicot pārbaudes procedūru, attiecīgajai personai ir jāaizpilda personas informācijas veidlapa.

9. Iecēlējinstitūcija savā pieprasījumā precizē klasificētas informācijas, kas jādara pieejama attiecīgajai personai, veidu un pakāpi, lai attiecīgās valsts kompetentās iestādes varētu veikt pārbaudi un sniegt atzinumu par piešķiramās atļaujas atbilstošu apjomu.

10. Uz visu drošības pārbaudes procedūru kopā ar iegūtajiem rezultātiem attiecas atbilstīgas tiesību normas, kas ir spēkā attiecīgajā dalībvalstī, ieskaitot tiesību normas par pārsūdzēšanu.

11. Ja dalībvalsts kompetentās iestādes sniedz pozitīvu atzinumu, iecēlējinstitūcija var piešķirt attiecīgajai personai atļauju.

12. Attiecīgās valsts kompetento iestāžu negatīvu atzinumu dara zināmu attiecīgajai personai, kura var lūgt, lai viņu uzklausītu iecēlējinstitūcija. Vajadzības gadījumā iecēlējinstitūcija var lūgt attiecīgās valsts kompetentās iestādes sniegt pēc iespējas tuvākus precizējumus. Ja negatīvu atzinumu apstiprina, atļauju nepiešķir.

13. Visas personas, kurām ir piešķirta atļauja 4. un 5. panta nozīmē, atļaujas piešķiršanas laikā un turpmāk regulāri saņem visas vajadzīgās instrukcijas par klasificētas informācijas aizsargāšanu un šādas aizsardzības nodrošināšanas līdzekļiem. Šādas personas paraksta deklarāciju par instrukciju saņemšanu un apņemas tās ievērot.

▼B

14. Iecēlējinstitūcija veic vajadzīgos pasākumus šī lēmuma īstenošanai, jo īpaši attiecībā uz noteikumiem, kas reglamentē piekļuvi atļauju saņēmušo personu sarakstam.

15. Izņēmuma gadījumā, ja to prasa dienesta pienākumi, iecēlējinstitūcija pēc paziņojuma iesniegšanas attiecīgās valsts kompetentajām iestādēm un ar noteikumu, ka mēneša laikā no tām nav saņemta atbilde, piešķir pagaidu atļauju uz laiku, kas nepārsniedz trīs mēnešus, līdz 7. pantā norādītās pārbaudes rezultātu saņemšanai.

16. Šādi piešķirtās pagaidu atļaujas nedod piekļuvi ES sevišķi slepenajai (*TRÈS SECRET UE/EU TOP SECRET*) informācijai; šādu piekļuvi piešķir tikai tiem ierēdņiem, kuriem faktiski ir veikta pārbaude ar pozitīviem rezultātiem saskaņā ar 7. punktu. Līdz pārbaudes iznākumam ierēdņiem, kuriem jāveic pārbaude "ES sevišķi slepenās" (*TRÈS SECRET UE/EU TOP SECRET*) informācijas līmenī, var piešķirt pagaidu atļauju piekļūt informācijai, kas klasificēta līdz "ES slepenās informācijas" (*SECRET UE*) līmenim un ieskaitot to.

▼B

VII IEDAĻA

ES KLASIFICĒTĀ MATERIĀLA SAGATAVOŠANA, IZPLATĪŠANA, PĀRRAIDE, UZGLABĀŠANA UN IZNĪCINĀŠANA

Saturs

Vispārīgi noteikumi	
I nodaļa	ES klasificēto dokumentu sagatavošana un izplatīšana
II nodaļa	ES klasificēto dokumentu nosūtīšana
III nodaļa	Elektroniskie un citi tehniskās pārraides līdzekļi
IV nodaļa	ES klasificēto dokumentu papildu kopijas un tulkojumi, un izraksti no tiem
V nodaļa	ES klasificēto dokumentu apkopošana un pārbaudes, uzglabāšana un iznīcināšana
VI nodaļa	Īpaši noteikumi attiecībā uz Padomei paredzētiem dokumentiem

▼B

Vispārīgi noteikumi

Šajā iedaļā ir sīki izklāstīti pasākumi ES klasificēto dokumentu sagatavošanai, izplatīšanai, pārraidei, uzglabāšanai un iznīcināšanai, kā noteikts šā pielikuma I daļā norādīto Drošības pamatprincipu un minimālo standartu 3. punkta a) apakšpunktā. To izmanto kā atsauci minēto pasākumu pielāgošanai citiem ES klasificētajiem materiāliem pēc to tipa un pamatojoties uz atsevišķiem gadījumiem.

I nodaļa

ES klasificēto dokumentu sagatavošana un izplatīšana

SAGATAVOŠANA

1. ES klasifikācijas un marķējumus izmanto, kā noteikts II iedaļā, un tie jābūt redzamiem katras lappuses augšējā un apakšējā daļā vidū un katra lappuse ir numurēta. Uz katra ES klasificētā dokumenta ir uzskaites numurs un datums. ES sevišķi slepenu (*TRÈS SECRET UE/EU TOP SECRET*) un slepenu (*SECRET UE*) dokumentu gadījumā šis uzskaites numurs ir uz katras lappuses. Ja tie ir jāizplata vairākos eksemplāros, uz katra ir eksemplāra numurs, kurš būs redzams uz pirmās lappuses līdz ar kopējo lappušu skaitu. Visus pielikumus un pievienojumus uzskaita dokumenta, kas klasificēts kā ES konfidenciālais (*CONFIDENTIEL UE*) vai augstāk, pirmajā lappusē.

2. Dokumentus, kas klasificēti kā ES konfidenciālie (*CONFIDENTIEL UE*) un augstāk, drukā, tulko, uzglabā, fotokopē, magnētiski reproducē vai uzņem mikrofilmās tikai personas, kuras pārbaudītas, lai piešķirtu tām piekļuvi ES klasificētajai informācijai vismaz līdz attiecīgā dokumenta pienācīgajai drošības klasifikācijai, izņemot īpašo gadījumu, kas aprakstīts šīs iedaļas 27. punktā.

   Noteikumi, kas regulē klasificētu dokumentu datorizētu sagatavošanu, ir norādīti XI sadaļā.

IZPLATĪŠANA

3. ES klasificēto informāciju izplata tikai personām, kurām ir vajadzība pēc informācijas un kurām veikta attiecīgā drošības pārbaude. Sākotnējo izplatīšanu precizē izcelsmes iestāde.

4. ES sevišķi slepenos (*TRÈS SECRET UE/EU TOP SECRET*) dokumentus izplata caur ES sevišķi slepenajiem (*TRÈS SECRET UE/EU TOP SECRET*) reģistriem (skatīt VIII iedaļu). ES sevišķi slepeno (*TRÈS SECRET UE/EU TOP SECRET*) ziņojumu gadījumā kompetentais reģistrs var atļaut sakaru centra vadītājam sagatavot adresātu sarakstā precizēto eksemplāru skaitu.

5. Dokumentus, kas klasificēti kā ES slepenie (*SECRET UE*), sākotnējais adresāts var atkārtoti izplatīt pārējiem adresātiem, pamatojoties uz vajadzību pēc informācijas. Izcelsmes iestādes tomēr skaidri norāda jebkādus brīdinājumus, ko tās vēlas izteikt. Ja izsaka šādus brīdinājumus, adresāti drīkst dokumentus izplatīt vienīgi ar izcelsmes iestādes atļauju.

6. Jebkuru dokumentu, kas klasificēts kā ES konfidenciālais (*CONFIDENTIEL UE*) un augstāk, ieraksta iestādes reģistrā, kad to saņem šajā iestādē vai kad to izsūta no šīs iestādes. Pēc ierakstāmām ziņām (atsauces, datums un, vajadzības gadījumā, eksemplāra numurs) jāvar identificēt dokumenti un tās ir jāieraksta reģistrācijas žurnālā vai īpaši aizsargāta elektroniskā datu nesējā.

II nodaļa

ES klasificēto dokumentu nosūtīšana

IESAIŅOJUMS

7. Dokumenti, kas klasificēti kā ES konfidenciālie (*CONFIDENTIEL UE*) un augstāk, ir jānosūta izturīgās, necaurredzamās dubultaploksnēs. Iekšējo aploksni marķē ar attiecīgo ES drošības klasifikāciju, kā arī, ja iespējams, uz tās norāda pilnīgas ziņas par saņēmēja amatu un adresi.

▼B

8. Tikai atbildīgais par reģistra kontroli drīkst atvērt iekšējo aploksni un apstiprināt tajā esošo dokumentu saņemšanu, ja vien aploksne nav adresēta konkrētai personai. Šādā gadījumā attiecīgajā reģistrā reģistrē aploksnes saņemšanu, bet iekšējo aploksni drīkst atvērt un tajā esošo dokumentu saņemšanu drīkst apstiprināt tikai persona, kam tā adresēta.

9. Saņemšanas dokuments ir ievietots iekšējā aploksnē. Saņemšanas dokumentā, kurš nebūs klasificēts, jāuzrāda dokumenta atsauces numurs, datums un eksemplāra numurs, bet nekad nenorāda tā priekšmetu.

10. Iekšējā aploksne ir ievietota ārējā aploksnē, uz kuras ir iesaiņojuma numurs saņemšanas formalitāšu veikšanai. Uz ārējās aploksnes nekādā gadījumā nedrīkst norādīt drošības klasifikāciju.

11. Par dokumentiem, kas klasificēti kā ES konfidenciālie (*CONFIDENTIEL UE*) vai augstāk, kurjeri un ziņneši saņem kvītis pēc iesaiņojuma numuriem.

NOSŪTĪŠANA ĒKĀ VAI ĒKU GRUPĀ

12. Attiecīgā ēkā vai ēku grupā klasificētus dokumentus drīkst pārnēsāt aizlīmētā aploksnē, uz kuras ir tikai adresāta vārds, ar noteikumu, ka to nes persona, kurai ir veikta pārbaude attiecībā uz attiecīgo dokumentu klasifikācijas līmeni.

DOKUMENTU NOSŪTĪŠANA VALSTS ROBEŽĀS

13. Valsts robežās ES sevišķi slepenie (*TRÈS SECRET UE/EU TOP SECRET*) dokumenti jānosūta, izmantojot tikai oficiālus kurjera pakalpojumus, vai ar personām, kurām ir atļauja piekļūt ES sevišķi slepenajai (*TRÈS SECRET UE/EU TOP SECRET*) informācijai.

14. Ja ES sevišķi slepena (*TRÈS SECRET UE/EU TOP SECRET*) dokumenta nosūtīšanai ārpus ēkas vai ēku grupas izmanto kurjera pakalpojumus, jāievēro šajā nodaļā ietvertie iesaiņošanas un saņemšanas noteikumi. Piegādes dienestu personāls ļauj nodrošināt to, ka saiņi, kuros ir ES sevišķi slepenie (*TRÈS SECRET UE/EU TOP SECRET*) dokumenti, visu laiku atrodas atbildīgā ierēdņa tiešā uzraudzībā.

15. Izņēmuma kārtā ES sevišķi slepenos (*TRÈS SECRET UE/EU TOP SECRET*) dokumentus ārpus ēkas vai ēku grupas vietējai izmantošanai sanāksmēs un pārrunās drīkst iznest ierēdņi, kas nav kurjeri, ar noteikumu, ka:

   a) nogādātājam ir atļauja piekļuvei attiecīgajiem ES sevišķi slepenajiem (*TRÈS SECRET UE/EU TOP SECRET*) dokumentiem;

   b) pārvietošanas veids atbilst attiecīgās valsts noteikumiem par valsts sevišķi slepeno (*TOP SECRET*) dokumentu nosūtīšanu;

   c) ierēdnis nekādā gadījumā neatstāj ES sevišķi slepenos (*TRÈS SECRET UE/EU TOP SECRET*) dokumentus bez uzraudzības;

   d) nosaka kārtību, kādā veido šādi pārnēsāto dokumentu sarakstu ES sevišķi slepenās informācijas (*TRÈS SECRET UE/EU TOP SECRET*) reģistrā, kurā glabā dokumentus, reģistrē žurnālā, un pārbauda pēc šī ieraksta, kad tos nosūta atpakaļ.

16. Noteiktā valstī ES slepenos (*SECRET UE*) un ES konfidenciālos (*CONFIDENTIEL UE*) dokumentus drīkst nosūtīt vai nu pa pastu, ja šāda nosūtīšana ir atļauta saskaņā ar attiecīgās valsts tiesību aktiem un atbilst šo tiesību aktu noteikumiem, vai, izmantojot kurjera pakalpojumus, vai ar personām, kurām veikta pārbaude pirms piekļuves piešķiršanas ES klasificētajai informācijai.

17. Katrai dalībvalstij vai ES decentralizētajai aģentūrai jāsagatavo norādījumi personālam, kas pārnēsā ES klasificētos dokumentus, pamatojoties uz šiem noteikumiem. Nogādātājam šie norādījumi ir jāizlasa un jāparaksta. Norādījumos jo īpaši jādara zināms, ka dokumentus nekādā gadījumā nedrīkst:

   a) atstāt bez nogādātāja pārziņas, ja vien tie nav drošā uzraudzībā saskaņā ar IV iedaļā ietvertajiem noteikumiem;

   b) atstāt bez uzraudzības sabiedriskajā transportā vai privātos transportlīdzekļos, vai tādās vietās kā restorāni vai viesnīcas. Tos nedrīkst uzglabāt viesnīcu seifos vai atstāt bez uzraudzības viesnīcu istabās;

▼B

c) lasīt tādās vietās kā lidmašīnas vai vilcieni.

NOSŪTĪŠANA NO VIENAS DALĪBVALSTS UZ CITU

18. Materiāli, kas klasificēti kā ES konfidenciālie (*CONFIDENTIEL UE*) un augstāk, jāaizved no vienas dalībvalsts uz citu ar diplomātisko vai militāro kurjeru pakalpojumu palīdzību.

19. Tomēr materiāla, kas klasificēts kā ES slepenais (*SECRET UE*) un ES konfidenciālais (*CONFIDENTIEL UE*), personīgu pārvadāšanu drīkst atļaut, ja pārvadāšanas noteikumi nodrošina, lai tas nevarētu nonākt nepiederošu personu rokās.

20. Valsts drošības iestādes var atļaut personīgu pārvadāšanu, ja nav pieejami diplomātiskie vai militārie kurjeri, vai šādu kurjeru izmantošanas rezultātā notiktu kavēšanās, kas kaitētu ES darbībām, un materiāls ir steidzami vajadzīgs paredzētajam saņēmējam. Katrai dalībvalstij ir jāsagatavo norādījumi, kas attiecas uz materiāla, kas klasificēts līdz ES slepenam (*SECRET UE*), to ieskaitot, personīgu pārvadāšanu starp valstīm, ko veic personas, kuras nav diplomātiskie vai militārie kurjeri. Norādījumos jānosaka, ka:

a) nogādātājam jābūt atbilstošai drošības atļaujai, ko piešķir dalībvalstis;

b) visi šādi pārvadātie materiāli tiek reģistrēti attiecīgā iestādē vai reģistrā;

c) uz iesaiņojumiem vai maisiņiem, kuros atrodas ES materiāls, ir oficiāls zīmogs, lai novērstu muitas pārbaudi, un etiķetes ar identifikāciju un norādījumiem atradējam;

d) nogādātājam ir visu ES valstu atzīta kurjera apliecība un/vai uzdevuma rīkojumu, kas atļauj viņam pārnēsāt saini, kā norādīts;

e) ceļojot pa sauszemi, netiek šķērsota neviena ārpuskopienas valsts vai tās robeža, ja vien nosūtītājai valstij nav īpašas garantijas no attiecīgās valsts;

f) nogādātāja ceļošanas kārtība attiecībā uz galamērķiem, izvēlētajiem maršrutiem un izmantotajiem transporta līdzekļiem ir saskaņā ar ES regulām, vai — ja valsts tiesību akti attiecībā uz šiem jautājumiem ir stingrāki, — saskaņā ar šādiem tiesību aktiem;

g) nogādātājs nedrīkst atstāt materiālu, ja vien tas netiek glabāts saskaņā ar IV iedaļā ietvertajiem drošas uzraudzības noteikumiem;

h) materiālu nedrīkst atstāt bez uzraudzības sabiedriskos vai privātos transportlīdzekļos, vai tādās vietās kā restorāni vai viesnīcas. To nedrīkst uzglabāt viesnīcu seifos vai atstāt bez uzraudzības viesnīcu istabās;

i) ja pārnēsātais materiāls satur dokumentus, tos nedrīkst lasīt publiskās vietās (piemēram, lidmašīnās, vilcienos u.c.).

Personai, kurai uzdots nogādāt klasificēto materiālu, jāizlasa un jāparaksta drošības informācija, kurā kā minimums ir iepriekš uzskaitītie norādījumi un procedūras, kas jāievēro ārkārtējā situācijā vai gadījumā, kad saini, kas satur klasificēto materiālu, gatavojas pārbaudīt muitas vai lidostas drošības amatpersonas.

ES IEROBEŽOTAS PIEEJAMĪBAS (*RESTREINT UE*) DOKUMENTU NOSŪTĪŠANA

21. ES ierobežotas pieejamības (*RESTREINT UE*) dokumentu pārvešanai nav paredzēti īpaši noteikumi, izņemot to, ka ir jānodrošina, lai dokumenti nenonāktu nepiederošas personas rokās.

KURJERU DROŠĪBA

22. Visiem kurjeriem un ziņnešiem, kas nodarbināti ES slepeno (*SECRET UE*) un ES konfidenciālo (*CONFIDENTIEL UE*) dokumentu nogādāšanā, ir veikta pienācīga drošības pārbaude.

▼B

III nodaļa

Elektroniskie un citi tehniskās pārraides līdzekļi

23. Komunikāciju drošības pasākumi ir izveidoti, lai nodrošinātu ES klasificētās informācijas drošu pārraidi. Sīki izstrādāti noteikumi, kas piemērojami šādas ES klasificētās informācijas pārraidei, ir aplūkoti XI iedaļā.

24. Informāciju, kas klasificēta kā ES konfidenciālā (*CONFIDENTIEL UE*) un ES slepenā (*SECRET UE*), drīkst pārraidīt tikai akreditēti sakaru centri un tīkli un/vai termināļi un sistēmas.

IV nodaļa

ES klasificēto dokumentu papildu kopijas, tulkojumi un izraksti no tiem

25. ES sevišķi slepeno (*TRÈS SECRET UE/EU TOP SECRET*) dokumentu kopēšanu vai tulkošanu drīkst atļaut tikai to izcelsmes iestāde.

26. Ja personām, kurām nav atļauja darbam ar ES sevišķi slepeno (*TRÈS SECRET UE/EU TOP SECRET*) informāciju, ir nepieciešama informācija, kura nav klasificēta kā ES sevišķi slepenā (*TRÈS SECRET UE/EU TOP SECRET*), lai gan atrodas šādi klasificētā dokumentā, ES sevišķi slepenās (*TRÈS SECRET UE/EU TOP SECRET*) informācijas reģistra vadītājam var atļaut izsniegt nepieciešamo izrakstu skaitu no attiecīgā dokumenta. Vienlaicīgs viņš veic vajadzīgos pasākumus, lai nodrošinātu, ka šiem izrakstiem piešķir atbilstošo drošības klasifikāciju.

27. Dokumentus, kuri klasificēti kā ES slepenie (*SECRET UE*) un zemāk, drīkst reproducēt un tulkot adresāts saskaņā ar valsts drošības noteikumiem un ar nosacījumu, ka tas stingri atbilst vajadzības pēc informācijas principam. Drošības pasākumi, kas piemērojami oriģināldokumentam, ir piemērojami arī tā reprodukcijām un tulkojumiem. ES decentralizētās aģentūras ievēro šo drošības reglamentu.

V nodaļa

ES klasificēto dokumentu apkopošana un pārbaudes, uzglabāšana un iznīcināšana

APKOPOŠANA UN PĀRBAUDES

28. Katru gadu katrs ES sevišķi slepenās (*TRÈS SECRET UE/EU TOP SECRET*) informācijas reģistrs, kā minēts VIII iedaļā, veic detalizētu ES sevišķi slepeno (*TRÈS SECRET UE/EU TOP SECRET*) dokumentu apkopošanu saskaņā ar VIII iedaļas 9. līdz 11. punktā norādītajiem noteikumiem. ES klasificētajiem dokumentiem, kuru līmenis zemāks nekā ES sevišķi slepenais (*TRÈS SECRET UE/EU TOP SECRET*), piemēro iekšējās pārbaudes saskaņā ar valsts pamatnostādnēm un, Padomes Ģenerālsekretariāta vai ES decentralizēto aģentūru gadījumā, — saskaņā ar ģenerālsekretāra/augstā pārstāvja norādījumiem.

Šīs darbības dod iespēju nodrošināt turētāju viedokli par:

a) iespēju dažus dokumentus ierindot zemākā kategorijā vai deklasificēt;

b) iznīcināmiem dokumentiem.

ES KLASIFICĒTĀS INFORMĀCIJAS UZGLABĀŠANA ARHĪVĀ

29. Lai mazinātu uzglabāšanas problēmas, visu reģistru atbildīgajiem par kontroli tiks dota atļauja uzņemt ES sevišķi slepenos (*TRÈS SECRET UE/EU TOP SECRET*), ES slepenos (*SECRET UE*) un ES konfidenciālos (*CONFIDENTIEL UE*) dokumentus uz mikrofilmām vai citādi uzglabāt magnētiskos vai optiskos datu nesējos arhivēšanai, ar noteikumu, ka:

a) pārfotografēšanu mikrofilmās/uzglabāšanas procesu uzņemas personāls, kam ir atļauja atbilstošajam klasifikācijas līmenim;

b) mikrofilmai/glabāšanas videi ir nodrošināta tāda pati drošība, kā oriģinālajiem dokumentiem;

▼B

c) par jebkura ES sevišķi slepenā (*TRÈS SECRET UE/EU TOP SECRET*) dokumenta fotografēšanu mikrofilmā/uzglabāšanu tiek ziņots izcelsmes iestādei;

d) filmu rullīši vai cita veida nesējs satur vienīgi tādas pašas klasifikācijas — ES sevišķi slepenās (*TRÈS SECRET UE/EU TOP SECRET*), ES slepenās (*SECRET UE*) vai ES konfidenciālās (*CONFIDENTIEL UE*) — dokumentus;

e) ES sevišķi slepenā (*TRÈS SECRET UE/EU TOP SECRET*) vai ES slepenā (*SECRET UE*) dokumenta uzņemšana mikrofilmā/uzglabāšana ir skaidri norādīta reģistrā, ko izmanto ikgadējai inventarizācijai;

f) oriģināldokumentus, kas uzņemti mikrofilmās vai citādi uzglabāti, iznīcina saskaņā ar 31. līdz 36. punktā norādītajiem noteikumiem.

30. Šie noteikumi attiecas arī uz visiem citiem uzglabāšanas veidiem, ko atļauj valsts drošības dienests, piemēram, uz elektromagnētiskiem datu nesējiem un optiskajiem diskiem.

ES KLASIFICĒTO DOKUMENTU KĀRTĒJĀ IZNĪCINĀŠANA

31. Lai novērstu nevajadzīgu ES klasificēto dokumentu uzkrāšanos, dokumentus, kurus glabāšanas iestādes vadītājs uzskata par novecojušiem un liekiem, iespējami ātrāk iznīcina šādā veidā:

a) ES sevišķi slepenos (*TRÈS SECRET UE/EU TOP SECRET*) dokumentus iznīcina tikai centrālais reģistrs, kas par tiem atbild. Katru iznīcināto dokumentu uzskaita iznīcināšanas sertifikātā, kuru paraksta atbildīgais par ES sevišķi slepenās (*TRÈS SECRET UE/EU TOP SECRET*) informācijas kontroli un ierēdnis, kas apliecina iznīcināšanu, kam ir piešķirta ES sevišķi slepenā (*TRÈS SECRET UE/EU TOP SECRET*) līmeņa atļauja. To ieraksta reģistrācijas žurnālā;

b) iznīcināšanas sertifikātus līdz ar izplatīšanas dokumentiem desmit gadus uzglabā reģistrā. Kopijas nosūta izcelsmes iestādei vai attiecīgam centrālajam reģistram tikai pēc skaidra pieprasījuma;

c) ES sevišķi slepenos (*TRÈS SECRET UE/EU TOP SECRET*) dokumentus, tostarp visus klasificētos atkritumus, kas radušies ES sevišķi slepeno (*TRÈS SECRET UE/EU TOP SECRET*) dokumentu sagatavošanas rezultātā, piemēram, bojātus eksemplārus, darba uzmetumus, drukātas piezīmes un koppapīru, iznīcina par ES sevišķi slepeno (*TRÈS* SECRET *UE/EU TOP SECRET*) informāciju atbildīgā ierēdņa uzraudzībā, sadedzinot, sasmalcinot vai citādi pārvēršot neatpazīstamā un neatjaunojamā formā.

32. ES slepenos (*SECRET UE*) dokumentus iznīcina reģistrs, kas atbild par šiem dokumentiem, personas, kurai veikta drošības pārbaude, uzraudzībā, izmantojot vienu no 31. punkta c) apakšpunktā norādītajiem procesiem. ES slepenos (*SECRET UE*) dokumentus, kurus iznīcina, uzskaita parakstītos iznīcināšanas sertifikātos, kas līdz ar izplatīšanas dokumentiem jāsaglabā reģistrā vismaz trīs gadus.

33. ES konfidenciālos (*CONFIDENTIEL UE*) dokumentus iznīcina reģistrs, kas atbild par šiem dokumentiem, personas, kurai veikta drošības pārbaude, uzraudzībā, izmantojot vienu no 31. punkta c) apakšpunktā norādītajiem procesiem. To iznīcināšanu reģistrē saskaņā ar attiecīgās valsts tiesību aktiem un, Padomes Ģenerālsekretariāta vai ES decentralizēto aģentūru gadījumā, saskaņā ar ģenerālsekretāra/augstā pārstāvja norādījumiem.

34. ES ierobežotas pieejamības (*SECRET UE*) dokumentus iznīcina reģistrs, kas atbild par šiem dokumentiem, vai lietotājs saskaņā ar attiecīgās valsts tiesību aktiem un, Padomes Ģenerālsekretariāta vai ES decentralizēto aģentūru gadījumā, saskaņā ar ģenerālsekretāra/augstā pārstāvja norādījumiem.

IZNĪCINĀŠANA ĀRKĀRTĒJĀS SITUĀCIJĀS

35. Padomes Ģenerālsekretariāts un ES decentralizētās aģentūras sagatavo plānus, pamatojoties uz vietējiem nosacījumiem ES klasificētā materiāla aizsardzībai krīzes gadījumā, vajadzības gadījumā ietverot plānus iznīcināšanai vai evakuācijai ārkārtējā situācijā; tie savās attiecīgajās organizācijās

▼B

izsludina norādījumus, ko uzskata par nepieciešamiem, lai novērstu ES klasificētā materiāla nonākšanu nepiederošu personu rokās.

36. ES slepenā (*SECRET UE*) un ES konfidenciālā (*CONFIDENTIEL UE*) materiāla aizsardzības un/vai iznīcināšanas pasākumi nekādā ziņā nedrīkst negatīvi ietekmēt ES sevišķi slepenā (*TRÈS SECRET UE/EU TOP SECRET*) materiāla aizsardzību vai iznīcināšanu, tostarp šifrēšanas aparatūru, kuras apstrāde ir prioritāra, salīdzinot ar visiem citiem uzdevumiem. Pasākumi, kas jāpieņem šifrēšanas iekārtas aizsardzībai un iznīcināšanai ārkārtējā situācijā, ir ietverti *ad hoc* norādījumos.

VI nodaļa

Īpaši noteikumi attiecībā uz Padomei paredzētiem dokumentiem

37. Padomes Ģenerālsekretariātā informāciju, kas klasificēta kā ES slepenā (*SECRET UE*) vai ES konfidenciālā (*CONFIDENTIEL UE*), kura ietverta Padomei paredzētos dokumentos, pārrauga Klasificētās informācijas birojs.

Personāla un administrācijas ģenerāldirektora pakļautībā tas:

a) vada darbības saistībā ar šādas informācijas reģistrāciju, reproducēšanu, tulkošanu, pārraidi, nosūtīšanu un iznīcināšanu;

b) atjaunina ziņas par klasificēto informāciju;

c) periodiski aplūko jautājumus par vajadzību saglabāt informācijas klasifikāciju;

d) sadarbībā ar Drošības biroju nosaka praktisko kārtību informācijas klasifikācijai un deklasifikācijai.

38. Klasificētās informācijas birojs reģistrē šādas ziņas:

a) klasificētās informācijas sagatavošanas datumu;

b) klasifikācijas līmeni;

c) klasifikācijas derīguma termiņu;

d) izdevēja vārdu un struktūrvienību;

e) saņēmēju vai saņēmējus, ar sērijas numuru;

f) priekšmetu;

g) numuru;

h) izplatīto eksemplāru skaitu;

i) Padomei iesniegtās klasificētās informācijas inventāra sarakstu sagatavošanu;

j) sarakstu par klasificētās informācijas deklasificēšanu un ierindošanu zemākā kategorijā.

39. Vispārīgie noteikumi, kas paredzēti šīs iedaļas I līdz V nodaļā, attiecas uz Padomes Ģenerālsekretariāta Klasificētās informācijas biroju, ja vien tos neizmaina ar šajā nodaļā izklāstītiem īpašiem noteikumiem.

▼B

VIII IEDAĻA

ES SEVIŠĶI SLEPENĀS (*TRÈS SECRET UE/EU TOP SECRET*) INFORMĀCIJAS REĢISTRI

1. ES sevišķi slepenās (*TRÈS SECRET UE/EU TOP SECRET*) informācijas reģistru mērķis ir nodrošināt ES sevišķi slepeno (*TRÈS SECRET UE/EU TOP SECRET*) dokumentu apstrādi un izplatīšanu saskaņā ar drošības reglamentu. Atbildīgais par ES sevišķi slepenās (*TRÈS SECRET UE/EU TOP SECRET*) informācijas kontroli ir ES sevišķi slepenās (*TRÈS SECRET UE/EU TOP SECRET*) informācijas reģistra vadītājs attiecīgi katrā dalībvalstī, Padomes Ģenerālsekretariātā un, vajadzības gadījumā, ES decentralizētajās aģentūrās.

2. Centrālie reģistri darbojas kā galvenā saņēmēja un nosūtītāja iestāde dalībvalstīs, Padomes Ģenerālsekretariātā un ES decentralizētajās aģentūrās, kur šādi reģistri ir izveidoti, kā arī, vajadzības gadījumā, citās ES iestādēs, starptautiskās organizācijās un trešās valstīs, ar kurām Padomei ir nolīgumi par klasificētās informācijas apmaiņas drošības procedūrām.

3. Vajadzības gadījumā izveido apakšreģistrus, kas atbildētu par ES sevišķi slepeno (*TRÈS SECRET UE/EU TOP SECRET*) dokumentu iekšējo lietvedību; tajos izdara jaunākos ierakstus par katra apakšreģistra pārziņā esoša dokumenta apriti.

4. ES sevišķi slepenās (*TRÈS SECRET UE/EU TOP SECRET*) informācijas apakšreģistrus izveido, kā precizēts I iedaļā, atsaucoties uz vajadzībām ilgākā laika posmā, un pievieno centrālam ES sevišķi slepenās (*TRÈS SECRET UE/EU TOP SECRET*) informācijas reģistram. Ja ir nepieciešamība ielūkoties ES sevišķi slepenajos (*TRÈS SECRET UE/EU TOP SECRET*) dokumentos tikai uz laiku un neregulāri, šos dokumentus drīkst izsniegt, neizveidojot ES sevišķi slepenās (*TRÈS SECRET UE/EU TOP SECRET*) informācijas apakšreģistru, ja ir paredzēti noteikumi, lai nodrošinātu, ka tie paliek attiecīga ES sevišķi slepenās (*TRÈS SECRET UE/EU TOP SECRET*) informācijas reģistra kontrolē un ka tiek ievēroti visi fiziskās un personāla drošības pasākumi.

5. Apakšreģistri nedrīkst pārsūtīt ES sevišķi slepenos (*TRÈS SECRET UE/EU TOP SECRET*) dokumentus tieši citiem tā paša ES sevišķi slepenās (*TRÈS SECRET UE/EU TOP SECRET*) informācijas reģistra apakšreģistriem bez skaidras šā reģistra piekrišanas.

6. Visus ES sevišķi slepeno (*TRÈS SECRET UE/EU TOP SECRET*) dokumentu apmaiņas gadījumus starp apakšreģistriem, kas nav pakļauti tam pašam centrālajam reģistram, novada caur centrālajiem ES sevišķi slepenās (*TRÈS SECRET UE/EU TOP SECRET*) informācijas reģistriem.

CENTRĀLIE ES SEVIŠĶI SLEPENĀS (TRÈS SECRET UE/EU TOP SECRET) INFORMĀCIJAS REĢISTRI

7. Kā atbildīgais par kontroli, centrālā ES sevišķi slepenās (*TRÈS SECRET UE/EU TOP SECRET*) informācijas reģistra vadītājs atbild par:

   a) ES sevišķi slepeno (*TRÈS SECRET UE/EU TOP SECRET*) dokumentu nosūtīšanu saskaņā ar VII iedaļā noteiktajiem noteikumiem,

   b) visu tam pakļauto ES sevišķi slepenās (*TRÈS SECRET UE/EU TOP SECRET*) informācijas apakšreģistru saraksta veidošanu ar iecelto atbildīgo par drošību un to pilnvaroto vietnieku vārdiem un parakstiem,

   c) no reģistriem saņemto saņemšanas dokumentu turēšanu par visiem centrālā reģistra izplatītajiem ES sevišķi slepenajiem (*TRÈS SECRET UE/EU TOP SECRET*) dokumentiem,

   d) glabāto un izplatīto ES sevišķi slepeno (*TRÈS SECRET UE/EU TOP SECRET*) dokumentu reģistrēšanu,

   e) visu centrālo ES sevišķi slepenās (*TRÈS SECRET UE/EU TOP SECRET*) informācijas reģistru, ar kuriem viņš parasti sarakstās, atjaunināta saraksta veidošanu, ieskaitot par drošību atbildīgo ierēdni un to pilnvaroto vietnieku vārdus, uzvārdus un parakstus,

▼B

f) visu ES sevišķi slepeno (*TRÈS SECRET UE/EU TOP SECRET*) dokumentu, kas atrodas reģistrā, fizisko aizsardzību saskaņā ar IV iedaļā ietvertajiem noteikumiem.

ES SEVIŠĶI SLEPENĀS (*TRÈS SECRET UE/EU TOP SECRET*) INFORMĀCIJAS APAKŠREĢISTRI

8. Kā atbildīgais par kontroli, ES sevišķi slepenās (*TRÈS SECRET UE/EU TOP SECRET*) informācijas apakšreģistra vadītājs atbild par:

a) ES sevišķi slepeno (*TRÈS SECRET UE/EU TOP SECRET*) dokumentu nosūtīšanu saskaņā ar VII iedaļā un VIII iedaļas 5. un 6. punktā ietvertajiem noteikumiem;

b) visu personu, kam ir ļauta piekļuve viņa kontrolē esošajai ES sevišķi slepenās (*TRÈS SECRET UE/EU TOP SECRET*) informācijai, atjaunināta saraksta veidošanu;

c) ES sevišķi slepeno (*TRÈS SECRET UE/EU TOP SECRET*) dokumentu izplatīšanu saskaņā ar izplatīšanas iestādes norādījumiem, vai pamatojoties uz vajadzību pēc informācijas, iepriekš pārliecinoties, vai adresātam ir veikta attiecīgā drošības pārbaude;

d) visu ES sevišķi slepeno (*TRÈS SECRET UE/EU TOP SECRET*) dokumentu, ko glabā vai izplata viņa kontrolē, vai kas tikuši nodoti citiem ES sevišķi slepenās (*TRÈS SECRET UE/EU TOP SECRET*) informācijas reģistriem, atjaunināta reģistra veidošanu un visu atbilstošo saņemšanas dokumentu glabāšanu;

e) atjaunināta ES sevišķi slepenās (*TRÈS SECRET UE/EU TOP SECRET*) informācijas reģistru, ar kuriem viņam atļauts apmainīties ar ES sevišķi slepenajiem (*TRÈS SECRET UE/EU TOP SECRET*) dokumentiem, saraksta veidošanu, ieskaitot par kontroli atbildīgo ierēdņu un viņu vietnieku vārdiem, uzvārdiem un parakstiem;

f) visu ES sevišķi slepeno (*TRÈS SECRET UE/EU TOP SECRET*) dokumentu, kas atrodas apakšreģistrā, fizisko aizsardzību saskaņā ar IV iedaļā ietvertajiem noteikumiem.

INVENTARIZĀCIJAS

9. Reizi divpadsmit mēnešos katrs ES sevišķi slepenās (*TRÈS SECRET UE/EU TOP SECRET*) informācijas reģistrs veic detalizētu ES sevišķi slepeno (*TRÈS SECRET UE/EU TOP SECRET*) dokumentu inventarizāciju, par kuriem tas atbild. Dokumentu uzskata par uzskaitītu, ja reģistrs šo dokumentu fiziski apskata vai pārbauda, vai tā rīcībā ir saņemšanas dokuments no ES sevišķi slepenās (*TRÈS SECRET UE/EU TOP SECRET*) informācijas reģistra, no kura tas ir pārvests, dokumenta iznīcināšanas sertifikāts vai norādījums ierindot dokumentu zemākā kategorijā vai deklasificēt.

10. Apakšreģistri nosūta savu ikgadējo inventarizāciju rezultātus centrālajam reģistram, kuram tie pakļauti, dienā, kuru tas nosaka.

11. Valsts drošības iestādes, kā arī tās ES iestādes, starptautiskās organizācijas un ES decentralizētās aģentūras, kurās izveidots centrālais ES sevišķi slepenās (*TRÈS SECRET UE/EU TOP SECRET*) informācijas reģistrs, nosūta centrālajos ES sevišķi slepenās (*TRÈS SECRET UE/EU TOP SECRET*) informācijas reģistros veikto inventarizāciju rezultātus ģenerālsekretāram/augstajam pārstāvim vēlākais līdz katra gada 1. aprīlim.

▼B

IX IEDAĻA

DROŠĪBAS PASĀKUMI, KAS PIEMĒROJAMI ĪPAŠU SANĀKSMJU LAIKĀ, KO RĪKO ĀRPUS PADOMES TELPĀM UN KUR IZSKATA KONFIDENCIĀLUS JAUTĀJUMUS

VISPĀRĪGI NOTEIKUMI

1. Ja ārpus Padomes telpām Briselē un Luksemburgā notiek Eiropadomes, Padomes, ministru vai citas svarīgas sanāksmes un ja īpašās drošības prasības saistībā ar aplūkoto jautājumu vai informācijas augsto konfidencialitāti to pamato, jāveic tālāk aprakstītie drošības pasākumi. Šie pasākumi attiecas tikai uz ES klasificētās informācijas aizsardzību; var būt nepieciešams ieplānot citus drošības pasākumus.

PIENĀKUMI

Uzņēmējas dalībvalstis

2. Dalībvalstij, kuras teritorijā notiek sanāksme (uzņēmējai dalībvalstij), sadarbībā ar Padomes Ģenerālsekretariātu jāuzņemas atbildība par Eiropadomes, Padomes, ministru vai citām svarīgām sanāksmēm un par galveno delegātu un darbinieku fizisko drošību.

Attiecībā uz drošības aizsardzību tai īpaši jānodrošina, ka:

a) tiek sastādīti plāni, lai risinātu draudus drošībai un ar drošību saistītus starpgadījumus, attiecīgos pasākumus attiecinot jo īpaši uz ES klasificēto dokumentu glabāšanu seifā birojos;

b) tiek veikti pasākumi, lai nodrošinātu iespējamu piekļuvi Padomes komunikācijas sistēmai, lai saņemtu un nosūtītu ES klasificētos ziņojumus. Uzņēmēja dalībvalsts vajadzības gadījumā arī nodrošinās piekļuvi drošai tālruņu sistēmai.

Dalībvalstis

3. Dalībvalstu iestādēm jāveic vajadzīgie pasākumi, lai nodrošinātu, ka:

a) tiek sniegts atbilstošs drošības pārbaudes apstiprinājums to delegātiem, ja vajadzīgs, ziņojuma vai faksa veidā tieši atbildīgajam par sanāksmes drošību vai ar Padomes Ģenerālsekretariāta Drošības biroja starpniecību;

b) uzņēmējas dalībvalsts iestādes un, vajadzības gadījumā, Padomes Ģenerālsekretariāta Drošības birojs, tiek informēts par jebkādu īpašu apdraudējumu, lai varētu attiecīgi rīkoties.

Atbildīgais par sanāksmes drošību

4. Jāieceļ atbildīgais par drošību, kura pienākums ir vispārēju iekšējo drošības pasākumu vispārējā sagatavošana un kontrole, kā arī saskaņošana ar citām attiecīgām drošības iestādēm. Viņa veiktajiem pasākumiem galvenokārt jāattiecas uz:

a) i) drošības pasākumiem sanāksmes vietā, lai nodrošinātu, ka sanāksme notiek bez jebkādiem starpgadījumiem, kas varētu apdraudēt visas tajā izmantotās ES klasificētās informācijas drošību;

ii) personāla, kuram ir atļauta piekļuve sanāksmes vietai, zonām, kur atrodas delegācijas, un konferenču telpām, pārbaudi un visu iekārtu pārbaudi;

iii) pastāvīgu koordināciju ar uzņēmējas dalībvalsts kompetentajām iestādēm un ar Padomes Ģenerālsekretariātu;

b) drošības instrukciju iekļaušanu sanāksmes dokumentācijā, pienācīgi ievērojot šajā drošības reglamentā norādītās prasības, un visu citu drošības norādījumu, ko uzskata par nepieciešamiem, iekļaušanu.

Padomes Ģenerālsekretariāta Drošības birojs

5. Padomes Ģenerālsekretariāta Drošības birojam jādarbojas kā padomdevējam par drošību sanāksmes sagatavošanā; tam jābūt pārstāvētam sanāksmē, lai

▼B

vajadzības gadījumā palīdzētu un dotu padomus atbildīgajam par sanāksmes drošību un delegācijām.

6. Katrai delegācijai, kas piedalās sanāksmē, jāieceļ atbildīgais par drošību, kurš atbildēs par drošības jautājumiem savā delegācijā un par sadarbību ar atbildīgo par sanāksmes drošību, kā arī, vajadzības gadījumā — ar Padomes Ģenerālsekretariāta Drošības biroja pārstāvi.

DROŠĪBAS PASĀKUMI

Drošības zonas

7. Jāizveido šādas drošības zonas:

   a) II kategorijas drošības zona, kuru veido redakcijas telpa, Padomes Ģenerālsekretariāta biroji un reprogrāfijas iekārtas, kā arī, vajadzības gadījumā — delegāciju biroji;

   b) I kategorijas drošības zona, kuru veido konferenču telpa un tulku un skaņu inženieru kabīnes;

   c) administratīvās zonas, kuras veido preses zona un tās sanāksmes vietas daļas, kuras izmanto administrācijai, ēdināšanai un izmitināšanai, kā arī zona, kas atrodas tieši blakus preses centram un sanāksmes vietai.

Caurlaides

8. Atbildīgajam par sanāksmes drošību pēc delegāciju pieprasījuma jāizdod atbilstoši žetoni saskaņā ar to vajadzībām. Vajadzības gadījumā var nodalīt piekļuvi dažādām drošības zonām.

9. Sanāksmes drošības instrukcijās jāparedz, ka visām attiecīgajām personām sanāksmes vietā žetoni visu laiku jānēsā tā, lai tie būtu labi redzami un drošības darbinieki varētu tos pēc vajadzības pārbaudīt.

10. Sanāksmes vietā bez dalībniekiem, kas nēsā žetonus, būtu jāielaiž iespējami mazāk cilvēku. Valstu delegācijām, kuras sanāksmes laikā vēlas pieņemt apmeklētājus, par to jāpaziņo atbildīgajam par sanāksmes drošību. Apmeklētājiem jāpiešķir apmeklētāja žetons. Jāaizpilda apmeklētāja caurlaides veidlapa, kurā ieraksta viņa vārdu un uzvārdu un apmeklējamās personas vārdu un uzvārdu. Apmeklētājiem vienmēr jābūt kopā ar apsardzi vai apmeklējamo personu. Apmeklētāja caurlaides veidlapa ir jānes pavadošajai personai, kura to līdz ar apmeklētāja žetonu nogādā atpakaļ drošības darbiniekiem, kad apmeklētājs atstāj sanāksmes vietu.

Foto un audio iekārtu kontrole

11. I kategorijas drošības zonā nedrīkst ienest fotoaparātus vai ieraksta aparatūru, izņemot fotogrāfu un skaņu inženieru ienestās ierīces, kam atbilstošu atļauju devis atbildīgais par sanāksmes drošību.

Portfeļu, pārnēsājamo datoru un saiņu pārbaude

12. Caurlaižu turētāji, kuriem ir dota piekļuve drošības zonai, parasti bez pārbaudes veikšanas drīkst ienest portfeļus un pārnēsājamos datorus (tikai ar savu barošanas avotu). Delegācijas drīkst pieņemt saiņus, kurus vai nu pārbaudīs delegācijas atbildīgais par drošību, vai arī caurlūkos ar īpašu aparatūru, vai pārbaudes nolūkos atvērs drošības darbinieki. Ja atbildīgais par sanāksmes drošību uzskata to par nepieciešamu, var noteikt stingrākus pasākumus portfeļu un saiņu pārbaudei.

Tehniskā drošība

13. Sanāksmes telpu tehniski nodrošināt var tehniskās drošības komanda, kura sanāksmes laikā arī veic elektronisko uzraudzību.

Delegāciju dokumenti

14. Delegācijām jāatbild par ES klasificēto dokumentu nogādāšanu uz sanāksmēm un no tām. Tām arī jāatbild par šo dokumentu pārbaudi un drošību to izmantošanas laikā delegācijām piešķirtajās telpās. Var lūgt uzņēmējas dalībvalsts palīdzību klasificēto dokumentu transportēšanā uz sanāksmes vietu un no tās.

▼B

Dokumentu droša glabāšana

15. Ja Padomes Ģenerālsekretariāts, Komisija vai delegācijas nespēj glabāt savus klasificētos dokumentus saskaņā ar apstiprinātiem standartiem, tās var noglabāt šos dokumentus aizlīmētā aploksnē pie atbildīgā par sanāksmes drošību, pretī saņemot kvīti, lai pēdējais varētu dokumentus glabāt saskaņā ar apstiprinātiem standartiem.

Biroju pārbaude

16. Atbildīgajam par sanāksmes drošību jāorganizē Padomes Ģenerālsekretariāta un delegāciju biroju pārbaude katras darba dienas beigās, lai nodrošinātu, ka visi ES klasificētie dokumenti tiek glabāti drošā vietā; ja tā nav, viņam jāveic attiecīgi pasākumi.

ES klasificēto atkritumu iznīcināšana

17. Pret visiem atkritumiem jāizturas kā pret ES klasificētiem atkritumiem un Padomes Ģenerālsekretariātam un delegācijām jānodod papīrgrozi un maisiņi, kur tos izmest. Pirms tiem piešķirto telpu atstāšanas Padomes Ģenerālsekretariātam un delegācijām jānodod atkritumi atbildīgajam par sanāksmes drošību, kurš organizē to iznīcināšanu saskaņā ar reglamentu.

18. Sanāksmes beigās visi dokumenti, kas atrodas Padomes Ģenerālsekretariāta vai delegāciju rīcībā, bet kuri tiem nav vajadzīgi, jāuzskata par atkritumiem. Pirms sanāksmei pieņemto drošības pasākumu atcelšanas rūpīgi jāpārmeklē Padomes Ģenerālsekretariāta un delegāciju telpas. Dokumenti, par kuriem parakstīts saņemšanas dokuments, pēc iespējas jāiznīcina, kā noteikts VII iedaļā.

▼B

X IEDAĻA

DROŠĪBAS PĀRKĀPUMI UN ES KLASIFICĒTĀS INFORMĀCIJAS APDRAUDĒJUMS

1. Drošības pārkāpums notiek darbības vai bezdarbības rezultātā, kas ir pretrunā Padomes vai valsts drošības reglamentam un kas var apdraudēt vai negatīvi ietekmēt ES klasificēto informāciju.

2. ES klasificētās informācijas apdraudējums notiek, ja tā ir pilnībā vai daļēji nonākusi nepiederošu personu rokās, proti, tādu, kurām nav veikta atbilstoša drošības pārbaude vai kurām nav nepieciešamība pēc informācijas, vai, ja pastāv iespēja, ka šāds gadījums ir noticis.

3. ES klasificēto informāciju var apdraudēt bezrūpība, nolaidība vai neapdomība, kā arī tādu dienestu darbība, kuru mērķis ir ES vai tās dalībvalstis attiecībā uz ES klasificēto informāciju, vai arī graujošu organizāciju darbības.

4. Svarīgi, lai personas, kurām jāstrādā ar ES klasificēto informāciju, būtu pamatīgi iepazīstinātas ar drošības procedūrām, briesmām, kas saistītas ar neapdomīgām sarunām un attiecībām ar presi. Tām jāapzinās, cik svarīgi ir nekavējoties ziņot par jebkuru pamanīto drošības pārkāpumu dalībvalsts, iestādes vai aģentūras, kurā tās strādā, drošības iestādei.

5. Ja drošības iestāde atklāj vai ir informēta par drošības pārkāpumu attiecībā uz ES klasificēto informāciju vai ES klasificētā materiāla nozaudēšanu vai pazušanu, tā savlaicīgi rīkojas, lai:

   a) konstatētu faktus;

   b) izvērtētu un mazinātu nodarīto kaitējumu;

   c) novērstu tā atkārtošanos;

   d) informētu attiecīgās iestādes par drošības pārkāpuma sekām.

   Šajā sakarā norāda šādu informāciju:

   i) iesaistītās informācijas aprakstu, tostarp tās klasifikāciju, atsauces un eksemplāra numuru, datumu, izcelsmes iestādi, priekšmetu un jomu;

   ii) drošības pārkāpuma apstākļu īsu aprakstu, tostarp dienu un laika posmu, kurā informācija bija pakļauta apdraudējumam;

   iii) paziņojumu par to, vai ir informēta izcelsmes iestāde.

6. Katras drošības iestādes pienākums ir, tiklīdz tā saņēmusi paziņojumu par šādu iespējamu drošības pārkāpumu, ziņot par šo faktu, izmantojot šādu procedūru: ES sevišķi slepenās (*EU TOP SECRET*) informācijas apakšreģistrs ziņo Padomes Ģenerālsekretariāta Drošības birojam caur savu centrālo ES sevišķi slepenās (*EU TOP SECRET*) informācijas reģistru; ja ES klasificētās informācijas apdraudējums noticis dalībvalsts jurisdikcijā, par to ziņo Padomes Ģenerālsekretariāta Drošības birojam, kā precizēts 5. punktā, caur atbildīgo valsts drošības iestādi.

7. Par gadījumiem, kuros iesaistīta ES ierobežotas pieejamības (*RESTREINT UE*) informācija, jāziņo tikai tad, ja tajos vērojamas neparastas iezīmes.

8. Saņemot informāciju par notikušu drošības pārkāpumu, ģenerālsekretārs/augstais pārstāvis:

   a) paziņo par to iestādei, kas sastādījusi attiecīgo klasificēto informāciju;

   b) lūdz attiecīgām drošības iestādēm uzsākt izmeklēšanu;

   c) koordinēt izmeklēšanu, ja tiek skarta vairāk nekā viena drošības iestāde;

   d) iegūt ziņojumu par pārkāpuma apstākļiem, dienu un laika posmu, kurā tas varētu būt noticis un ir ticis atklāts, līdz ar sīku iesaistītā materiāla satura un klasifikācijas aprakstu. Jāziņo arī par kaitējumu, kas nodarīts ES vai vienas vai vairāku tās dalībvalstu interesēm, un pasākumiem, kas veikti, lai novērstu tā atkārtošanos.

▼B

9. Izcelsmes iestāde informē visus adresātus un dod atbilstošus norādījumus.

10. Visām personām, kuras ir atbildīgas par ES klasificētās informācijas apdraudējumu, piemēro disciplināru atbildību saskaņā ar attiecīgiem noteikumiem. Šāda atbildība neierobežo jebkādu tiesisku darbību.

▼B

XI IEDAĻA

INFORMĀCIJAS AIZSARDZĪBA INFORMĀCIJAS TEHNOLOĢIJU UN KOMUNIKĀCIJAS SISTĒMĀS

Saturs

I nodaļa	Ievads
II nodaļa	Definīcijas
III nodaļa	Pienākumi saistībā ar drošību
IV nodaļa	Netehniskie drošības pasākumi
V nodaļa	Tehniskie drošības pasākumi
VI nodaļa	Drošība apstrādes laikā
VII nodaļa	Publiskais iepirkums
VIII nodaļa	Pagaidu vai neregulāra lietošana

▼B

I nodaļa

Ievads

VISPĀRĒJIE ASPEKTI

1. Šajā iedaļā ietvertā drošības politika un prasības attiecas uz visām komunikāciju un informācijas sistēmām un tīkliem (še turpmāk "SISTĒMAS"), kurās apstrādā informāciju, kas klasificēta kā ES konfidenciālā (*CONFIDENTIEL UE*) un augstāk.

2. SISTĒMĀM, kurās apstrādā ierobežotas pieejamības (*RESTREINT UE*) informāciju, arī ir nepieciešami drošības pasākumi, lai aizsargātu šīs informācijas konfidencialitāti. Visām SISTĒMĀM ir nepieciešami drošības pasākumi, lai aizsargātu šo sistēmu un tajās esošās informācijas integritāti un pieejamību. Drošības pasākumus, kas piemērojami šīm sistēmām, noteiks nozīmēta drošības akreditācijas iestāde (SAA) atbilstoši novērtētajam riskam un politikai, kas minēta šajā drošības reglamentā.

3. Sensoru sistēmu, kurās ir ietvertas IT sistēmas, aizsardzību nosaka un precizē vispārējā sakarā ar sistēmām, kurām tās pieder, iespējami izmantojot attiecīgus šīs iedaļas noteikumus.

SISTĒMU APDRAUDĒJUMS UN IEVAINOJAMĪBA

4. Apdraudējumu vispārīgi var definēt kā iespēju, ka nejauši vai tīši notiek negatīva ietekme uz drošību. SISTĒMU gadījumā šāda negatīva ietekme ietver vienas vai vairāku konfidencialitātes, integritātes un pieejamības iezīmju zaudēšanu. Ievainojamību var definēt kā kontroles vājumu vai trūkumu, kas atvieglotu vai pieļautu apdraudējuma īstenošanu pret noteiktu lietu vai mērķi. Ievainojamību var izraisīt nolaidība, vai arī tā var būt saistīta ar kontroles stingrības, pilnības vai konsekvences trūkumu; tā var būt tehniska, procesuāla vai operatīva.

5. ES klasificētā un neklasificētā informācija, ko apstrādā SISTĒMĀS koncentrētā veidā un kas paredzēta ātrai iegūšanai, komunicēšanai un lietošanai, ir pakļauta daudziem riskiem. To vidū ir nesankcionētu lietotāju piekļuve informācijai, vai, pretēji — piekļuves atteikums pilnvarotiem lietotājiem. Pastāv arī informācijas neatļautas izpaušanas, sabojāšanas, izmainīšanas vai izdzēšanas risks. Turklāt sarežģītā un dažkārt jutīgā aparatūra ir dārga, un to bieži ir grūti ātri salabot vai aizstāt. Tādēļ šīs SISTĒMAS ir izdevīgi mērķi informācijas vākšanas operācijām un sabotāžai, īpaši ja drošības pasākumus uzskata par neefektīviem.

DROŠĪBAS PASĀKUMI

6. Galvenais šajā iedaļā noteikto drošības pasākumu mērķis ir nodrošināt aizsardzību pret neatļautu informācijas izpaušanu (konfidencialitātes zaudēšanu) un pret informācijas integritātes un pieejamības zaudēšanu. Lai panāktu pietiekamu SISTĒMAS, kurā apstrādā ES klasificēto informāciju, aizsardzību, precizē attiecīgus parastās drošības standartus līdz ar īpašām drošības procedūrām un metodēm, kas īpaši izstrādātas katrai SISTĒMAI.

7. Identificē un īsteno līdzsvarotu drošības pasākumu kopumu, lai radītu drošu vidi, kurā darboties SISTĒMAI. Šo pasākumu piemērošanas jomas attiecas uz fiziskiem elementiem, personālu, netehniskām procedūrām, datoriem un komunikāciju darbību.

8. Ir vajadzīgi datoru drošības pasākumi (aparatūras un programmatūras drošības elementiem), lai īstenotu principu par vajadzības pēc informācijas un novērstu vai atklātu informācijas neatļauta izpaušanu. To, ciktāl izmantojami datoru drošības pasākumi, nosaka drošības prasību izstrādes procesā. Akreditācijas procesā konstatē, ka nodrošinājuma līmenis ir pietiekams, lai atbalstītu šo datoru drošības pasākumu izmantošanu.

SISTĒMAI RAKSTURĪGU DROŠĪBAS PRASĪBU PAZIŅOJUMS (*SSRS*)

9. Par visām SISTĒMĀM, kurās apstrādā informāciju, kas klasificēta kā ES konfidenciālā (*CONFIDENTIEL UE*) un augstāk, IT sistēmu darbības iestādei (*ITSOA*) ir jāsniedz SISTĒMAI raksturīgu drošības prasību paziņojums (*SSRS*) ar nepieciešamo projekta personāla un *INFOSEC* iestādes palī-

▼B

dzību, ko apstiprinājusi drošības akreditācijas iestāde. SSRS ir nepieciešams arī tad, ja drošības akreditācijas iestāde uzskata par svarīgu ierobežotas pieejamības (*RESTREINT UE*) vai neklasificētas informācijas pieejamību un integritāti.

10. *SSRS* formulē projekta uzsākšanas visagrākajā posmā un attīsta un pastiprina, projektam attīstoties, dažādos projekta un SISTĒMAS aprites cikla posmos izpildot dažādus uzdevumus.

11. *SSRS* veido saistošu nolīgumu starp IT sistēmu darbības iestādi un Drošības akreditācijas iestādi, saskaņā ar ko SISTĒMA ir akreditējama.

12. *SSRS* ir pilnīgs un skaidrs vērā ņemamo drošības principu un izpildāmo sīki izstrādāto drošības prasību pārskats. Tā pamatā ir Padomes drošības politika un riska novērtējums, vai arī to īsteno pēc parametriem, kas attiecas uz ekspluatācijas vidi, zemāko personāla drošības pārbaudes līmeni, augstāko apstrādātās informācijas klasifikāciju, drošības darbības režīmu vai prasībām lietotājiem. *SSRS* ir projekta dokumentācijas, ko iesniedz attiecīgām iestādēm tehniskas, budžeta un drošības apstiprināšanas nolūkā, sastāvdaļa. Galīgajā formā *SSRS* sastāv no pilnīga pārskata pār to, ko nozīmē droša SISTĒMA.

DROŠĪBAS REŽĪMI

13. Visas SISTĒMAS, kurās apstrādā informāciju, kas klasificēta kā ES konfidenciālā (*CONFIDENTIEL UE*) un augstāk, ir akreditētas, lai darbotos vienā, vai, ja tā pamatā ir prasības dažādos laika posmos, — vairāk nekā vienā no šiem drošības darbības režīmiem, vai līdzvērtīgā attiecīgās valsts režīmā:

    a) speciālas drošības darbības režīmā;

    b) augstas sistēmas drošības darbības režīmā un

    c) daudzlīmeņu drošības darbības režīmā.

II nodaļa

Definīcijas

PAPILDU MARĶĒJUMI

14. Papildu marķējumus, kā, piemēram, CRYPTO, vai jebkādu citu ES atzītu īpašas apstrādes apzīmētāju izmanto, ja ir vajadzība pēc ierobežotas izplatīšanas un īpašas apstrādes papildus tai, kas norādīta drošības klasifikācijā.

15. SPECIĀLAS DROŠĪBAS DARBĪBAS REŽĪMS ir: darbības režīms, kurā VISIEM indivīdiem, kam ir piekļuve SISTĒMAI, ir veikta drošības pārbaude, lai dotu piekļuvi visaugstākajam SISTĒMĀ apstrādātās informācijas līmenim, un ar vispārēju vajadzību pēc VISAS SISTĒMĀ apstrādātās informācijas.

    Piezīmes:

    1) Vispārējā vajadzība pēc informācijas norāda, ka nepastāv obligāta prasība, lai datoru drošības elementi nodrošinātu informācijas dalīšanu SISTĒMĀ.

    2) Pārējie drošības elementi (piemēram, fiziskie, personāla un procesuālie) atbilst prasībām visaugstākajam klasifikācijas līmenim un visiem SISTĒMĀ apstrādātās informācijas apzīmējumiem.

16. AUGSTAS SISTĒMAS DROŠĪBAS DARBĪBAS REŽĪMS ir: darbības režīms, kurā VISIEM indivīdiem, kam ir piekļuve SISTĒMAI, ir veikta drošības pārbaude, lai dotu piekļuvi visaugstākajam SISTĒMĀ apstrādātās informācijas līmenim, bet NE VISIEM indivīdiem, kam ir piekļuve SISTĒMAI, ir vispārēja vajadzība pēc SISTĒMĀ apstrādātās informācijas.

    Piezīmes:

    1) Vispārējās vajadzības pēc informācijas trūkums norāda, ka pastāv prasība, lai datoru drošības elementi nodrošinātu selektīvu piekļuvi informācijai un informācijas dalīšanu SISTĒMĀ.

▼B

2) Pārējie drošības elementi (piemēram, fiziskie, personāla un procesuālie) atbilst visaugstākā klasifikācijas līmeņa prasībām un visiem SISTĒMĀ apstrādātās informācijas apzīmējumiem.

3) Visu informāciju, ko apstrādā vai kas ir pieejama SISTĒMĀ šajā darbības režīmā, līdz ar sagatavoto izlaidi, aizsargā kā informāciju, kurai potenciāli piešķirta kategorija, un kurai ir piešķirts visaugstākais klasifikācijas līmenis, līdz tiek noteikts citādi, ja vien nepastāv marķēšanas funkcija ar pietiekamu uzticamības līmeni.

17. DAUDZLĪMEŅU DROŠĪBAS DARBĪBAS REŽĪMS ir: darbības režīms, kurā NE VISIEM indivīdiem, kam ir piekļuve SISTĒMAI, ir veikta drošības pārbaude, lai dotu piekļuvi visaugstākajam SISTĒMĀ apstrādātās informācijas līmenim, un NE VISIEM indivīdiem, kam ir piekļuve SISTĒMAI, ir vispārēja vajadzība pēc SISTĒMĀ apstrādātās informācijas.

Piezīmes:

1) šis darbības režīms pašreiz atļauj apstrādāt dažādu klasifikācijas līmeņu informāciju un dažādus informācijas kategoriju apzīmējumus,

2) tas, ka ne visiem indivīdiem ir veikta drošības pārbaude piekļuvei visaugstākajiem līmeņiem, līdz ar vispārējas vajadzības pēc informācijas trūkumu, norāda, ka ir nepieciešams, lai datordrošības elementi nodrošinātu selektīvu pieeju informācijai un tās dalīšanu SISTĒMĀ.

18. *INFOSEC* ir: drošības pasākumu piemērošana, lai aizsargātu informāciju, kuru apstrādā, uzglabā vai pārraida komunikācijas, informācijas un citās elektroniskajās sistēmās, pret konfidencialitātes, integritātes vai pieejamības zaudēšanu nejauši vai ar nolūku, un lai novērstu pašu sistēmu integritātes un pieejamības zaudēšanu. *INFOSEC* ietver pasākumus, kas attiecas uz datoru, pārraides, emisijas un kriptogrāfisko drošību un informācijas un SISTĒMU apdraudējumu atklāšanu, dokumentāciju un novēršanu.

19. DATORDROŠĪBA (*COMPUSEC*) ir: aparatūras, programmaparatūras un programmatūras drošības elementu piemērošana datorsistēmai, lai to aizsargātu pret neatļautu informācijas izpaušanu, manipulēšanu, izmainīšanu/izdzēšanu vai pakalpojuma atteikumu, vai to novērstu.

20. DATORDROŠĪBAS PRODUKTS ir: vispārīgs datordrošības elements, kurš ir paredzēts iestrādei IT sistēmā, lai to izmantotu apstrādātās informācijas konfidencialitātes, integritātes vai pieejamības veicināšanā vai nodrošināšanā.

21. KOMUNIKĀCIJAS DROŠĪBA (*COMSEC*) ir: drošības pasākumu piemērošana telekomunikācijām, lai nepieļautu nepiederošu personu piekļuvi vērtīgai informācijai, kura, iespējams, iegūta saistībā ar šādu telekomunikāciju piederību un izpēti, vai nodrošinātu šādu telekomunikāciju autentiskumu.

Piezīme:

Šādi pasākumi ietver kriptogrāfisko, pārraides un emisijas drošību; un ietver arī procesuālo, fizisko, personāla, dokumentu un datoru drošību.

22. NOVĒRTĒŠANA ir: SISTĒMAS drošības aspektu vai kriptogrāfiska vai datordrošības produkta precīza tehniska pārbaude, ko veic attiecīga iestāde.

Piezīmes:

1) Novērtēšanā izmeklē, vai pastāv nepieciešamā drošības funkcionalitāte un vai nav negatīvas šādas funkcionalitātes blakus iedarbības, kā arī novērtē šādas funkcionalitātes izmaiņu neiespējamību.

2) Novērtēšanā nosaka to, ciktāl tiek izpildītas SISTĒMAS drošības prasības vai datordrošības produkta drošības prasības, un nosaka SISTĒMAS drošības līmeni, vai arī kriptogrāfiskā vai datordrošības produkta drošo funkciju.

23. SERTIFICĒŠANA ir: oficiāla paziņojuma izdošana, kā pamatā ir novērtējuma veikšanas un rezultātu neatkarīgs pārskats par to, ciktāl SISTĒMA atbilst drošības prasībām, vai datordrošības produkts atbilst iepriekš noteiktām drošības prasībām.

▼B

24. AKREDITĒŠANA ir: atļauja un apstiprinājums, ko piešķir SISTĒMAI, lai apstrādātu ES klasificēto informāciju tās ekspluatācijas vidē.

Piezīme:

Šādu akreditēšanu veic pēc visu attiecīgo drošības procedūru īstenošanas un kad ir sasniegts pietiekams sistēmas resursu aizsardzības līmenis. Akreditēšana parasti jāveic, pamatojoties uz SSRS, ietverot:

a) paziņojumu par objektīvu sistēmas akreditēšanu; jo īpaši, kāda(–u) klasifikācijas līmeņa(–u) informācija ir jāapstrādā un kāds(–i) sistēmas vai tīkla darbības drošības režīms(–i) tiek piedāvāts(–i);

b) riska pārvaldības pārskata sniegšanu, lai identificētu draudus un ievainojamību un pasākumus pret tiem;

c) darba kārtību saistībā ar drošību līdz ar piedāvāto darbību sīku aprakstu (piemēram, režīmi, pakalpojumi, kas jānodrošina), un ietverot SISTĒMAS drošības elementus, kas veido akreditācijas pamatu;

d) drošības elementu īstenošanas un uzturēšanas plānu;

e) plānu sākotnējai un turpmākai sistēmas drošībai, vai tīkla drošības testu, novērtēšanu un sertificēšanu, un

f) vajadzības gadījumā, sertificēšanu līdz ar citiem akreditēšanas elementiem.

25. IT SISTĒMA ir: iekārtu, metožu un procedūru kopums un, vajadzības gadījumā, personāls, kas organizēts, lai izpildītu informācijas apstrādes funkcijas.

Piezīmes:

1) Uzskata, ka tas nozīmē ierīču kopumu, kas izstrādāts, lai apstrādātu informāciju sistēmā.

2) Šādas sistēmas var izmantot konsultāciju, vadības, kontroles, komunikāciju, zinātniskam vai administratīvam lietojumam, tostarp tekstapstrādei.

3) Sistēmas robežas parasti noteiks kā elementus, kas atrodas vienas IT sistēmas darbības iestādes kontrolē.

4) IT sistēma var ietvert apakšsistēmas, no kurām dažas pašas ir IT sistēmas.

26. IT SISTĒMAS DROŠĪBAS ELEMENTI ietver visas datoru aparatūras/programmaparatūras/programmatūras funkcijas, īpašības un elementus; darbības procedūras, pārskata procedūras un piekļuves kontroles, IT zonu, attālo termināļu/darbstaciju zonu un vadības noteikumus, fizisko struktūru un ierīces, personāla un komunikāciju kontroles pasākumus, kas nepieciešami, lai nodrošinātu pietiekamu aizsardzības līmeni klasificētai informācijai, kas apstrādājama IT sistēmā.

27. IT TĪKLS ir: ģeogrāfiski izkliedētu IT sistēmu organizācija, kas savstarpēji savienotas datu apmaiņas nolūkā un ietver savstarpēji savienoto IT sistēmu un to saskarnes ar datu vai komunikāciju papildtīkliem komponentus.

Piezīmes:

1) IT tīkls var izmantot viena vai vairāku datu apmaiņas nolūkā savstarpēji savienotu komunikāciju tīklu pakalpojumus; vairāki IT tīkli var izmantot kopēja komunikāciju tīkla pakalpojumus.

2) IT tīklu sauc par "vietēju", ja tas savieno vairākus datorus vienā vietā.

28. IT TĪKLA DROŠĪBAS ELEMENTI ietver atsevišķu IT sistēmu drošības elementus, kuras kopā veido tīklu kopā ar tiem papildu komponentiem un elementiem, kas saistīti ar tīklu kā tādu (piemēram, tīkla komunikācijas, drošības identifikācija un marķēšanas mehānismi un procedūras, piekļuves kontroles, programmas un auditācijas pieraksti), kuri vajadzīgi, lai nodrošinātu pietiekamu aizsardzības līmeni klasificētai informācijai.

▼B

29. IT ZONA ir: zona, kurā atrodas viens vai vairāki datori, to vietējās perifērās un glabāšanas vienības, kontroles vienības un speciālās tīkla un komunikāciju iekārtas.

Piezīme:

Tas neietver atsevišķu zonu, kurā atrodas attālinātas perifērās iekārtas vai termināļi/darbstacijas, pat ja šīs iekārtas ir savienotas ar ierīcēm IT zonā.

30. ATTĀLĀ TERMINĀĻA/DARBSTACIJAS ZONA ir: zona, kurā atrodas dažas datoriekārtas, to vietējās perifērās iekārtas vai termināļi/darbstacijas, un jebkādas saistītas komunikāciju iekārtas, kas ir atsevišķi no IT zonas.

31. Pārejoša elektromagnētiskā impulsa noplūdes standarta (*TEMPEST*) pretpasākumi: drošības pasākumi, kuru nolūks ir aizsargāt iekārtas un komunikāciju infrastruktūras pret klasificētas informācijas apdraudējumu, ko izraisa nejaušas elektromagnētiskas emisijas.

III nodaļa

Pienākumi drošības jomā

VISPĀRĪGI JAUTĀJUMI

32. Drošības komitejas pienākumi, kas noteikti I iedaļas 4. punktā, ietver INFOSEC jautājumus. Drošības komiteja organizē savas darbības tā, lai tā varētu sniegt ekspertu konsultācijas iepriekš minētajos jautājumos.

33. Ja rodas problēmas saistībā ar drošību (starpgadījumi, pārkāpumi u.c.), atbildīgā Valsts iestāde un/vai Padomes Ģenerālsekretariāta Drošības birojs nekavējoties rīkojas. Par visām problēmām ziņo Padomes Ģenerālsekretariāta Drošības birojam.

34. Ģenerālsekretārs/augstais pārstāvis vai, vajadzības gadījumā, ES decentralizētās aģentūras vadītājs izveido INFOSEC biroju, lai sniegtu drošības iestādei norādes attiecībā uz īpašu drošības elementu, kas izstrādāti kā SISTĒMU daļa, īstenošanu un kontroli.

DROŠĪBAS AKREDITĀCIJAS IESTĀDE

35. Drošības akreditācijas iestāde ir vai nu

— valsts drošības iestāde,

— ģenerālsekretāra/augstā pārstāvja izraudzīta iestāde,

— ES decentralizētās aģentūras drošības iestāde, vai arī

— to deleģētie/izraudzītie pārstāvji, atkarībā no akreditējamās SISTĒMAS.

36. Drošības akreditācijas iestāde atbild par to, lai nodrošinātu SISTĒMU atbilstību Padomes drošības politikai. Viens no tās uzdevumiem ir piešķirt SISTĒMAS apstiprinājumu apstrādāt ES klasificēto informāciju līdz noteiktam klasifikācijas līmenim tās ekspluatācijas vidē. Attiecībā uz Padomes Ģenerālsekretariātu un, attiecīgā gadījumā, ES decentralizētajām aģentūrām drošības akreditācijas iestāde atbild par drošību ģenerālsekretāra/augstā pārstāvja vai decentralizēto aģentūru vadītāju vārdā.

Padomes Ģenerālsekretariāta drošības akreditācijas iestādes jurisdikcijā ir visas SISTĒMAS, kuras darbojas Padomes Ģenerālsekretariāta telpās. SISTĒMAS un SISTĒMU komponenti, kas darbojas dalībvalstī, paliek šīs dalībvalsts jurisdikcijā. Ja Padomes Ģenerālsekretariāta drošības akreditācijas iestādes un citu drošības akreditācijas iestāžu jurisdikcijā nonāk dažādi SISTĒMAS komponenti, visas puses ieceļ apvienoto akreditācijas padomi, ko koordinē Padomes Ģenerālsekretariāta drošības akreditācijas iestāde.

INFOSEC IESTĀDE

37. *INFOSEC* iestāde atbild par *INFOSEC* biroja darbībām. Attiecībā uz Padomes Ģenerālsekretariātu un, attiecīgā gadījumā, ES decentralizētajām aģentūrām *INFOSEC* iestāde atbild par:

▼B

— tehnisku konsultāciju un palīdzības sniegšanu drošības akreditācijas iestādei,

— palīdzības sniegšanu sistēmai raksturīgu drošības prasību paziņojumu (*SSRS*) izstrādē,

— *SSRS* pārskatīšanu, lai nodrošinātu atbilstību šim drošības reglamentam un *INFOSEC* politikām un arhitektūras dokumentiem,

— dalību akreditēšanas kolēģijās/padomēs pēc vajadzības un *INFOSEC* akreditācijas ieteikuma sniegšanu drošības akreditācijas iestādei,

— atbalsta nodrošināšanu *INFOSEC* mācību un izglītības darbībām,

— tehnisku konsultāciju sniegšanu ar *INFOSEC* saistītu starpgadījumu izmeklēšanā,

— tehniskās politikas vadlīniju noteikšanu, lai nodrošinātu tikai atļautas programmatūras izmantošanu.

IT SISTĒMU DARBĪBAS IESTĀDE

38. *INFOSEC* iestāde iespējami agrākā posmā deleģē atbildību par SISTĒMAS kontroles pasākumu un īpašo drošības elementu ieviešanu un darbību IT sistēmu darbības iestādei. Šī atbildība ilgst visu SISTĒMAS darbības ciklu no projekta koncepcijas posma līdz galīgai realizācijai.

39. IT sistēmu darbības iestāde ir atbildīga par visiem drošības pasākumiem, kas izstrādāti kā kopējās SISTĒMAS daļa. Šī atbildība ietver ar drošību saistās darba kārtības sagatavošanu. IT sistēmu darbības iestāde precizē drošības standartus un praksi, kas jāievēro SISTĒMAS piegādātājam.

40. IT sistēmu darbības iestāde attiecīgā gadījumā var deleģēt daļu savas atbildības, piemēram, *INFOSEC* atbildīgajam par drošību un *INFOSEC* atbildīgajam par drošību objektā. Dažādas *INFOSEC* funkcijas var izpildīt viena persona.

LIETOTĀJI

41. Visu lietotāju pienākums ir nodrošināt, lai viņu darbības negatīvi neietekmētu viņu lietoto SISTĒMU drošību.

INFOSEC MĀCĪBAS

42. *INFOSEC* izglītība un mācības ir pieejamas dažādos līmeņos un dažādam personālam attiecīgi Padomes Ģenerālsekretariātā, ES decentralizētajās aģentūrās vai dalībvalstu valdību struktūrvienībās.

IV nodaļa

Netehniskie drošības pasākumi

PERSONĀLA DROŠĪBA

43. SISTĒMAS lietotājiem veic drošības pārbaudi un viņiem ir vajadzība pēc informācijas atbilstīgi viņu konkrētajā SISTĒMĀ apstrādātās informācijas klasifikācijai un saturam. Piekļuve noteiktām iekārtām vai informācijai, kas būtiska SISTĒMU drošībai, prasīs īpašas pārbaudes veikšanu saskaņā ar Padomes procedūrām.

44. Drošības akreditācijas iestāde norāda visus augsta riska amatus un precizē pārbaudes līmeni un uzraudzību, kāda veicama visam personālam šajos amatos.

45. SISTĒMAS precizē un veido tā, lai atvieglotu pienākumu un atbildības sadalīšanu personālam, lai novērstu to, ka vienai personai ir pilnīga informācija vai kontrole pār sistēmas drošības galvenajiem punktiem. Tā mērķis ir nodrošināt, ka, lai varētu veikt izmaiņas vai ļaunprātīgas darbības sistēmā vai tīklā, būtu vajadzīga slepena noruna starp divām vai vairāk personām.

FIZISKĀ DROŠĪBA

46. IT un attālās terminālu/darbstaciju zonas (kā noteikts 29. un 30. punktā), kurās ar IT palīdzību apstrādā informāciju, kas klasificēta kā ES konfiden-

▼B

ciālā (CONFIDENTIEL UE) un augstāk, vai kur ir iespējama piekļuve šādai informācijai, izveido attiecīgi kā ES I kategorijas vai II kategorijas drošības zonas vai to ekvivalentus attiecīgajās valstīs.

47. IT un attālās termināļu/darbstaciju zonas, kurās var mainīt SISTĒMAS drošību, neaizņem tikai viens pilnvarots ierēdnis/cits darbinieks.

SISTĒMAS PIEKĻUVES KONTROLE

48. Visa informācija un materiāls, kas ļauj kontrolēt piekļuvi sistēmai, ir aizsargāts ar pasākumiem, kas samērojami ar visaugstāko klasifikāciju un kategorijas noteikšanu informācijai, kurai tas var piešķirt piekļuvi.

49. Kad piekļuves kontroles informāciju un materiālu vairs neizmanto šim mērķim, to iznīcina saskaņā ar 61. līdz 63. punktu.

V nodaļa

Tehniskie drošības pasākumi

INFORMĀCIJAS DROŠĪBA

50. Informācijas autora pienākums ir identificēt un klasificēt visus dokumentus, kuros ir informācija, neatkarīgi no tā, vai tie ir cietās kopijas veidā vai uz elektroniskā informācijas nesēja. Katru cietās kopijas lappusi augšā un apakšā marķē atbilstoši klasifikācijai. Izlaidei neatkarīgi no tā, vai tā ir cietās kopijas veidā vai elektroniskā informācijas nesējā, ir tāda pati klasifikācija kā tās veidošanai izmantotās informācijas visaugstākā klasifikācija. SISTĒMAS darbības veids arī var ietekmēt šīs sistēmas izlaides klasifikāciju.

51. Organizācijas un tās informācijas turētāju pienākums ir aplūkot atsevišķu informācijas elementu kopības jautājumus un secinājumus, ko var izdarīt no saistītajiem elementiem, un noteikt, vai informācijas kopumam būtu lietderīgi piemērot augstāku klasifikāciju.

52. Tas, ka informācija, iespējams, ir saīsinājuma kods, pārraides kods vai ir jebkāda bināra atveidojuma formā, nenodrošina aizsardzību, un tādēļ tas nedrīkst ietekmēt informācijas klasifikāciju.

53. Ja informāciju pārsūta no vienas SISTĒMAS citai, informāciju pārsūtīšanas laikā un saņēmējā SISTĒMĀ aizsargā atbilstoši sākotnējai klasifikācijai un informācijas kategorijai.

54. Visus elektroniskos informācijas nesējus apstrādā atbilstoši uzglabātās informācijas visaugstākajai klasifikācijai vai nesēja etiķetei un tos vienmēr pienācīgi aizsargā.

55. Atkārtoti izmantojamie elektroniskie informācijas nesēji, ko izmanto ES klasificētās informācijas ierakstīšanai, saglabā visaugstāko klasifikāciju, kurai tie tikuši izmantoti, līdz informācija ir pienācīgi ierindota zemākā kategorijā vai deklasificēta un nesējs attiecīgi pārklasificēts, vai arī nesējs ir deklasificēts vai iznīcināts saskaņā ar apstiprinātu Padomes Ģenerālsekretariāta vai attiecīgās valsts procedūru (skatīt 61. līdz 63. punktu).

INFORMĀCIJAS KONTROLE UN PĀRSKATĀMĪBA

56. Ar automātiskiem (auditācijas pierakstu) vai manuāliem pierakstiem reģistrē piekļuvi informācijai, kas klasificēta kā ES slepenā (*SECRET UE*) un augstāk. Šos pierakstus saglabā saskaņā ar šo drošības reglamentu.

57. ES klasificētās izlaides, ko glabā IT zonā, var apstrādāt kā vienu klasificētu elementu un tās nevajag reģistrēt, ar noteikumu, ka materiāls ir identificēts, uz tā ir klasifikācijas marķējums un tas tiek pienācīgi kontrolēts.

58. Ja izlaidi iegūst no SISTĒMAS, kurā apstrādā ES klasificēto informāciju, un pārraida no IT zonas uz attālu termināla/darbstacijas zonu, attālās izlaides kontrolēšanai ar Drošības akreditācijas iestādes piekrišanu izveido procedūras. ES slepenajai (*SECRET UE*) informācijai un augstākai šādas procedūras ietver īpašus norādījumus par informācijas pārskatāmību.

▼B

NOŅEMAMU ELEKTRONISKO INFORMĀCIJAS NESĒJU APSTRĀDE UN KONTROLE

59. Visus noņemamos elektroniskos informācijas nesējus, kas klasificēti kā ES konfidenciāli (*CONFIDENTIEL UE*) un augstāk, apstrādā kā klasificētu materiālu un tiem piemēro vispārīgus noteikumus. Datu nesēju īpašajam fiziskajam izskatam jāpiemēro atbilstīgs identifikācijas un klasifikācijas marķējums, lai skaidri varētu atpazīt nesējus.

60. Lietotāju pienākums ir nodrošināt, ka ES klasificētā informācija tiek uzglabāta nesējos ar attiecīgu klasifikācijas marķējumu un aizsardzību. Izveido procedūras, lai nodrošinātu, ka visos ES informācijas līmeņos glabāšana elektroniskajos informācijas nesējos notiek saskaņā ar šo drošības reglamentu.

ELEKTRONISKO INFORMĀCIJAS NESĒJU DEKLASIFIKĀCIJA UN IZNĪCINĀŠANA

61. Elektroniskos informācijas nesējus, kurus izmanto ES klasificētās informācijas ierakstīšanai, var ierindot zemākā kategorijā, ja piemēro apstiprinātas Padomes Ģenerālsekretariāta vai attiecīgās valsts procedūras.

62. Elektroniskos informācijas nesējus, kuros glabāta ES sevišķi slepenā (*TRÈS SECRET UE/EU TOP SECRET*) vai īpašas kategorijas informācija, nedeklasificē un nelieto atkārtoti.

63. Ja elektronisko informācijas nesēju nevar deklasificēt, vai tas nav atkārtoti izmantojams, to iznīcina ar apstiprinātu Padomes Ģenerālsekretariāta vai attiecīgās valsts procedūru.

KOMUNIKĀCIJU DROŠĪBA

64. Ja elektromagnētiski pārraida ES klasificēto informāciju, šādu pārraižu konfidencialitātes, integritātes un pieejamības aizsardzības nolūkā īsteno īpašus pasākumus. Drošības akreditācijas iestāde nosaka prasības pārraižu aizsardzībai pret atklāšanu un pārtveršanu. Komunikāciju sistēmā pārraidīto informāciju aizsargā, pamatojoties uz konfidencialitātes, integritātes un pieejamības prasībām.

65. Ja konfidencialitātes, integritātes un pieejamības aizsardzības nodrošināšanai ir nepieciešamas kriptogrāfiskās metodes, šādas metodes vai saistītus produktus īpaši apstiprina Drošības akreditācijas iestāde.

66. Nosūtīšanas laikā ES slepenās (*SECRET UE*) un augstāk klasificētas informācijas konfidencialitāti aizsargā ar kriptogrāfiskām metodēm vai produktiem, ko Padome apstiprinājusi pēc Padomes Drošības komitejas ieteikuma. Nosūtīšanas laikā ES konfidenciālās (*CONFIDENTIEL UE*) vai ES ierobežotas pieejamības (*RESTREINT UE*) informācijas konfidencialitāti aizsargā ar kriptogrāfiskām metodēm vai produktiem, ko apstiprinājis vai nu ģenerālsekretārs/augstais pārstāvis pēc Padomes Drošības komitejas ieteikuma, vai arī attiecīgā dalībvalsts.

67. Īpašās drošības instrukcijās, ko Padome apstiprinājusi pēc Padomes Drošības komitejas ieteikuma, norāda sīki izstrādātus noteikumus, kas piemērojami ES klasificētās informācijas nosūtīšanai.

68. Ārkārtējos darbības apstākļos informāciju, kas klasificēta kā ES konfidenciālā (*CONFIDENTIEL UE*) vai ES ierobežotas pieejamības (*RESTREINT UE*), drīkst pārraidīt skaidrā tekstā ar noteikumu, ka katrs gadījums ir skaidri atļauts. Ārkārtēji apstākļi ir šādi:

a) gaidāmas vai esošas krīzes, konflikta vai kara situācijas, un

b) ja piegādes ātrums ir sevišķi svarīgs, nav pieejami šifrēšanas līdzekļi nav pieejami un tiek novērtēts, ka pārraidīto informāciju nevar paspēt izmantot, lai negatīvi ietekmētu darbības.

69. SISTĒMAI vajadzības gadījumā piemīt spēja liegt piekļuvi ES klasificētai informācijai ikvienā vai visās tās attālajās darbstacijās vai terminālos, izmantojot fizisku atslēgšanu vai īpašus Drošības akreditācijas iestādes apstiprinātu programmatūras elementus.

▼B

UZSTĀDĪŠANAS UN IZSTAROŠANAS DROŠĪBA

70. SISTĒMU sākotnējais uzstādījums un jebkādas būtiskas izmaiņas precizē tā, ka uzstādīšanu veic uzstādītāji, kam veikta drošības pārbaude, kurus nepārtraukti uzrauga tehniski kvalificēts personāls. Personālam ir veikta pārbaude, lai piešķirtu piekļuvi ES klasificētajai informācijai, kuras līmenis ir līdzvērtīgs visaugstākajai klasifikācijai, kādu var uzglabāt un apstrādāt SISTĒMĀ.

71. Visas iekārtas uzstāda saskaņā ar pašreizējo Padomes drošības politiku.

72. SISTĒMAS, kurās apstrādā informāciju, kas klasificēta kā ES konfidenciālā (*CONFIDENTIEL UE*) un augstāk, aizsargā tā, lai to drošību neapdraudētu informācijas noplūde, kuras izpēti un kontroli apzīmē ar terminu "*TEMPEST*".

73. *TEMPEST* pretpasākumus Padomes Ģenerālsekretariāta un ES decentralizēto aģentūru uzstādījumiem pārskata un apstiprina *TEMPEST* iestāde, ko izraudzījusies Padomes Ģenerālsekretariāta Drošības iestāde. Attiecīgo valstu iekārtām, kurās apstrādā ES klasificēto informāciju, apstiprināšanas iestāde ir atzītā attiecīgās valsts *TEMPEST* apstiprināšanas iestāde.

VI nodaļa

Drošība apstrādes laikā

DARBA KĀRTĪBA SAISTĪBĀ AR DROŠĪBU

74. Darba kārtībā saistībā ar drošību ir noteikti principi, kas jāpieņem attiecībā uz drošības jautājumiem, darba kārtība, kas jāievēro, un personāla pienākumi. Darba kārtību saistībā ar drošību sagatavo IT sistēmu darbības iestādes pārziņā.

PROGRAMMATŪRAS AIZSARDZĪBAS/KONFIGURĀCIJAS VADĪBA

75. Lietojumprogrammu aizsardzību nosaka, pamatojoties drīzāk uz pašas programmas drošības klasifikācijas vērtējumu, nevis uz tās informācijas klasifikāciju, kura tai jāapstrādā. Izmantotie programmatūras varianti regulāri jāpārbauda, lai nodrošinātu to integritāti un pareizu darbību.

76. ES klasificētās informācijas apstrādei nedrīkst izmantot jaunus vai izmainītus programmatūras variantus, kamēr tos nav apstiprinājusi IT sistēmu darbības iestāde.

ĻAUNDABĪGAS PROGRAMMATŪRAS/DATORA VĪRUSU ESAMĪBAS PĀRBAUDE

77. Ļaundabīgas programmatūras/datora vīrusu esamību periodiski pārbauda saskaņā ar Drošības akreditācijas iestādes prasībām.

78. Visi elektroniskie informācijas nesēji, kas nonāk Padomes Ģenerālsekretariātā, ES decentralizētajās aģentūrās vai dalībvalstīs, pirms ievadīšanas jebkurā SISTĒMĀ jāpārbauda, vai tajos nav ļaundabīgas programmatūras/datoru vīrusi.

UZTURĒŠANA

79. Līgumos un procedūrās apkopei pēc grafika un pēc izsaukuma, ko veic SISTĒMĀM, kurām ir sastādīts sistēmai raksturīgu drošības prasību ziņojums, precizē prasības un kārtību apkopes personālam un tā saistītajām iekārtām, kas nonāk IT zonā.

80. Prasības skaidri norāda sistēmai raksturīgu drošības prasību ziņojumā, un procedūras skaidri norāda darba kārtībā saistībā ar drošību. Līgumslēdzēju veiktu apkopi, kam nepieciešamas attālās piekļuves diagnostikas procedūras, atļauj tikai ārkārtas apstākļos, ar stingru drošības kontroli un vienīgi ar Drošības akreditācijas iestādes atļauju.

▼B

VII nodaļa

Publiskais iepirkums

81. Jebkuram iepērkamajam drošības produktam, ko paredzēts izmantot SISTĒMĀ, ir vai nu jābūt novērtētam un sertificētam, vai pašreiz jāatrodas novērtēšanas un sertificēšanas procesā, ko pēc starptautiski atzītiem kritērijiem (piemēram, Vienotajiem informācijas tehnoloģiju drošības novērtējuma kritērijiem, skatīt ISO 15408) veic attiecīga novērtēšanas vai sertificēšanas iestāde.

82. Pieņemot lēmumu par to, vai iekārtas, īpaši elektroniskos informācijas nesējus nomāt vai pirkt, jāatceras, ka šādas iekārtas, kas reiz izmantotas ES klasificētās informācijas apstrādei, nevar laist ārpus pietiekami drošas vides, pirms tās nav deklasificētas ar Drošības akreditācijas iestādes apstiprinājumu, un ka šāds apstiprinājums ne vienmēr var būt iespējams.

AKREDITĀCIJA

83. Visas SISTĒMAS, kurām pirms ES klasificētās informācijas apstrādes jāsastāda sistēmai raksturīgu drošības prasību ziņojums, akreditē Drošības akreditācijas iestāde, pamatojoties uz sistēmai raksturīgu drošības prasību ziņojumā, darba kārtībā saistībā ar drošību un citos attiecīgos dokumentos sniegto informāciju. Apakšsistēmas un attālos terminālus/darbstacijas akreditē kā visu SISTĒMU, kurām tos pievieno, daļu. Ja SISTĒMA apkalpo gan Padomi, gan citas organizācijas, Padomes Ģenerālsekretariāts un attiecīgās drošības iestādes savstarpēji vienojas par akreditāciju.

84. Akreditācijas procesu var veikt saskaņā ar akreditācijas stratēģiju, kas ir atbilstoša konkrētajai SISTĒMAI un ko noteikusi Drošības akreditācijas iestāde.

NOVĒRTĒŠANA UN SERTIFICĒŠANA

85. Pirms akreditēšanas dažos gadījumos SISTĒMAS aparatūras, programmaparatūras un programmatūras drošības elementus novērtē un sertificē kā tādus, kas spēj aizsargāt informāciju paredzētajā klasifikācijas līmenī.

86. Novērtēšanas un sertificēšanas prasības iekļauj sistēmas plānošanā un skaidri norāda sistēmai raksturīgu drošības prasību ziņojumā.

87. Novērtēšanas un sertificēšanas procesus veic saskaņā ar apstiprinātām vadlīnijām tehniski kvalificēts un pietiekami pārbaudīts personāls, kas rīkojas IT sistēmu darbības iestādes vārdā.

88. Komandas var nodrošināt no izraudzītas dalībvalsts novērtēšanas vai sertificēšanas iestādes vai no tās izraudzītiem pārstāvjiem, piemēram, kompetentu un pārbaudītu darbuzņēmēju.

89. Iesaistīto novērtēšanas un sertificēšanas procesu pakāpi var mazināt (piemēram, tikai iesaistot integrācijas aspektus), ja SISTĒMU pamatā ir esoši valsts novērtēti un sertificēti datordrošības produkti.

DROŠĪBAS ELEMENTU REGULĀRA PĀRBAUDE TURPMĀKAI AKREDITĒŠANAI

90. IT sistēmu darbības iestāde izveido regulāras kontroles procedūras, kas nodrošina to, ka visi SISTĒMAS drošības elementi joprojām ir derīgi.

91. Pārmaiņu veidus, kuru dēļ būtu jāveic atkārtota akreditēšana vai kam ir nepieciešama Drošības akreditācijas iestādes iepriekšēja piekrišana, skaidri identificē un norāda sistēmai raksturīgu drošības prasību ziņojumā. Pēc jebkādām izmaiņām, remonta vai kļūmes, kas, iespējams, ietekmējusi SISTĒMAS drošības elementus, IT sistēmu darbības iestāde nodrošina pārbaudes veikšanu, lai pārliecinātos par drošības elementu pareizu darbību. SISTĒMAS turpmāka akreditēšana parasti ir atkarīga no apmierinoši veiktām pārbaudēm.

92. Drošības akreditācijas iestāde periodiski pārbauda vai pārskata visas SISTĒMAS, kur īstenoti drošības elementi. SISTĒMĀM, kurās apstrādā ES sevišķi slepeno (*TRÈS SECRET UE/EU TOP SECRET*) vai papildus marķēto informāciju, pārbaudes veic vismaz reizi gadā.

▼B

VIII nodaļa

Pagaidu vai neregulāra lietošana

MIKRODATORU/PERSONĀLO DATORU DROŠĪBA

93. Mikrodatorus/personālos datorus (*PC*) ar fiksētiem diskiem (vai citus energoneatkarīgas atmiņas informācijas nesējus), kas darbojas autonomā režīmā vai kā tīkla konfigurācijas, un pārnēsājamas skaitļošanas ierīces (piemēram, pārnēsājamos *PC* un elektroniskās "piezīmju grāmatiņas") ar fiksētiem cietajiem diskiem uzskata par informācijas nesējiem tādā pašā nozīmē, kā disketes vai citus noņemamos elektroniskos informācijas nesējus.

94. Šīm iekārtām nodrošina aizsardzības līmeni, kas piekļuves, apstrādes, uzglabāšanas un transportēšanas ziņā atbilst visaugstākajam informācijas līmenim, ko jebkad uzglabā vai apstrādā (līdz to ierindo zemākā kategorijā vai deklasificē saskaņā ar apstiprinātām procedūrām).

PRIVĀTAS IT IEKĀRTAS IZMANTOŠANA OFICIĀLAM PADOMES DARBAM

95. ES klasificētās informācijas apstrādei ir aizliegts izmantot privātus noņemamus elektroniskos informācijas nesējus, programmatūru un IT aparatūru (piemēram, *PC* un pārnēsājamas skaitļošanas ierīces) ar uzglabāšanas iespēju.

96. Privātu aparatūru, programmatūru un nesējus neienes I kategorijas vai II kategorijas zonā, kur apstrādā ES klasificēto informāciju, bez Padomes Ģenerālsekretariāta Drošības biroja vai dalībvalsts struktūrvienības vai attiecīgās ES decentralizētās aģentūras vadītāja atļaujas.

DARBUZŅĒMĒJIEM PIEDEROŠU VAI VALSTS NODROŠINĀTU IT IEKĀRTU IZMANTOŠANA OFICIĀLAM PADOMES DARBAM

97. Izmantot darbuzņēmējiem piederošas IT iekārtas un programmatūru oficiālā Padomes darbā var atļaut tikai Padomes Ģenerālsekretariāta Drošības biroja vai dalībvalsts struktūrvienības, vai attiecīgās ES decentralizētās aģentūras vadītājs. Darbiniekiem Padomes Ģenerālsekretariātā vai ES decentralizētā aģentūrā var atļaut izmantot arī valsts nodrošinātas IT iekārtas un programmatūru; šajā gadījumā IT iekārtas iekļauj attiecīgajā Padomes Ģenerālsekretariāta inventāra sarakstā. Abos gadījumos, ja IT iekārtas ir izmantojamas ES klasificētās informācijas apstrādei, apspriežas ar Drošības akreditācijas iestādi, lai pienācīgi tiktu apsvērti un īstenoti *INFOSEC* elementi, kas piemērojami šādu iekārtu lietošanai.

▼B

XII IEDAĻA

ES KLASIFICĒTĀS INFORMĀCIJAS NODOŠANA TREŠĀM VALSTĪM VAI STARPTAUTISKĀM ORGANIZĀCIJĀM

PRINCIPI, KAS REGULĒ ES KLASIFICĒTĀS INFORMĀCIJAS NODOŠANU

1. Lēmumu par ES klasificētās informācijas nodošanu trešām valstīm vai starptautiskām organizācijām pieņem Padome, pamatojoties uz:

   — šādas informācijas raksturu un saturu,

   — saņēmēja vajadzību pēc informācijas,

   — ES ieguvumu aprēķinu.

   Nododamās ES klasificētās informācijas autoram dalībvalstī lūgs piekrišanu.

2. Šos lēmumus pieņem, katru gadījumu izskatot atsevišķi atkarībā no:

   — vēlamās sadarbības pakāpes ar attiecīgām trešām valstīm vai starptautiskām organizācijām,

   — to uzticamības, ko nosaka drošības līmenis, kāds tiktu piemērots ES klasificētajai informācijai, kura uzticēta šīm valstīm vai organizācijām, un no tajās piemērojamo drošības noteikumu atbilstības ES piemērotajiem drošības noteikumiem; Padomes Drošības komiteja sniegs Padomei tehnisko atzinumu šajā jautājumā.

3. Pieņemot ES klasificēto informāciju, trešās valstis vai starptautiskās organizācijas garantēs, ka šī informācija netiks izmantota citiem mērķiem kā vien tiem, kas motivē izsniegt informāciju vai apmainīties ar to, un ka tās nodrošinās Padomes noteikto aizsardzību.

LĪMEŅI

4. Tiklīdz Padomes ir nolēmusi, ka klasificēto informāciju drīkst nodot noteiktai valstij vai starptautiskai organizācijai, vai apmainīties ar informāciju ar tām, tā pieņems lēmumu par iespējamo sadarbības līmeni. Tas būs atkarīgs no drošības politikas un reglamenta, ko piemēro attiecīgā valsts vai organizācija.

5. Pastāv trīs sadarbības līmeņi:

   1. līmenis Sadarbība ar trešām valstīm vai starptautiskām organizācijām, kuru drošības politika un reglaments ir ļoti tuvi ES drošības politikai un reglamentam.

   2. līmenis Sadarbība ar trešām valstīm vai starptautiskām organizācijām, kuru drošības politika un reglaments būtiski atšķiras no ES drošības politikas un reglamenta.

   3. līmenis Neregulāra sadarbība ar trešām valstīm vai ar starptautiskām organizācijām, kuru politiku un drošības reglamentu nevar novērtēt.

6. Katrā sadarbības līmenī noteiks drošības reglamentu, kuru atsevišķos gadījumos formulēs, ņemot vērā Padomes Drošības komitejas tehnisko viedokli, ko saņēmējiem lūgs piemērot tiem nodotās klasificētās informācijas aizsardzībai. Šīs procedūras un drošības reglaments ir sīkāk izklāstīti 4., 5. un 6. papildinājumā.

NOLĪGUMI

7. Tiklīdz Padome ir nolēmusi, ka ir pastāvīga vai ilglaicīga vajadzība pēc klasificētas informācijas apmaiņas starp ES un trešām valstīm vai starptautiskām organizācijām, tā sastāda "nolīgumus par drošības procedūrām klasificētas informācijas apmaiņai" ar tām, nosakot sadarbības mērķi un savstarpējus noteikumus par apmainītās informācijas aizsardzību.

8. 3. līmeņa neregulārās sadarbības gadījumā, kas pēc definīcijas ir ierobežota laika un mērķa ziņā, "nolīguma par drošības procedūrām klasificētas informācijas apmaiņai" vietā var noslēgt vienkāršu saprašanās memorandu, kurā

▼B

noteikts apmaināmās klasificētās informācijas raksturs un savstarpējie pienākumi attiecībā uz informāciju, — ar nosacījumu, ka tā klasificēta ne augstāk kā ES ierobežotas pieejamības (*RESTREINT UE*).

9. Nolīgumu projektus par drošības procedūrām vai saprašanās memorandus pirms to iesniegšanas Padomei lēmuma pieņemšanai apstiprinās Drošības komiteja.

10. Valsts drošības iestādes sniegs ģenerālsekretāram/augstajam pārstāvim visu vajadzīgo palīdzību, lai nodrošinātu, ka nododamo informāciju izmanto un aizsargā saskaņā ar nolīgumu par drošības procedūrām vai saprašanās memorandu noteikumiem.

▼M3

XIII IEDAĻA

KOPĒJIE MINIMĀLIE RŪPNIECĪBAS DROŠĪBAS STANDARTI

1) Šajā iedaļā aplūko ražotājdarbību drošības aspektus, kas attiecas tikai uz sarunām un līgumu piešķiršanu gadījumā, ja rūpniecības vai citām struktūrām uztic uzdevumus, kas ir saistīti ar ES klasificēto informāciju un/vai kuros tā ietverta, tostarp ES klasificētās informācijas nodošana vai piekļuve tai valsts iepirkuma procedūru laikā (konkursa laikā un sarunās pirms līguma slēgšanas).

DEFINĪCIJAS

2) Šajos kopējos minimālajos standartos izmanto šādas definīcijas:

a) "klasificēts līgums": tāds līgums par ražojumu piegādi, darbu veikšanu vai pakalpojumu sniegšanu, kura izpilde prasa vai ir saistīta ar piekļuvi ES klasificētajai informācijai vai tās radīšanu;

b) "klasificēts apakšlīgums": tāds līgums par ražojumu piegādi, darbu veikšanu vai pakalpojumu sniegšanu, ko līgumslēdzējs slēdz ar citu līgumslēdzēju (t.i., apakšlīgumslēdzēju) un kura izpilde prasa vai ir saistīta ar piekļuvi ES klasificētajai informācijai vai tās radīšanu;

c) "līgumslēdzējs": fiziska vai juridiska persona, kuras tiesībspēja un rīcībspēja ļauj slēgt līgumus;

d) "Izraudzītā drošības iestāde (IDI)": iestāde, kas ir pakļauta ES dalībvalsts Valsts drošības iestādei (VDI) un ir atbildīga par to, ka rūpniecības un citas struktūras ir informētas par valsts politiku visā rūpniecības drošības jomā, kā arī par virzību un palīdzību tās īstenošanā. IDI uzdevumus var veikt VDI;

e) "iestādes drošības pārbaude (IDP)": VDI/IDI administratīvais konstatējums, ka no drošības viedokļa iestāde spēj nodrošināt pietiekamu drošības aizsardzību ES klasificētajai informācijai konkrētajā drošības klasifikācijas līmenī, kā arī to, ka attiecībā uz visiem tās darbiniekiem, kas pieprasa piekļuvi ES klasificētajai informācijai, ir pienācīgi veikta drošības pārbaude un tie ir informēti par attiecīgām vajadzīgām drošības prasībām, lai piekļūtu ES klasificētajai informācijai un to aizsargātu;

f) "rūpniecības vai cita struktūra": struktūra, ka piegādā ražojumus, veic darbu vai sniedz pakalpojumus; tās var būt rūpniecības, komerciālas, pakalpojumu sniedzēju, zinātniskas, pētniecības, izglītības vai attīstības struktūras;

g) "rūpniecības drošība": aizsardzības pasākumu un procedūru piemērošana, lai novērstu, atklātu un atlīdzinātu tās ES klasificētās informācijas zudumu vai apdraudējumu, ar ko rīkojas līgumslēdzējs vai apakšlīgumslēdzējs attiecībā uz sarunām pirms līguma slēgšanas un līgumiem;

h) "Valsts drošības iestāde (VDI)": ES dalībvalsts iestāde, kas ir galīgi atbildīga par ES klasificētās informācijas aizsardzību;

i) "vispārējs līguma drošības klasifikācijas līmenis": līguma drošības klasifikācijas noteikšana kopumā, pamatojoties uz tās informācijas un/vai materiāla klasifikāciju, ko radīs vai nodos, vai kam piekļūs, vai ko varētu radīt vai nodot, vai kam varētu piekļūt saistībā ar jebkuru vispārējā līguma elementu. Vispārējais līguma drošības klasifikācijas līmenis nedrīkst būt zemāks par jebkura tā elementa augstāko klasifikāciju, bet tas var būt augstāks kopības efekta dēļ;

j) "drošības aspektu vēstule (DAV)": līgumslēdzējas iestādes izdots īpašu līguma nosacījumu kopums, kas ir tā klasificētā līguma neatņemama sastāvdaļa, kurš saistīts ar piekļuvi ES klasificētai informācijai vai ar tās radīšanu, un kurā identificē drošības prasības vai tos līguma elementus, kam vajadzīga drošības aizsardzība;

k) "drošības klasifikācijas metodiskais līdzeklis (DKML)": dokuments, kurā aprakstīti klasificētie programmas vai līguma elementi, precizējot piemērojamus drošības klasifikācijas līmeņus. Drošības klasifikācijas meto-

▼M3

disko līdzekli programmas vai līguma darbības laikā var paplašināt, un informācijas elementus var pārklasificēt vai ierindot zemākā kategorijā. DKML ir jābūt daļai no DAV.

ORGANIZĀCIJA

3) Padomes Ģenerālsekretariāts (PĢS) var uzticēt uzdevumus, kas saistīti ar ES klasificēto informāciju un/vai kuros tā ietverta, līgumslēdzējām rūpniecības vai citām struktūrām, kas reģistrētas dalībvalstī.

4) PĢS nodrošina to, ka, piešķirot klasificētu līgumu, tiek ievērotas visas prasības, kas izriet no šiem minimālajiem standartiem.

5) Katra dalībvalsts nodrošina to, ka tās VDI ir atbilstīgas struktūras, lai piemērotu šos minimālos rūpniecības drošības standartus. Tās var ietvert vienu vai vairākas IDI.

6) Galīgo atbildību par ES klasificētās informācijas aizsardzību rūpniecības vai citās struktūrās uzņemas to vadība.

7) Ja piešķir līgumu vai apakšlīgumu, uz ko attiecas šie minimālie standarti, attiecīgi PĢS un/vai VDI/IDI nekavējoties paziņo tās dalībvalsts VDI/IDI, kurā līgumslēdzējs vai apakšlīgumslēdzējs ir reģistrēts.

KLASIFICĒTI LĪGUMI

8) Klasificētu līgumu drošības klasifikācijā jāņem vērā šādi principi:

   a) PĢS pēc vajadzības precizē līguma aspektus, kam nepieciešama aizsardzība, un attiecīgo drošības klasifikāciju; to darot, jāņem vērā sākotnējā klasifikācija, ko izcelsmes iestāde uz informāciju attiecināja pirms līguma piešķiršanas;

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

   c) ES klasificēto informāciju, ko rada, veicot ar līgumu saistītas darbības, klasificē saskaņā ar DKML;

   d) vajadzības gadījumos PĢS ir atbildīgs par vispārēja līguma klasifikācijas līmeņa vai jebkura tā elementa drošības klasifikācijas izmaiņu, apspriežoties ar izcelsmes iestādi, un par visu ieinteresēto personu informēšanu;

   e) klasificēto informāciju, ko nodod līgumslēdzējam vai apakšlīgumslēdzējam vai ko rada, veicot ar līgumu saistītas darbības, nedrīkst izmantot nolūkiem, kas nav precizēti klasificētā līgumā, un to nedrīkst nodot trešām personām bez iepriekšējas tās izcelsmes iestādes rakstiskas piekrišanas.

9) Dalībvalstu VDI/IDI ir atbildīga par to, lai līgumslēdzēji un apakšlīgumslēdzēji, kam piešķirti ar tādu informāciju saistīti klasificēti līgumi, kas klasificēta kā *CONFIDENTIEL UE* vai *SECRET UE*, veiktu visus attiecīgos pasākumus, lai aizsargātu šādu viņiem nodotu vai viņu radītu ES klasificēto informāciju, izpildot klasificētu līgumu saskaņā ar valsts normatīvajiem aktiem. Drošības prasību neievērošanas gadījumā līguma darbību var izbeigt.

10) Visām klasificētos līgumos iesaistītām rūpniecības vai citām struktūrām, kas saistīti ar piekļuvi *CONFIDENTIEL UE* vai *SECRET UE* informācijai, jāveic valsts IDP. VIDP veic dalībvalsts VDI/IDI, lai apliecinātu, ka iestāde spēj piemērot un nodrošināt pietiekamu drošības aizsardzību ES klasificētajai informācijai attiecīgā drošības klasifikācijas līmenī.

11) VDI/IDI ir atbildīga par personāla drošības pārbaudes (PDP) veikšanu saskaņā ar valsts noteikumiem visām personām, kuras ir nodarbinātas šajā dalībvalstī reģistrētajos ražošanas un citos uzņēmumos un kuru pienākumu pildīšanai nepieciešama piekļuve *CONFIDENTIEL UE* vai *SECRET UE* informācijai attiecībā uz klasificētu līgumu.

12) Klasificētos līgumos jāiekļauj DAV, kā noteikts 2. punkta j) apakšpunktā iepriekš. DAV jāiekļauj DKML.

13) Pirms klasificēta līguma sarunu sākšanas PĢS sazināsies ar to dalībvalstu VDI/IDI, kurā reģistrēti iesaistītie rūpnieciskie vai cita veida uzņēmumi, lai

▼M3

saņemtu apstiprinājumu, ka tiem ir veikta derīga VIDP atbilstīgi līguma drošības klasifikācijai.

14) Līgumslēdzējai iestādei nedrīkst parakstīt klasificētu līgumu ar izvēlēto pretendentu, pirms tā nav saņēmusi derīgu VIDP sertifikātu.

15) Ja vien to neprasa dalībvalstu normatīvie akti, VIDP nav jāveic attiecībā uz līgumiem, kuros iesaistīta informācija, kas klasificēta kā *RESTREINT UE*.

16) Attiecībā uz konkursiem, kas saistīti ar klasificētiem līgumiem, aicinājumā piedalīties jāiekļauj prasība, ka pretendentam, kurš neiesniedz priekšlikumu vai nav izvēlēts, visi dokumenti jāatdod atpakaļ noteiktajā termiņā.

17) Iespējams, ka līgumslēdzējam jāslēdz klasificēti apakšlīgumi ar apakšlīgumslēdzējiem dažādos līmeņos. Līgumslēdzējs ir atbildīgs par to, ka visas ar apakšlīgumu saistītas darbības izpilda saskaņā ar šajā iedaļā iekļautajiem kopējiem minimālajiem standartiem. Tomēr līgumslēdzējs nedrīkst nosūtīt ES klasificēto informāciju vai materiālus apakšlīgumslēdzējam bez iepriekšējas dokumenta sagatavotāja rakstiskas piekrišanas.

18) Nosacījumi par kārtību, kādā līgumslēdzējs var slēgt apakšlīgumu, jādefinē gan piedāvājumā, gan līgumā. Struktūrām, kas reģistrētas valstī, kas nav ES dalībvalsts, nedrīkst piešķirt apakšlīgumu, ja PĢS iepriekš nav devis skaidri izteiktu rakstisku atļauju.

19) Līguma darbības laikā attiecīgā VDI/IDI, sadarbojoties ar PĢS, pārraudzīs visu drošības noteikumu ievērošanu. Par drošības starpgadījumu paziņo saskaņā ar drošības reglamenta II daļas X iedaļu. Par izmaiņu VDIP vai tās atcelšanu nekavējoties ziņo PĢS un visām VDI/IDI, kam par to ir paziņots.

20) Ja pārtrauc līgumu vai apakšlīgumu, attiecīgi PĢS un/vai VDI/IDI nekavējoties paziņo tās dalībvalsts VDI/IDI, kur līgumslēdzējs vai apakšlīgumslēdzējs ir reģistrēts.

21) Līgumslēdzēji vai apakšlīgumslēdzēji šajā iedaļā iekļautos kopējos minimālos standartus turpina ievērot un klasificētās informācijas konfidencialitāti saglabā pēc klasificētā līguma vai apakšlīguma izbeigšanas vai pārtraukšanas.

22) Īpašus noteikumus par klasificētās informācijas iznīcināšanu līguma darbības beigās paredzēs DAV vai citos attiecīgos noteikumos par drošības prasībām.

APMEKLĒJUMI

23) PĢS personāla apmeklējumi rūpniecības vai citās struktūrās, kas dalībvalstīs pilda ES klasificētos līgumus, jāorganizē ar attiecīgās VDI/IDI palīdzību. Rūpniecības vai citu struktūru personāla apmeklējumi saistībā ar ES klasificēto līgumu jāorganizē, vienojoties iesaistītajām VDI/IDI. Tomēr VDI/IDI, kas iesaistītas ES klasificētā līgumā, var vienoties par kārtību, kādā rūpniecības vai citu struktūru personāla apmeklējumus var organizēt tieši.

ES KLASIFCĒTĀS INFORMĀCIJAS IZPLATĪŠANA UN NOSŪTĪŠANA

24) Attiecībā uz ES klasificētās informācijas izplatīšanu piemēro šā drošības reglamenta II daļas VII iedaļas II nodaļu un attiecīgos gadījumos XI iedaļu. Lai papildinātu šādus noteikumus, piemēros jebkurus pašreizējus dalībvalstīs spēkā esošos noteikumus.

25) Tās ES klasificētās informācijas starptautisku nosūtīšanu, kas saistīta ar klasificētiem līgumiem, veic saskaņā ar dalībvalstu noteikumiem. Izskatot drošības pasākumus starptautiskai nosūtīšanai, piemēro šādus principus:

a) drošība ir nodrošināta visos posmos un visos gadījumos sūtīšanas laikā no izcelsmes vietas līdz galamērķim;

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

c) vajadzības gadījumā veic VIDP uzņēmumiem, kas nodrošina sūtīšanu. Šajos gadījumos personālam, kas darbojas ar sūtījumu, veic pārbaudi atbilstīgi šīs iedaļas kopējiem minimālajiem standartiem;

▼**M3**

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

e) ja iespējams, maršrutiem būtu jāved tikai caur ES dalībvalstīm. Maršrutus caur valstīm, kas nav ES dalībvalstis, izvēlas tikai tad, kad ir saņemta atļauja gan no sūtītāja, gan no saņēmēja dalībvalsts VDI/IDI;

f) pirms nosūta ES klasificēto materiālu, sūtītājs sagatavo sūtīšanas plānu un iesaistītās VDI/IDI to apstiprina.

▼M2

1. papildinājums

Valsts drošības iestāžu saraksts

BEĻGIJA

Service public fédéral des affaires étrangères, du commerce extérieur et de la coopération au développement
Autorité nationale de sécurité (ANS)
Direction du protocole et de la sécurité
Service de la sécurité P&S 6
Rue des Petits Carmes 15
B-1000 Bruxelles
Telephone Secretariat: + 32/2/519 05 74
Telephone Presidency: + 32/2/501 82 20
+ 32/2/501 87 10
Fax: + 32/2/519 05 96

ČEHIJA

Národní bezpečnostní úřad
(National Security Authority)
Na Popelce 2/16
150 06 Praha 56
Tel.: (420) 257 28 33 35
Fax: (420) 257 28 31 10

DĀNIJA

Politiets Efterretningstjeneste
(Danish Security Intelligence Service)
Klausdalsbrovej 1
DK-2860 Søborg
Telephone: (45) 33 14 88 88
Fax: (45) 33 43 01 90

Forsvarets Efterretningstjeneste
(Danish Defence Intelligence Service)
Kastellet 30
DK-2100 København Ø
Telephone: (45) 33 32 55 66
Fax: (45) 33 93 13 20

VĀCIJA

Bundesministerium des Innern
Referat IS 4
Alt-Moabit 101 D
D-11014 Berlin
Telefon: + 49-1-888 681 15 26
Fax: + 49-1-888 681 558 06

IGAUNIJA

Eesti Vabariigi Kaitseministeerium
(Ministry of Defence, Republic of Estonia, Department of Security National Security Authority)
Sakala 1
EE-15094 Tallinn
Telephone: + 372/717 00 30
+ 372/717 00 31
+ 372/717 00 77
Fax: + 372/717 00 01

GRIEĶIJA

Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)

▼**M2**

Διακλαδική Διεύθυνση Στρατιωτικών Πληροφοριών (ΔΔΣΠ)
Διεύθυνση Ασφαλείας και Αντιπληροφοριών
GR-ΣΤΓ 1020 Χολαργός (Αθήνα)
Τηλέφωνα: (30-210) 657 20 09 (ώρες γραφείου)
(30-210) 657 20 10 (ώρες γραφείου)
Φαξ: (30-210) 642 64 32
(30-210) 652 76 12

[Hellenic National Defence General Staff (HNDGS)]
Military Intelligence Sectoral Directorate
Security Counterintelligence Directorate
GR-STG 1020 Holargos — Athens
Telephone: (30-210) 657 20 09 (office hours)
(30-210) 657 20 10 (office hours)
Fax: (30-210) 642 64 32
(30-210) 652 76 12

SPĀNIJA

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
Carretera nacional radial VI, km 8,5
E-28023 Madrid
Telephone: + 34/913 72 57 07
+ 34/913 72 50 27
Fax: + 34/913 72 58 08

FRANCIJA

Secrétariat général de la défense nationale
Service de sécurité de défense (SGDN/SSD)
51, boulevard de la Tour-Maubourg
F-75700 Paris 07 SP
Telephone: + 33/1/71 75 81 77
Fax: + 33/1/71 75 82 00

ĪRIJA

National Security Authority
Department of Foreign Affairs
80 St. Stephens Green
IRL-Dublin 2
Telephone (353-1) 478 08 22
Fax (353-1) 478 14 84

ITĀLIJA

Presidenza del Consiglio dei Ministri
Autorità Nazionale per la Sicurezza
Cesis III Reparto (UCSi)
Via di Santa Susanna, 15
I-00187 Roma
Telephone: + 39/06/611 742 66
Fax: + 39/06/488 52 73

KIPRA

Υπουργείο Άμυνας
Στρατιωτικό επιτελείο του υπουργού
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Υπουργείο Άμυνας
Λεωφόρος Εμμανουήλ Ροΐδη 4
CY-1432 Λευκωσία
Τηλέφωνα: (357-22) 80 75 69
(357-22) 80 75 19

▼M2

(357-22) 80 77 64
Φαξ: (357-22) 30 23 51

Ministry of Defence
Minister's Military Staff
National Security Authority (NSA)
4 Emanuel Roidi Street
CY-1432 Nicosia
Telephone: (357-22) 80 75 69
(357-22) 80 75 19
(357-22) 80 77 64
Fax: (357-22) 30 23 51

LATVIJA

National Security Authority of Constitution Protection
Bureau of the Republic of Latvia
Miera iela 85 A
LV-1013 Riga
Telephone: + 371/702 54 18
Fax: + 371/702 54 54

LIETUVA

Lithuanian National Security Authority
Gedimino ave. 40/1
LT-01110 Vilnius
Telephone: + 370/5/266 32 01
Fax: + 370/5/266 32 00

LUKSEMBURGA

Autorité nationale de sécurité
Ministère d'État
Boîte postale 23 79
L-1023 Luxembourg
Telephone: + 352/478 22 10 central
+ 352/478 22 35 direct
Fax: + 352/478 22 43
+ 352/478 22 71

UNGĀRIJA

National Security Authority Republic of Hungary
Nemzeti Biztonsági Felügyelet
Pf.: 2
HU-1352 Budapest
Telephone: + 361/346 96 52
Fax: + 361/346 96 58

MALTA

Ministry of Justice and Home Affairs
P.O. Box 146
MT-Valletta
Telephone: + 356/21 24 98 44
Fax: + 356/21 23 53 00

NĪDERLANDE

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20010
2500 EA Den Haag
Nederland
Telephone: (31-70) 320 44 00
Fax: (31-70) 320 07 33

Ministerie van Defensie

▼M2

Beveiligingsautoriteit (BA)
Postbus 20701
2500 ES Den Haag
Nederland
Telephone: (31-70) 318 70 60
Fax: (31-70) 318 75 22

AUSTRIJA

Informationssicherheitskommission
Bundeskanzleramt
Ballhausplatz 2
A-1014 Wien
Telefon: + 43-1-531 15 23 96
Fax: + 43-1-531 15 25 08

POLIJA

Wojskowe Służby Informacyjne (Military Information Services
National Security Authority – Military Sphere)
PL-00-909 Warszawa 60
Telephone: + 48/22/684 13 62
Fax: + 48/22/684 10 76

Agencja Bezpieczeństwa Wewnętrznego – ABW (Internal Security Agency
National Security Authority – Civilian Sphere
Department for the Protection of Classified Information)
ul. Rakowiecka 2A
PL-00-993 Warszawa
Telephone: + 48/22/585 73 60
Fax: + 48/22/585 85 09

PORTUGĀLE

Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Avenida Ilha da Madeira, 1
P-1400-204 Lisboa
Tel.: (351) 21 301 17 10
Fax: (351) 21 303 17 11

SLOVĒNIJA

Office of the Government of the Republic of Slovenia
For the Protection of Classified Information – NSA
Slovenska cesta 5
SI-1000 Ljubljana
Tel.: (386-1) 426 91 20
Faks: (386-1) 426 91 21

SLOVĀKIJA

Národný bezpečnostný úrad
(National Security Authority)
Budatínska 30
SK-851 05 Bratislava
Telephone: + 421/2/68 69 23 14
Fax: + 421/2/68 69 17 00

SOMIJA

Ulkoasiainministeriö/Utrikesministeriet
Alivaltiosihteeri (Hallinto)/Understatssekreteraren (Administration)
Laivastokatu 22/Maringatan 22
PL/PB 176
FIN-00161 Helsinki/Helsingfors
Telephone: (358-9) 16 05 53 38

▼**M2**

Fax: (358-9) 16 05 53 03

ZVIEDRIJA

Utrikesdepartementet
SSSB
S-103 39 Stockholm
Telephone: + 46/8/405 54 44
Fax: + 46/8/723 11 76

APVIENOTĀ KARALISTE

UK National Security Authority
PO Box 49359
London, SW1P 1LU
United Kingdom
Telephone (44-207) 930 87 68
Fax (44-207) 821 86 04

▼M2

2. papildinājums

Drošības klasifikāciju salīdzinājums

ES un ES dalībvalstu klasifikācija	TRÈS SECRET UE/EU TOP SECRET	SECRET UE	CONFIDENTIEL UE	RESTREINT UE
Euratom	*Eura — Top Secret*	*Eura — Secret*	*Eura — Confidential*	*Eura — Restricted*
Beļģija	Très Secret Zeer geheim	Secret Geheim	Confidentiel Vertrouwelijk	Diffusion restreinte Beperkte verspreiding
Čehija	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Dānija	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Vācija	Streng geheim	Geheim	VS (9) — Vertraulich	VS — Nur für den Dienstgebrauch
Igaunija	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
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 (10)	Secret Défense	Confidentiel Défense	nota (11)
Īrija	Top Secret	Secret	Confidential	Restricted
Itālija	Segretissimo	Segreto	Riservatissimo	Riservato
Kipra	Άκρως Απόρρητο	Απόρρητο	Εμπιστευτικό	Περιορισμένης Χρήσης
Latvija	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Lietuva	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Luksemburga	Très Secret	Secret	Confidentiel	Diffusion restreinte

▼M2

ES un ES dalībvalstu klasifikācija	TRÈS SECRET UE/EU TOP SECRET	SECRET UE	CONFIDENTIEL UE	RESTREINT UE
Ungārija	Szigorúan titkos!	Titkos!	Bizalmas!	Korlátozott terjesztésű!
Malta	L-Ghola Segretezza	Sigriet	Kunfidenzjali	Ristrett
Nīderlande	Zeer geheim	Geheim	Confidentieel	Vertrouwelijk
Austrija	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Polija	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugāle	Muito Secreto	Secreto	Confidencial	Reservado
Slovēnija	Strogo tajno	Tajno	Zaupno	Interno
Slovākija	Prísne tajné	Tajné	Dôverné	Vyhradené
Somija	Erittäin salainen	Erittäin salainen	Salainen	Luottamuksellinen
Zviedrija	Kvalificerat hemlig	Hemlig	Hemlig	Hemlig
Apvienotā Karaliste	Top Secret	Secret	Confidential	Restricted
Starptautisko organizāciju klasifikācija	TRÈS SECRET UE/EU TOP SECRET	SECRET UE	CONFIDENTIEL UE	RESTREINT UE
NATO klasifikācija	COSMIC TOP SECRET	NATO SECRET	NATO CONFIDENTIAL	NATO RESTRICTED
RES klasifikācija	Focal Top Secret	WEU Secret	WEU Confidential	WEU Restricted

([9]) Vācijā: VS = Verschlusssache.
([10]) Francijā: klasifikāciju "Très secret défense", kas attiecas uz valdības prioritārajiem jautājumiem, drīkst mainīt tikai ar premjerministra atļauju.
([11]) Francija savā valsts sistēmā nelieto klasifikācijas kategoriju "DIFFUSION RESTREINTE". Ar dokumentiem, kam ir marķējums "RESTREINT UE" Francija rīkojas un aizsargā tos saskaņā ar saviem spēkā esošajiem valsts normatīvajiem aktiem, kas nav mazāk stingri kā Padomes drošības reglamenta noteikumi.

3. papildinājums

Praktiskās klasifikācijas metodiskais līdzeklis

Šis metodiskais līdzeklis ir uzskatāms par norādošu, un nedrīkst uzskatīt, ka tas maina II un III iedaļā noteiktos būtiskos noteikumus.

Klasifikācija	Kad?	Kas?	Marķējumi	Ierindošana zemākā kategorijā/deklasifikācija/iznīcināšana	
				Kas?	Kad?
ES sevišķi slepeni (*TRÈS SECRET UE/EU TOP SECRET*): Šo klasifikāciju piemēro tikai informācijai un materiālam, kura neatļauta izpaušana var izraisīt ārkārtīgi nopietnu apdraudējumu Eiropas Savienības vai vienas, vai vairāku tās dalībvalstu būtiskām interesēm.	Aktīvu, kas apzīmēti kā ES sevišķi slepeni (*TRÈS SECRET UE/EU TOP SECRET*), apdraudejums: — tieši apdraudētu ES vai vienas tās dalībvalsts, vai draudzīgu valstu iekšējo stabilitāti, — izraisītu ārkārtīgi nopietnu kaitējumu attiecībām ar draudzīgām valdībām, — tieši izraisītu cilvēku bojāeju plašos apmēros, — izraisītu ārkārtīgi nopietnu kaitējumu dalībvalstu vai citu ieguldītāju darbības efektivitātei vai drošībai, vai ārkārtīgi vērtīgu drošības vai izlūkošanas darbību nepārtrauktai efektivitātei, — izraisītu nopietnu ilglaicīgu kaitējumu ES vai dalībvalstu ekonomikai.	Dalībvalstis: attiecīgi pilnvarotas personas (autori) [SIII(4)], Padomes Ģenerālsekretariāts: attiecīgi pilnvarotas personas (autori) [SIII(4)], ģenerālsekretārs/augstais pārstāvis un ģenerālsekretāra vietnieks. Autori precizē dienu vai laika posmu, kad saturu var ierindot zemākā kategorijā vai deklasificēt. Citādi tie pārskata dokumentus vismaz reizi piecos gados, lai pārliecinātos, vai ir nepieciešama sākotnējā klasifikācija [SIII (10)].	Klasifikāciju ES sevišķi slepeni (*TRÈS SECRET UE/EU TOP SECRET*) piemēro ES sevišķi slepeniem (*TRÈS SECRET UE/EU TOP SECRET*) dokumentiem un pēc vajadzības pielieto *ESDP* marķējumu ar mehāniskiem līdzekļiem vai ar roku [SII(8)]. ES klasifikācijas ir redzamas katras lappuses augšējā un apakšējā daļā vidū, un katru lappusi numurē. Uz katra dokumenta ir uzskaites numurs un datums; šis uzskaites numurs ir redzams uz katras lappuses. Ja tie ir jāizplata vairākos eksemplāros, uz katra ir eksemplāra numurs, kurš būs redzams uz pirmās lappuses, līdz ar kopējo lappušu skaitu. Visus pielikumus un pievienojumus uzskaita pirmajā lappusē [SVII(l)].	Deklasificēšana vai ierindošana zemākā kategorijā ir vienīgi autora ziņā, vai ģenerālsekretāra/augstā pārstāvja ziņā, kurš informē par izmaiņām jebkādus turpmākus adresātus, kuriem tie nosūtījuši vai nokopējuši dokumentu [SVIII(9)]. ES sevišķi slepenos (*TRÈS SECRET UE/EU TOP SECRET*) dokumentus iznīcina tikai centrālais reģistrs vai apakšreģistrs, kas par tiem atbild. Katru iznīcināto dokumentu uzskaita iznīcināšanas sertifikātā, kuru paraksta atbildīgais par ES sevišķi slepenās (*TRÈS SECRET UE/EU TOP SECRET*) informācijas kontroli un ierēdnis, kas apliecina iznīcināšanu, kurām ir veikta ES sevišķi slepenā (*TRÈS SECRET UE/EU TOP SECRET*) līmeņa pārbaude. Reģistrācijas žurnālā ieraksta piezīmi par to. Iznīcināšanas sertifikātus līdz ar izplatīšanas dokumentiem uzglabā reģistrā desmit gadus [SVII(31)].	Liekie eksemplāri un dokumenti, kas vairs nav vajadzīgi, ir jāiznīcina [SVII(31)]. ES sevišķi slepenos (*TRÈS SECRET UE/EU TOP SECRET*) dokumentus, tostarp visus klasificētos atkritumus, kas radušies ES sevišķi slepeno (*TRÈS SECRET UE/EU TOP SECRET*) dokumentu sagatavošanas rezultātā, piemēram, bojātus eksemplārus, darba uzmetumus, drukātas piezīmes un koppapīru, iznīcina atbildīgā par ES sevišķi slepeno (*TRÈS SECRET UE/EU TOP SECRET*) informāciju uzraudzībā, sadedzinot, pārvēršot mīkstā masā, sasmalcinot vai citādi pārvēršot neatpazīstamā un neatjaunojamā formā. [SVII(31)].

Klasifikācija	Kad?	Kas?	Marķējumi	Ierindošana zemākā kategorijā/deklasifikācija/iznīcināšana	
				Kas?	Kad?
Slepeni (*SECRET*): Šo klasifikāciju piemēro tikai informācijai un materiālam, kura neatļauta atklāšana varētu nopietni kaitēt Eiropas Savienības vai vienas, vai vairāku tās dalībvalstu būtiskām interesēm [SII(2)].	Aktīvu, kas apzīmēti kā ES slepeni (*SECRET UE*), apdraudējums: — izraisītu starptautisku saspīlējumu, — nopietni kaitētu attiecībām ar draudzīgām valdībām, — tieši apdraudētu cilvēku dzīvību vai nopietni ietekmētu sabiedrisko kārtību vai indivīdu drošību vai brīvību, — izraisītu nopietnu kaitējumu dalībvalstu vai citu ieguldītāju darbības efektivitātei vai drošībai, vai ļoti vērtīgu drošības vai izlūkošanas darbību nepārtrauktai efektivitātei, — izraisītu ļoti būtisku kaitējumu ES vai vienas tās dalībvalsts finansiālajām, monetārajām, ekonomiskajām un komercinteresēm.	Dalībvalstis: pilnvarotas personas (autori) [SIII(2)], Padomes Ģenerālsekretariāts un ES decentralizētās aģentūras: pilnvarotas personas (autori) [SIII(2)], ģenerāldirektori, ģenerālsekretārs/augstais pārstāvis un ģenerālsekretāra vietnieks. Autori precizē dienu vai laika posmu, kad saturu var ierindot zemākā kategorijā vai deklasificēt. Citādi tie pārskata dokumentus vismaz reizi piecos gados, lai pārliecinātos, vai ir nepieciešama sākotnējā klasifikācija [SVII (1)].	Klasifikāciju ES slepeni (*SECRET UE*) piemēro ES slepeniem (*SECRET UE*) dokumentiem un pēc vajadzības ievieš aizsardzības marķējumu — *ESDP*, ar mehāniskiem līdzekļiem vai ar roku [SIII(8)]. ES klasifikācijas ir redzamas katras lappuses augšējā un apakšējā daļā vidū, un katru lappusi numurē. Uz katra dokumenta ir uzskaites numurs un datums; šis uzskaites numurs ir redzams uz katras lappuses. Ja tie ir jāizplata vairākos eksemplāros, uz katra ir eksemplāra numurs, kurš būs redzams uz pirmās lappuses, līdz ar kopējo lappušu skaitu. Visus pielikumus un pievienojumus uzskaita pirmajā lappusē [SVII(l)].	Deklasificēšana un ierindošana zemākā kategorijā ir vienīgi autora ziņā, vai ģenerālsekretāra/augstā pārstāvja ziņā, kurš informē par izmaiņām jebkādus turpmākus adresātus, kuriem tie nosūtījuši vai nokopējuši dokumentu [SVII(9)]. ES slepenos (*SECRET UE*) dokumentus iznīcina reģistrs, kas par šiem dokumentiem atbild, personas, kam veikta drošības pārbaude, uzraudzībā. ES slepenos (*SECRET UE*) dokumentus, kurus iznīcina, uzskaita parakstītos iznīcināšanas sertifikātos, kas līdz ar iznīcināšanas dokumentiem jāsaglabā reģistrā vismaz trīs gadus [SVII(32)].	Liekie eksemplāri un dokumenti, kas vairs nav vajadzīgi, ir jāiznīcina [SVII(31)]. ES slepenos (SECRET UE) dokumentus, tostarp visus klasificētos atkritumus, kas radušies ES slepeno (*SECRET UE*) dokumentu sagatavošanas rezultātā, piemēram, bojātus eksemplārus, darba uzmetumus, drukātas piezīmes un koppapīru, iznīcina sadedzinot, pārvēršot mīkstā masā, sasmalcinot vai citādi pārvēršot neatpazīstamā un neatjaunojamā formā [SVII (31), (32)].

Klasifikācija	Kad?	Kas?	Marķējumi	Ierindošana zemākā kategorijā/deklasifikācija/iznīcināšana	
				Kas?	Kad?
ES konfidenciāli (*CONFIDENTIEL UE*): Šo klasifikāciju piemēro informācijai un materiālam, kura neatļauta izpaušana varētu kaitēt Eiropas Savienības vai vienas, vai vairāku tās dalībvalstu būtiskām interesēm [SII(3)].	Aktīvu, kas apzīmēti kā ES konfidenciāli (*CONFIDENTIEL UE*), apdraudējums: — ievērojami kaitētu diplomātiskām attiecībām, tas ir, izraisītu oficiālu protestu vai citas sankcijas, — ierobežotu indivīdu drošību vai brīvību, — izraisītu kaitējumu dalībvalstu vai citu ieguldītāju darbības efektivitātei vai drošībai, vai vērtīgu drošības vai izlūkošanas darbību efektivitātei, — ievērojami apdraudētu galveno organizāciju finansiālo dzīvotspēju, — kavētu izmeklēšanu vai atvieglotu smagu noziegumu izdarīšanu, — būtiski darbotos pret ES vai dalībvalstu finansiālajām, monetārajām, ekonomiskajām un komercinteresēm, — nopietni kavētu galveno ES politiku izstrādi vai darbību, — noslēgtu vai citādi būtiski pārtrauktu ievērojamas ES darbības.	Dalībvalstis: pilnvarotas personas (autori) [SIII(2)], Padomes Ģenerālsekretariāts un ES decentralizētās aģentūras: pilnvarotas personas (autori) [SIII(2)], ģenerāldirektori, ģenerālsekretārs/augstais pārstāvis un ģenerālsekretāra vietnieks. Autori precizē dienu vai laika posmu, kad saturu var ierindot zemākā kategorijā vai deklasificēt. Citādi tie pārskata dokumentus vismaz reizi piecos gados, lai pārliecinātos, vai ir nepieciešama sākotnējā klasifikācija [SIII (10)].	Klasifikāciju ES konfidenciāli (*CONFIDENTIEL UE*) piemēro ES konfidenciāliem (*CONFIDENTIEL UE*) dokumentiem un pēc vajadzības ievieš aizsardzības marķējumu — *ESDP*, ar mehāniskiem līdzekļiem vai ar roku, vai uzspiežot uz iepriekš iespiesta, reģistrēta papīra [SII(8)]. ES klasifikācijas ir redzamas katras lappuses augšējā un apakšējā daļā vidū, un katru lappusi numurē. Uz katra dokumenta ir uzskaites numurs un datums. Visus pielikumus un pievienojumus uzskaita pirmajā lappusē [SVII(l)].	Deklasificēšana un ierindošana zemākā kategorijā ir vienīgi autora ziņā, vai ģenerālsekretāra/augstā pārstāvja ziņā, kurš informē par izmaiņām jebkādus turpmākus adresātus, kuriem tie nosūtījuši vai nokopējuši dokumentu [SVII(31)]. ES konfidenciālos (*CONFIDENTIEL UE*) dokumentus iznīcina reģistrs, kas par šiem dokumentiem atbild, personas, kam veikta drošības pārbaude, uzraudzībā. To iznīcināšanu reģistrē saskaņā ar valsts tiesību aktiem un, Padomes Ģenerālsekretariāta vai ES decentralizēto aģentūru gadījumā, saskaņā ar Ģenerālsekretāra/Augstā pārstāvja vai Ģenerālsekretāra vietnieka norādījumiem [SVII(33)].	Liekie eksemplāri un dokumenti, kas vairs nav vajadzīgi, ir jāiznīcina [SVII(31)]. ES konfidenciālos (*CONFIDENTIEL UE*) dokumentus, tostarp visus klasificētos atkritumus, kas radušies ES konfidenciālo (*CONFIDENTIEL UE*) dokumentu sagatavošanas rezultātā, piemēram, bojātus eksemplārus, darba uzmetumus, drukātas piezīmes un koppapīru, iznīcina sadedzinot, pārvēršot mīkstā masā, sasmalcinot vai citādi pārvēršot neatpazīstamā un neatjaunojamā formā [SVII (31), (33)].

▼B

Klasifikācija	Kad?	Kas?	Marķējumi	Ierindošana zemākā kategorijā/deklasifikācija/iznīcināšana	
				Kas?	Kad?
ES ierobežotas pieejamības (*RESTREINT UE*): Šo klasifikāciju piemēro informācijai un materiālam, kura neatļauta izpaušana varētu būt neizdevīga ES vai vienas, vai vairāku tās dalībvalstu interesēm [SII(4)].	Aktīvu, kas apzīmēti kā ES ierobežotas pieejamības (*RESTREINT UE*), apdraudējums: — negatīvi ietekmētu diplomātiskās attiecības, — radītu pamatīgas briesmas indivīdiem, — apgrūtinātu dalībvalstu un citu ieguldītāju darbības efektivitātes vai drošības saglabāšanu, — izraisītu finansiālus zaudējumus vai atvieglotu nelikumīgus ieguvumus vai izdevīgumu indivīdiem un uzņēmumiem, — pārkāptu saistības saglabāt trešo pušu sniegtas informācijas konfidencialitāti, — pārkāptu likumiskus informācijas izpaušanas ierobežojumus, — kavētu izmeklēšanu vai atvieglotu noziegumu izdarīšanu, — radītu neizdevīgus apstākļus ES vai dalībvalstīm tirdzniecības vai politiskās sarunās ar citiem, — kavētu ES politiku efektīvu izstrādi vai darbību, — grautu pienācīgu ES un tās darbību vadību.	Dalībvalstis: pilnvarotas personas (autori) [SIII(2)], Padomes Ģenerālsekretariāts un ES decentralizētās aģentūras: pilnvarotas personas (autori) [SIII(2)], ģenerāldirektori, ģenerālsekretārs/augstais pārstāvis un ģenerālsekretāra vietnieks. Autori precizē dienu vai laika posmu, kad saturu var ierindot zemākā kategorijā vai deklasificēt. Citādi tie pārskata dokumentus vismaz reizi piecos gados, lai pārliecinātos, vai ir nepieciešama sākotnējā klasifikācija [SIII (10)].	Klasifikāciju ES ierobežotas pieejamības (*RESTREINT UE*) piemēro ES ierobežotas pieejamības (*RESTREINT UE*) dokumentiem un pēc vajadzības ievieš aizsardzības marķējumu — *ESDP*, ar mehāniskiem vai elektroniskiem līdzekļiem [SIII(8)]. ES klasifikācijas ir redzamas katras lappuses augšējā un apakšējā daļā vidū, un katru lappusi numurē. Uz katra dokumenta ir uzskaites numurs un datums [SVII(l)].	Deklasificēšana un ierindošana zemākā kategorijā ir vienīgi autora ziņā, vai ģenerālsekretāra/augstā pārstāvja ziņā, kurš informē par izmaiņām jebkādus turpmākus adresātus, kuriem tie nosūtījuši vai nokopējuši dokumentu [SIII(9)]. ES ierobežotas pieejamības (RESTREINT UE) dokumentus iznīcina reģistrs, kas atbild par šiem dokumentiem, vai lietotājs, saskaņā ar valsts tiesību aktiem un, Padomes Ģenerālsekretariāta vai ES decentralizēto aģentūru gadījumā, saskaņā ar ģenerālsekretāra/augstā pārstāvja ģenerālsekretāra vietnieka norādījumiem [SVII(34)].	Liekie eksemplāri un dokumenti, kas vairs nav vajadzīgi, ir jāiznīcina [SVII(31)].

▼B

4. papildinājums

Pamatnostādnes ES klasificētās informācijas nodošanai trešām valstīm un starptautiskām organizācijām

1 . līmeņa sadarbība

PROCEDŪRAS

1. Padomes ziņā ir lemt par atļauju nodot ES klasificēto informāciju valstīm, kas nav Līguma par Eiropas Savienību parakstītājas, vai citām starptautiskām organizācijām, kuru drošības politika un reglaments ir salīdzināmi ar ES drošības politiku un reglamentu.

2. Padome var deleģēt lēmumu nodot klasificēto informāciju. Deleģējumā nosaka nododamās informācijas raksturu un tās klasifikācijas līmeni, kas parasti nav augstāks par ES konfidenciālo (*CONFIDENTIEL UE*).

3. Pēc drošības nolīguma noslēgšanas attiecīgo valstu vai starptautisko organizāciju drošības institūcijas iesniegs ģenerālsekretāram/augstajam pārstāvim pieprasījumus nodos tām ES klasificēto informāciju, kuros norāda šīs nodošanas mērķus un nododamās klasificētās informācijas raksturu.

   Pieprasījumus attiecībā uz ES klasificētās informācijas nodošanu var iesniegt arī dalībvalsts vai ES decentralizētā aģentūra; tās norādīs šādas nodošanas mērķus un labumu ES, precizējot nododamās informācijas raksturu un klasifikāciju.

4. Pieprasījumu izskatīs Padomes Ģenerālsekretariāts, kurš:

   — lūdz attiecīgi dalībvalsts vai decentralizētās ES aģentūras, kas ir nododamās informācijas autori, atzinumu,

   — nodibina vajadzīgos sakarus ar saņēmēju valstu vai starptautisko organizāciju drošības iestādēm, lai pārbaudītu, vai to drošības politika un reglaments ir tādi, kas garantētu nodotās klasificētās informācijas aizsardzību saskaņā ar šo drošības reglamentu,

   — lūdz dalībvalstu Valsts drošības iestāžu tehniskos atzinumus par saņēmēju valstu vai starptautisko institūciju uzticamību.

5. Padomes Ģenerālsekretariāts nosūtīs pieprasījumu un Drošības biroja ieteikumu Padomei lēmuma pieņemšanai.

DROŠĪBAS REGLAMENTS, KAS JĀPIEMĒRO SAŅĒMĒJIEM

6. Ģenerālsekretārs/augstais pārstāvis paziņos saņēmējām valstīm vai starptautiskajām organizācijām par Padomes lēmumu atļaut ES klasificētās informācijas nodošanu, nosūtot tik daudzus šā drošības reglamenta eksemplārus, cik uzskata par nepieciešamu. Ja pieprasījumu iesniegusi dalībvalsts, šī valsts paziņos saņēmējam par nodošanas atļauju.

   Lēmums par nodošanu stāsies spēkā tikai tad, kad saņēmēji ir devuši rakstisku garantiju, ka viņi:

   — neizmantos informāciju citiem mērķiem, kā vien tiem, par ko ir vienošanās,

   — aizsargās informāciju saskaņā ar šo drošības reglamentu un jo īpaši tālāk izklāstītajiem īpašajiem noteikumiem.

7. *Personāls*

   a) Ierēdņu skaits, kam ir piekļuve ES klasificētajai informācijai, būs stingri ierobežots, pamatojoties uz vajadzības pēc informācijas principu, līdz tām personām, kuru pienākumu pildīšanai nepieciešama šāda piekļuve;

   b) visiem ierēdņiem, kuriem dota piekļuve informācijai, kas klasificēta kā ES konfidenciālā (*CONFIDENTIEL UE*) vai augstāk, ir vai nu attiecīga līmeņa drošības sertifikāts, vai līdzvērtīgs drošības pārbaudes apliecinājums, ko izsniegusi viņu pašu valsts valdība.

▼B

8. *Dokumentu nosūtīšana*

a) Lēmumu par dokumentu nosūtīšanas praktisko procedūras pieņems pēc vienošanās, pamatojoties uz Padomes Drošības reglamenta VII iedaļas noteikumiem. Tajās īpaši precizēs reģistrus, uz kādiem jānosūta ES klasificētā informācija;

b) ja klasificētā informācija, kuru Padome ir atļāvusi nodot, ietver ES sevišķi slepeno (*TRÈS SECRET UE/EU TOP SECRET*) informāciju, saņēmēja valsts vai starptautiskā organizācija izveido centrālo ES reģistru un, pēc vajadzības, ES apakšreģistrus. Uz šiem reģistriem attieksies šā drošības reglamenta VIII iedaļas noteikumi.

9. *Reģistrācija*

Tiklīdz reģistrs saņem ES dokumentu, kas klasificēts kā ES konfidenciāls (*CONFIDENTIEL UE*) vai augstāk, tas iegrāmatos šo dokumentu īpašā organizācijas reģistrā, kurā ir ailes saņemšanas dienai, ziņām par dokumentu (datums, uzskaites un eksemplāra numurs), tā klasifikācijai, nosaukumam, saņēmēja vārdam, uzvārdam un amatam, saņemšanas dokumenta atdošanas dienai un dienai, kad dokumentu nosūta atpakaļ ES autoram vai iznīcina.

10. *Iznīcināšana*

a) ES klasificētos dokumentus iznīcinās saskaņā ar norādījumiem, kas izklāstīti šā drošības reglamenta VI iedaļā. ES slepeno (*SECRET UE*) un ES sevišķi slepeno (*TRÈS SECRET UE/EU TOP SECRET*) dokumentu iznīcināšanas sertifikātu kopijas nosūta ES reģistram, kas sūtījis dokumentus;

b) ES klasificētos dokumentus iekļaus pašu saņēmēju institūciju klasificēto dokumentu ārkārtas iznīcināšanas plānos.

11. *Dokumentu aizsardzība*

Tiks veikti visi pasākumi, lai novērstu nepiederošu personu piekļuvi ES klasificētajai informācijai.

12. *Kopijas, tulkojumi, izraksti*

Dokumentam, kas klasificēts kā ES konfidenciālais (*CONFIDENTIEL UE*) vai ES slepenais (*SECRET UE*), nedrīkst izgatavot fotokopijas vai tulkojumu, vai izrakstus no šāda dokumenta bez attiecīgās drošības organizācijas vadītāja atļaujas, kurš reģistrēs un pārbaudīs šīs kopijas, tulkojumus vai izrakstus un pēc vajadzības apzīmogos.

ES sevišķi slepena (*TRÈS SECRET UE/EU TOP SECRET*) dokumenta pārpublicēšanu vai tulkošanu drīkst atļaut tikai izcelsmes iestāde, kura precizēs atļauto kopiju skaitu; ja izcelsmes iestādi nevar noteikt, pieprasījumu nosūtīs Padomes Ģenerālsekretariāta Drošības birojam.

13. *Drošības pārkāpumi*

Ja ir noticis drošības pārkāpums attiecībā uz ES klasificētu dokumentu vai ir aizdomas par šādu pārkāpumu, pēc drošības nolīguma noslēgšanas nekavējoties jāveic šādas darbības:

a) veic izmeklēšanu, lai konstatētu drošības pārkāpuma apstākļus;

b) informē Padomes Ģenerālsekretariāta Drošības dienestu, Valsts drošības iestādi un izcelsmes iestādi, vai arī skaidri dara zināmu, ka pēdējai nav paziņots, ja tas nav izdarīts;

c) veic pasākumus, lai mazinātu drošības pārkāpuma sekas;

d) pārskata un īsteno pasākumus, lai novērstu visus atkārtotus pārkāpumus;

e) īsteno visus Padomes Ģenerālsekretariāta Drošības biroja ieteiktus pasākumus, lai novērstu atkārtotus pārkāpumus.

14. *Pārbaudes*

Padomes Ģenerālsekretariāta Drošības birojam ar attiecīgo valstu vai starptautisko organizāciju piekrišanu atļaus veikt nodotās ES klasificētās informācijas aizsardzības pasākumu efektivitātes novērtējumu.

▼B

15. *Ziņojumu sagatavošana*

Saskaņā ar drošības nolīgumu, kamēr valsts vai starptautiskas organizācijas rīcībā glabājas ES klasificētā informācija, tai reizi gadā jāiesniedz ziņojums dienā, ko precizē, dodot atļauju informācijas nodošanai, — apstiprinot, ka ir ticis ievērots šis drošības reglaments.

▼B

5. papildinājums

Pamatnostādnes ES klasificētās informācijas nodošanai trešām valstīm un starptautiskām organizācijām

2 . līmeņa sadarbība

PROCEDŪRAS

1. Padomei ir tiesības nodot ES klasificēto informāciju trešām valstīm vai starptautiskām organizācijām, kuru drošības politika un reglaments ievērojami atšķiras no ES drošības politikas un reglamenta. Principā tas attiecas uz informāciju, kas klasificēta līdz ES slepenai (*SECRET UE*), to ieskaitot; netiek ietverta attiecīgās valsts informācija, kas īpaši paredzēta dalībvalstīm, un ES klasificētās informācijas kategorijas, kas aizsargātas ar īpašiem marķējumiem.

2. Padome var deleģēt lēmuma pieņemšanu: deleģējumā tā, ievērojot 1. punktā noteiktos ierobežojumus, nosaka informācijas, kuru drīkst nodot, raksturu un klasifikācijas līmeni, kas nebūs augstāks kā ES ierobežotas pieejamības (*RESTREINT UE*).

3. Ievērojot noslēgto drošības nolīgumu, attiecīgo valstu vai starptautisko organizāciju drošības institūcijas iesniedz ģenerālsekretāram/augstajam pārstāvim pieprasījumus nodot tām ES klasificēto informāciju, kuros norāda šīs nodošanas mērķus un nododamās informācijas raksturu un klasifikāciju.

   Pieprasījumus attiecībā uz ES klasificētās informācijas nodošanu var iesniegt arī dalībvalsts vai ES decentralizētā aģentūra; tās norāda šādas nodošanas mērķus un labumu ES, precizējot nododamās informācijas raksturu un klasifikāciju.

4. Pieprasījumu izskatīs Padomes Ģenerālsekretariāts, kas:

   — lūdz attiecīgi dalībvalsts vai ES decentralizētās aģentūras, kas ir nododamās informācijas autori, atzinumu,

   — iepriekš nodibina sakarus ar saņēmēju valstu vai starptautisko organizāciju drošības iestādēm, lai iegūtu informāciju par to drošības politiku un reglamentu, un jo īpaši sastādītu tabulu, kurā salīdzinātas ES un attiecīgajā valstī vai organizācijā piemērojamās klasifikācijas,

   — organizē Padomes Drošības komitejas sanāksmi vai, ja nepieciešams, slēptā procedūrā noskaidro informāciju no dalībvalstu Valsts drošības iestādēm, lai iegūtu Drošības komitejas tehnisko atzinumu.

5. Padomes Drošības komitejas tehniskais atzinums attieksies uz šādiem jautājumiem:

   — saņēmēju valstu vai starptautisko organizāciju uzticamību, lai novērtētu ES vai dalībvalstīm radītos drošības riskus,

   — saņēmēja spēju aizsargāt ES nodoto klasificēto informāciju,

   — priekšlikumiem attiecībā uz praktiskām procedūrām ES klasificētās informācijas (piemēram, pārstrādātu teksta variantu nodrošināšana) un nosūtāmo dokumentu apstrādei (ES klasifikācijas virsrakstu, īpašo marķējumu u.c. saglabāšana vai svītrošana),

   — izcelsmes iestādes veikto ierindošanu zemākā kategorijā vai deklasificēšanu pirms informācijas nodošanas saņēmējām valstīm vai starptautiskajām organizācijām ([1]).

6. Ģenerālsekretārs/augstais pārstāvis Padomei lēmuma pieņemšanai nosūtīs pieprasījumu un Padomes Drošības komitejas tehnisko atzinumu, ko ieguvis Padomes Ģenerālsekretariāta Drošības birojs.

([1]) Tas nozīmē, ka attiecībā uz visiem eksemplāriem, kas ir apritē ES, izcelsmes iestāde piemēro III iedaļas 9. punktā noteikto procedūru.

▼B

DROŠĪBAS REGLAMENTS, KAS JĀPIEMĒRO SAŅĒMĒJIEM

7. Par Padomes lēmumu atļaut nodot ES klasificēto informāciju saņēmējas valstis vai starptautiskās organizācijas informē Padomes ģenerālsekretārs/augstais pārstāvis, norādot arī uz tabulu, kurā salīdzinātas ES un attiecīgajās valstīs un organizācijās piemērojamās klasifikācijas. Ja pieprasījumu iesniegusi dalībvalsts, šī valsts paziņos saņēmējam par nodošanas atļauju.

   Lēmums par nodošanu stāsies spēkā tikai tad, kad saņēmēji ir devuši rakstisku garantiju, ka viņi:

   — neizmantos informāciju citiem mērķiem, par ko nav panākta vienošanās,

   — aizsargās informāciju saskaņā ar Padomes noteikto reglamentu.

8. Izveidos šādus drošības noteikumus, ja vien Padome pēc Padomes Drošības komitejas tehniskā atzinuma saņemšanas nenolems par konkrētu procedūru ES klasificēto dokumentu apstrādei (svītrojot pieminēto ES klasifikāciju, īpašu marķējumu u.c.).

   Noteikumus šajā gadījumā pielāgos.

9. *Personāls*

   a) Ierēdņu skaits, kam ir piekļuve ES klasificētajai informācijai, ir stingri jāierobežo, pamatojoties uz vajadzības pēc informācijas principu, atļaujot to personām, kuru pienākumu pildīšanai nepieciešama šāda piekļuve;

   b) visiem ierēdņiem vai valstu pilsoņiem, kam ir atļauta piekļuve ES nodotajai klasificētajai informācijai, ir veikta valsts drošības pārbaude vai piešķirta piekļuves atļauja, valsts klasificētās informācijas gadījumā — atbilstošajam līmenim, kas līdzvērtīgs ES līmenim, kā noteikts salīdzināmajā tabulā;

   c) šīs valsts drošības pārbaudes vai atļaujas nosūtīs ģenerālsekretāram/augstajam pārstāvim zināšanai.

10. *Dokumentu nosūtīšana*

   a) Par dokumentu nosūtīšanas praktiskajām procedūrām Padomes Ģenerālsekretariāta Drošības birojs un saņēmēju valstu vai starptautisko organizāciju drošības institūcijas vienosies, pamatojoties uz noteikumiem, kas izklāstīti šā reglamenta VII iedaļā. Jo īpaši norādīs precīzas adreses, uz kurām dokumenti jānosūta, kā arī kurjera vai pasta pakalpojumu, ko izmanto ES klasificētās informācijas nosūtīšanai;

   b) dokumentus, kuri klasificēti kā ES konfidenciālie (*CONFIDENTIEL UE*) un augstāk, nosūtīs dubultaploksnē. Uz iekšējās aploksnes būs marķējums "*UE*" līdz ar drošības klasifikāciju. Katram klasificētajam dokumentam pievienos saņemšanas veidlapu. Saņemšanas veidlapā, kas nebūs klasificēta, norādīs tikai ziņas par dokumentu (tā uzskaites numuru, datumu, eksemplāra numuru) un tā valodu, bet ne nosaukumu;

   c) tad iekšējo aploksni ievietos ārējā aploksnē, uz kuras norādīs iepakojuma numuru saņemšanas uzskaites nolūkos. Uz ārējās aploksnes nenorādīs drošības klasifikāciju;

   d) kurjeriem vienmēr izsniegs saņemšanas dokumentu, uz kura norādīts iepakojuma numurs.

11. *Reģistrācija saņemot*

   Adresāta valsts drošības iestāde vai tai līdzvērtīga iestāde valstī, kura savas valdības vārdā saņem ES nosūtīto klasificēto informāciju, vai saņēmējas starptautiskās organizācijas drošības birojs atvērs īpašu reģistru, lai saņemot reģistrētu ES klasificēto informāciju. Reģistrā būs ietvertas slejas, kurās norāda saņemšanas dienu, ziņas par dokumentu (datums, uzskaites un eksemplāra numurs), tā klasifikāciju, nosaukumu, adresāta vārdu, uzvārdu un amatu, saņemšanas dokumenta atpakaļ nosūtīšanas dienu un dienu, kad dokuments nosūtīts atpakaļ uz ES vai iznīcināts.

12. *Dokumentu atgriešana*

▼B

Kad saņēmējs nosūta atpakaļ klasificētu dokumentu Padomei vai dalībvalstij, kas to nodevusi, tā rīkosies saskaņā ar 10. punktā norādīto procedūru.

13. *Aizsardzība*

a) Ja dokumentus neizmanto, tie tiks uzglabāti seifā, kurš ir apstiprināts valsts līmenī klasificēta tādas pašas klasifikācijas materiāla uzglabāšanai. Uz seifa nebūs norādes par tā saturu, kas būs pieejams tikai personām, kurām ir atļauja apstrādāt ES klasificēto informāciju. Ja izmanto kodu slēdzenes, koda kombinācija būs zināma tikai tiem valsts vai organizācijas ierēdņiem, kuriem ir atļauta piekļuve ES klasificētajam materiālam, kas tiek uzglabāts seifā, un to maina reizi sešos mēnešos, vai ātrāk, ja ierēdņi tiek nomainīti, ja vienam no ierēdņiem, kam zināma kombinācija, atņemta pielaide vai, ja pastāv apdraudējuma risks;

b) ES klasificētos dokumentus no seifa izņems tikai tie ierēdņi, kuri saņēmuši atļauju piekļūt ES klasificētajiem dokumentiem un kuriem ir nepieciešamība pēc informācijas. Viņu atbildība par šo dokumentu glabāšanu seifā saglabāsies tik ilgi, kamēr tie atradīsies viņu pārziņā un, jo īpaši, atbildība par to, lai dokumentiem nepiekļūtu neviena nepiederoša persona. Viņi arī nodrošinās, lai dokumenti glabātos seifā tad, kad tos nelasa, kā arī ārpus darba laika;

c) dokumentam, kas klasificēts kā ES konfidenciāls (*CONFIDENTIEL UE*) un augstāk, nedrīkst izgatavot fotokopijas, nedz izrakstus bez Padomes Ģenerālsekretariāta Drošības biroja atļaujas;

d) jānosaka procedūra dokumentu ātrai un pilnīgai iznīcināšanai ārkārtējā situācijā un tā jāapstiprina Padomes Ģenerālsekretariāta Drošības birojā.

14. *Fiziskā drošība*

a) Seifus, kuros uzglabā ES klasificētos dokumentus, tur aizslēgtus vienmēr, kad tos nelieto;

b) ja personālam, kas veic tīrīšanas un remontdarbus, ir nepieciešams ieiet telpā, kurā atrodas seifi, to vienmēr pavada valsts vai organizācijas drošības dienesta darbinieks vai ierēdnis, kas atbild par telpas drošību;

c) ārpus parastā darba laika (naktī, nedēļas nogalēs un valsts svētku dienās) seifus, kuros atrodas ES klasificētā informācija, apsargā sargs vai automātiska signalizācijas sistēma.

15. *Drošības pārkāpumi*

Ja ir noticis drošības pārkāpums saistībā ar ES klasificētu dokumentu, vai ir aizdomas, ka tāds ir noticis, nekavējoties veic šādus pasākumus:

a) tūlīt nosūta ziņojumu Padomes Ģenerālsekretariāta Drošības birojam vai dalībvalsts valsts drošības iestādei, kura ir ierosinājusi dokumentu nosūtīšanu (ar kopiju Padomes Ģenerālsekretariāta Drošības birojam);

b) veic izmeklēšanu, kuras beigās iesniedz pilnu ziņojumu drošības institūcijai (skatīt a) apakšpunktu iepriekš). Pēc tam jāpieņem vajadzīgie pasākumi, lai labotu stāvokli.

16. *Pārbaudes*

Padomes Ģenerālsekretariāta Drošības birojam ar attiecīgo valstu vai starptautisko organizāciju piekrišanu atļaus veikt nodotās ES klasificētās informācijas aizsardzības pasākumu efektivitātes novērtējumu.

17. *Ziņojumu sagatavošana*

Kamēr valsts vai starptautiskas organizācijas rīcībā glabājas ES klasificētā informācija, tā līdz dienai, ko norāda, dodot atļauju informācijas nodošanai, iesniedz gada pārskatu, apstiprinot, ka ir ievērots šis drošības reglaments.

▼B

6. papildinājums

Pamatnostādnes ES klasificētās informācijas nodošanai trešām valstīm un starptautiskām organizācijām

3 . līmeņa sadarbība

PROCEDŪRAS

1. Laiku pa laikam Padome var vēlēties sadarboties noteiktos īpašos apstākļos ar valstīm vai organizācijām, kas nevar dod šajā drošības reglamentā noteiktās garantijas, taču šai sadarbībai, iespējams, var būt nepieciešama ES klasificētās informācijas nodošana. Šāda nodošana neietvers valsts informāciju, kas īpaši rezervēta dalībvalstīm.

2. Šādos īpašos apstākļos sadarbības pieprasījumus ar ES no trešo valstu vai starptautisku organizāciju puses, vai arī, ja to ierosinājušas dalībvalstis vai, attiecīgā gadījumā, ES decentralizētās aģentūras, vispirms pēc būtības izskatīs Padome, kas vajadzības gadījumā lūgs atzinumu no dalībvalsts vai decentralizētās aģentūras, kura izstrādājusi informāciju. Padome apsvērs, cik saprātīga ir klasificētās informācijas nodošana, novērtēs saņēmēja vajadzību pēc informācijas un pieņems lēmumu, kāda rakstura klasificēto informāciju drīkstētu nosūtīt.

3. Ja Padome piekrīt, ģenerālsekretāra/augstā pārstāvja uzdevums ir sasaukt Padomes Drošības komiteju vai jautāt dalībvalstu valsts drošības iestādēm, ja vajadzīgs, slēptā procedūrā, lai iegūtu Drošības komitejas tehnisko atzinumu.

4. Padomes Drošības komiteja sniedz tehnisko atzinumu par:

   a) ES vai tās dalībvalstīm radīto drošības risku novērtējumu;

   b) attiecīgā gadījumā, informācijas, kuru drīkst nodot, klasifikāciju pēc tās būtības;

   c) informācijas ierindošanu zemākā kategorijā vai deklasificēšanu, ko veic izcelsmes iestāde pirms tās nodošanas attiecīgajām valstīm vai starptautiskām organizācijām ([1]);

   d) nododamo dokumentu apstrādes procedūrām (skatīt tālāk 5. punktu);

   e) iespējamām nosūtīšanas metodēm (sabiedrisko pasta pakalpojumu, publiski pieejamu vai drošu telekomunikāciju sistēmu, diplomātiskā kurjera, kurjeru, kam veikta drošības pārbaude, u.c. izmantošana).

5. Dokumentus, kurus nodod valstīm vai organizācijām, uz kurām attiecas šis papildinājums, principā sagatavos bez atsauces uz avotu vai ES klasifikāciju. Padomes Drošības komiteja var ieteikt:

   — izmantot īpašu marķējumu vai kodu,

   — izmantot īpašu klasifikācijas sistēmu, kas saista informācijas konfidencialitāti ar kontroles pasākumiem, kas nepieciešami saņēmēja dokumentu nosūtīšanas metodēm (skatīt piemērus 14. punktā).

6. Padomes Ģenerālsekretariāta Drošības birojs iesniegs Padomei Drošības komitejas tehnisko atzinumu, vajadzības gadījumā pievienojot ierosināto pilnvaru deleģēšanu uzdevuma izpildei, it īpaši steidzamos apstākļos.

7. Tiklīdz Padome ir apstiprinājusi ES klasificētās informācijas nodošanu un praktiskās īstenošanas procedūras, Padomes Ģenerālsekretariāta Drošības birojs nodibinās vajadzīgos sakarus ar attiecīgās valsts vai organizācijas drošības institūciju, lai atvieglotu paredzēto drošības pasākumu piemērošanu.

8. Padomes Ģenerālsekretariāta Drošības birojs atsaucei visām dalībvalstīm un, vajadzības gadījumā, attiecīgajām ES decentralizētajām aģentūrām nosūta

([1]) Tas nozīmē, ka attiecībā uz visiem eksemplāriem, kas ir apritē ES, izcelsmes iestāde piemēro III iedaļas 9. punktā noteikto procedūru.

▼B

tabulu, kurā apkopots informācijas raksturs un klasifikācija un kurā uzskaitītas organizācijas un valstis, kurām to drīkst nodot pēc Padomes lēmuma.

9. Tās dalībvalsts valsts drošības iestādes, kura nodod informāciju, vai Padomes Ģenerālsekretariāta Drošības birojs veic visus vajadzīgos pasākumus, lai atvieglotu jebkādu turpmāku kaitējuma novērtējumu un procedūru pārskatīšanu.

10. Turpmāku atsauci uz Padomi veiks vienmēr, kad tiks izmainīti sadarbības nosacījumi.

DROŠĪBAS REGLAMENTS, KAS JĀPIEMĒRO SAŅĒMĒJIEM

11. Padomes ģenerālsekretārs/augstais pārstāvis informē saņēmējas valstis vai starptautiskās organizācijas par Padomes lēmumu atļaut nodot ES klasificēto informāciju, iekļaujot arī sīki izstrādātos aizsardzības noteikumus, ko ierosinājusi Padomes Drošības komiteja un apstiprinājusi Padome. Ja pieprasījumu iesniegusi dalībvalsts, šī valsts paziņos saņēmējam par nodošanas atļauju.

    Lēmums stāsies spēkā tikai tad, kad saņēmēji būs devuši rakstisku garantiju, ka viņi:

    — neizmantos informāciju citiem mērķiem, kā vien sadarbībai, par kuru nolēmusi Padome,

    — piedāvās Padomes noteikto informācijas aizsardzību.

12. *Dokumentu nosūtīšana*

    a) Par dokumentu nosūtīšanas praktiskajām procedūrām vienosies Padomes Ģenerālsekretariāta Drošības birojs un Saņēmēju valstu vai starptautisko organizāciju drošības institūcijas. Tās jo īpaši norādīs precīzas adreses, uz kurām jānosūta dokumenti;

    b) dokumentus, kuri klasificēti kā ES konfidenciālie (*CONFIDENTIEL UE*) un augstāk, nosūtīs dubultaploksnē. Uz iekšējās aploksnes atradīsies īpašais ar lēmumu apstiprinātais zīmogs vai kods un būs pieminēta īpašā dokumentam apstiprinātā klasifikācija. Katram klasificētajam dokumentam pievienos saņemšanas veidlapu. Saņemšanas veidlapā, kas nebūs klasificēta, norādīs tikai ziņas par dokumentu (tā uzskaites numuru, datumu, eksemplāra numuru) un tā valodu, bet ne nosaukumu;

    c) tad iekšējo aploksni ievietos ārējā aploksnē, uz kuras norādīs iepakojuma numuru saņemšanas uzskaites nolūkos. Uz ārējās aploksnes nenorādīs drošības klasifikāciju;

    d) kurjeriem vienmēr izsniegs saņemšanas dokumentu, uz kura norādīts iepakojuma numurs.

13. *Reģistrācija saņemot*

    Adresāta valsts drošības iestāde vai tai līdzvērtīga iestāde valstī, kura savas valdības vārdā saņem ES nosūtīto klasificēto informāciju, vai saņēmējas starptautiskās organizācijas drošības birojs atvērs īpašu reģistru, lai reģistrētu ES klasificēto informāciju, to saņemot. Reģistrā būs ietvertas slejas, kurās norāda saņemšanas dienu, ziņas par dokumentu (datums, uzskaites un eksemplāra numurs), tā klasifikāciju, nosaukumu, adresāta vārdu un uzvārdu un amatu, saņemšanas dokumenta atpakaļ nosūtīšanas dienu un dienu, kad saņemšanas dokumentu nosūta atpakaļ uz ES vai iznīcina.

14. *Klasificētās informācijas, ar kuru notiek apmaiņa, izmantošana un aizsardzība*

    a) ES slepenā (*SECRET UE*) līmeņa informāciju apstrādās īpaši izraudzīti ierēdņi, kuriem ir atļauta piekļuve šādi klasificētai informācijai. To glabā labas kvalitātes seifos, kurus var atvērt tikai personas, kurām atļauta piekļuve tajos esošajai informācijai. Zonas, kurās novietoti šie seifi, tiks pastāvīgi apsargātas un tiks izveidota pārbaudes sistēma, lai nodrošinātu, ka tajās var ienākt tikai personas ar atbilstošām atļaujām. ES slepenā (*SECRET UE*) līmeņa informāciju nosūtīs ar diplomātisko kurjeru, ar drošu pasta pakalpojumu un drošu telekomunikāciju palī-

▼B

dzību. ES slepeno (*SECRET UE*) dokumentu drīkst kopēt tikai ar izcelsmes iestādes rakstisku piekrišanu. Visas kopijas reģistrēs un apsekos. Par visām darbībām saistībā ar ES slepenajiem (*SECRET UE*) dokumentiem izsniegs kvītis;

b) ES konfidenciālā (*UE CONFIDENTIEL*) līmeņa informāciju apstrādās atbilstoši izraudzīti ierēdņi, kuriem ir atļauja būt informētām par šo jautājumu. Dokumentus glabās aizslēgtos seifos kontrolētās zonās.

ES konfidenciālā (*CONFIDENTIEL UE*) līmeņa informāciju nosūta ar diplomātisko kurjeru, militārā pasta pakalpojumu un drošu telekomunikāciju palīdzību. Kopijas drīkst izgatavot saņēmēja institūcija, to skaitu un izplatīšanu reģistrē īpašos reģistros;

c) ES ierobežotas pieejamības (*RESTREINT UE*) līmeņa informāciju apstrādās telpās, kuras nav pieejamas nepiederošam personālam, un glabās aizslēgtos seifos. Dokumentus drīkst nosūtīt ar valsts pasta pakalpojumu palīdzību kā reģistrētu pastu dubultaploksnē un, ārkārtējās situācijās operāciju laikā, izmantojot neaizsargātas publiski pieejamas telekomunikāciju sistēmas. Saņēmēji drīkst izgatavot kopijas;

d) neklasificētai informācijai netiks prasīti īpaši aizsardzības pasākumi un to drīkstēs nosūtīt pa pastu un izmantojot publiski pieejamas telekomunikāciju sistēmas. Adresāti drīkst izgatavot kopijas.

15. *Iznīcināšana*

Dokumenti, kuri vairs nav vajadzīgi, ir jāiznīcina. ES ierobežotas pieejamības (*RESTREINT UE*) un ES konfidenciālā (*CONFIDENTIEL UE*) līmeņa dokumentu gadījumā īpašajos reģistros ievadīs atbilstošu piezīmi. ES slepenā (*SECRET UE*) līmeņa dokumentu gadījumā izdos iznīcināšanas sertifikātus, kurus parakstījušas personas, kas apliecina to iznīcināšanu.

16. *Drošības pārkāpumi*

Ja tiek apdraudēta ES konfidenciālā (*CONFIDENTIEL UE*) vai ES slepenā (*SECRET UE*) līmeņa informācija, vai ja ir aizdomas par šādu apdraudējumu, valsts drošības iestāde vai drošības dienesta vadītājs organizācijā veiks apdraudējuma apstākļu izmeklēšanu. Ja izmeklēšanas rezultāti būs pozitīvi, par to paziņos izcelsmes iestādei. Tiks veikti vajadzīgie pasākumi, lai labotu neatbilstošas procedūras vai glabāšanas metodes, ja tās ir bijušas apdraudējuma pamatā. Padomes ģenerālsekretārs/augstais pārstāvis vai tās dalībvalsts valsts drošības iestāde, kas nodevusi apdraudēto informāciju, izmeklēšanā drīkst lūgt saņēmējam sniegt sīkākas ziņas.