►**B**

# KOMISIJAS LĒMUMS

**(2001. gada 29. novembris),**

**ar ko groza tās iekšējo reglamentu**

*(izziņots ar dokumenta numuru C(2001) 3031)*

(2001/844/EK, EOTK, *Euratom*)

(OV L 317, 3.12.2001, lpp. 1)

Grozīts ar:

| | | Oficiālais Vēstnesis | | |
|---|---|---|---|---|
| | | Nr. | Lappuse | Datums |
| ►**M1** | Komisijas Lēmums 2005/94/EK, Euratom (2005. gada 3. februāris) | L 31 | 66 | 4.2.2005 |
| ►**M2** | Komisijas Lēmums 2006/70/EK, Euratom (2006. gada 31. janvāris) | L 34 | 32 | 7.2.2006 |
| ►**M3** | Komisijas Lēmums 2006/548/EK, Euratom (2006. gada 2. augusts) | L 215 | 38 | 5.8.2006 |

▼B

# KOMISIJAS LĒMUMS

**(2001. gada 29. novembris),**

**ar ko groza tās iekšējo reglamentu**

*(izziņots ar dokumenta numuru C(2001) 3031)*

**(2001/844/EK, EOTK, *Euratom*)**

EIROPAS KOPIENU KOMISIJA,

ņemot vērā Eiropas Kopienas dibināšanas līgumu, un jo īpaši tā 218. panta 2. punktu,

ņemot vērā Eiropas Ogļu un tērauda kopienas dibināšanas līgumu, un jo īpaši tā 16. pantu,

ņemot vērā Eiropas Atomenerģijas kopienas dibināšanas līgumu, un jo īpaši tā 131. pantu,

ņemot vērā Līgumu par Eiropas Savienību, un jo īpaši tā 28. panta 1. punktu un 41. panta 1. punktu,

IR PIEŅĒMUSI ŠO LĒMUMU.

*1. pants*

Ar šo Komisijas drošības noteikumus, kuru teksts ir pievienots šim lēmumam, pievieno Komisijas reglamentam kā pielikumu.

*2. pants*

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

To piemēro no 2001. gada 1. decembra.

▼B

*PIELIKUMS*

**KOMISIJAS DROŠĪBAS NOTEIKUMI**

Tā kā:

1) lai attīstītu Komisijas darbības jomās, kam jāpiešķir konfidencialitāte, ir lietderīgi izveidot vispārēju nodrošinājuma sistēmu, ko piemēro Komisijai, citām iestādēm, struktūrām, birojiem un aģentūrām, kas ir izveidotas saskaņā ar EK līgumu vai Līgumu par Eiropas Savienību vai pamatojoties uz tiem, dalībvalstīm un jebkuram citam Eiropas Savienības klasificētas informācijas saņēmējam, še turpmāk — "ES klasificētā informācija";

2) lai nodrošinātu šādi izveidotu nodrošinājuma sistēmu efektivitāti, Komisija dara zināmu ES klasificēto informāciju tikai tām ārpuskopienas struktūrām, kas sniedz garantijas, ka ir veikušas visus nepieciešamos pasākumus, lai piemērotu nosacījumus, kuri pilnīgi atbilst šiem noteikumiem;

3) šos noteikumus pieņem, neierobežojot Padomes Regulu (*Euratom*) Nr. 3 (1958. gada 31. jūlijs), ar ko īsteno Eiropas Atomenerģijas kopienas dibināšanas līguma 24. pantu ([1]), Padomes Regulu (EEK, *Euratom*) Nr. 1588/90 (1990. gada 11. jūnijs) par tādas statistikas informācijas nosūtīšanu Eiropas Kopienu Statistikas birojam, uz kuru attiecas konfidencialitāte ([2]), un Komisijas 1995. gada 23. novembra Galīgo lēmumu C (95) 1510 par informācijas sistēmu aizsardzību;

4) Komisijas drošības sistēma pamatota ar principiem, kuri ir izklāstīti Padomes Lēmumā 2001/264/EK (2001. gada 19. maijs), ar ko pieņem Padomes drošības reglamentu ([3]), lai nodrošinātu Savienības lēmumu pieņemšanas procesa vienmērīgu darbību;

5) Komisija uzsver to, cik svarīgi ir attiecīgā gadījumā saistīt citas iestādes ar konfidencialitātes noteikumiem un standartiem, kas ir vajadzīgi, lai aizsargātu Savienības un tās dalībvalstu intereses;

6) Komisija atzīst nepieciešamību izveidot savu drošības jēdzienu, ņemot vērā visus drošības elementus un Komisijas kā iestādes īpašo raksturu;

7) šos noteikumus pieņem, neierobežojot Līguma 255. pantu un Eiropas Parlamenta un Padomes Regulu (EK) Nr. 1049/2001 (2001 gada 30. maijs) par publisku piekļuvi Eiropas Parlamenta, Padomes un Komisijas dokumentiem ([4]);

▼M2

(8) Šie noteikumi neskar Līguma 286. pantu un Eiropas Parlamenta un Padomes 2000. gada 18. decembra Regulu (EK) Nr. 45/2001 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Kopienas iestādēs un struktūrās, kā arī par šādu datu brīvu apriti.

▼B

*1. pants*

Komisijas noteikumi par drošību ir izklāstīti pielikumā.

*2. pants*

1. Komisijas loceklis, kas atbild par drošības jautājumiem, veic nepieciešamos pasākumus, lai nodrošinātu to, ka ES klasificētās informācijas apstrādē Komisijā un visās Komisijas telpās, tostarp tās pārstāv-

([1]) OV 17/58, 6.10.1958., 406/58. lpp.
([2]) OV L 151, 15.6.1990., 1. lpp.
([3]) OV L 101, 11.4.2001., 1. lpp.
([4]) OV L 145, 31.5.2001., 43. lpp.

▼B

niecības un birojus Savienībā un tās delegācijas trešajās valstīs, Komisijas ierēdņi un citi darbinieki, darbam Komisijā norīkotais personāls, kā arī ārpus Komisijas esošie līgumdarbinieki ievēro 1. pantā minētos noteikumus.

▼M3

Ja līgumā vai subsīdiju līgumā starp Komisiju un ārpus Komisijas esošu līgumdarbinieku vai subsīdijas saņēmēju ir paredzēta ES klasificētās informācijas apstrāde līgumdarbinieka vai saņēmēja telpās, minētā ārpus Komisijas esošā līgumslēdzēja vai saņēmēja veicamajiem pasākumiem, lai nodrošinātu 1. pantā minēto noteikumu ievērošanu, apstrādājot ES klasificēto informāciju, ir jābūt iekļautiem līgumā vai subsīdiju līgumā.

▼B

2. Dalībvalstīm, citām iestādēm, struktūrām, birojiem un aģentūrām, kas ir izveidotas atbilstoši Līgumiem vai pamatojoties uz tiem, ir atļauts saņemt ES klasificēto informāciju, ja tās nodrošina, ka ES klasificētās informācijas apstrādē to personāls ievēro un to telpās tiek ievēroti noteikumi, kuri pilnīgi atbilst 1. pantā minētajiem, jo īpaši:

a) dalībvalstu pastāvīgo pārstāvniecību Eiropas Savienībā locekļi, kā arī valsts delegāciju locekļi, kas apmeklē Komisijas vai tās struktūru sanāksmes vai piedalās citās Komisijas darbībās;

b) citi dalībvalstu administrāciju locekļi, kas apstrādā ES klasificēto informāciju, neatkarīgi no tā, vai tie strādā dalībvalsts teritorijā vai ārzemēs;

c) ārpus Komisijas esošie līgumdarbinieki un norīkotie darbinieki, kas apstrādā ES klasificēto informāciju.

*3. pants*

Trešām valstīm, starptautiskām organizācijām un citām struktūrām ir atļauts saņemt ES klasificēto informāciju, ja tās nodrošina to, ka šādas informācijas apstrādē tiek ievēroti noteikumi, kas atbilst 1. pantā minētajiem.

*4. pants*

Ievērojot drošības pamatprincipus un minimālos standartus, kuri ir izklāstīti pielikuma I daļā, Komisijas loceklis, kas atbild par drošības jautājumiem, drīkst veikt pasākumus saskaņā ar pielikuma II daļu.

*5. pants*

No piemērošanas datuma, šie noteikumi aizstāj:

a) Komisijas 1994. gada 30. novembra Lēmumu C(94) 3282 par drošības pasākumiem, ko piemēro klasificētai informācijai, kuru sagatavo vai nosūta saistībā ar Eiropas Savienības darbībām;

b) Komisijas 1999. gada 25. februāra Lēmumu C (99) 423 par procedūru, sakarā ar kuru Eiropas Komisijas ierēdņiem un citiem darbiniekiem var sniegt piekļuvi klasificētai informācijai, kas ir Komisijas rīcībā.

*6. pants*

No šo noteikumu piemērošanas datuma visu klasificēto informāciju, kas līdz šim datumam ir atradusies Komisijas rīcībā, izņemot Eiropas Atomenerģijas kopienas slepeno informāciju:

▼B

a) ja to ir sagatavojusi Komisija, uzskata par pārklasificētu kā " ►M1 RESTREINT UE ◄" pēc konfidencialitātes pakāpes, ja vien tās autors līdz 2002. gada 31. janvārim nepiešķir tai citu klasifikāciju. Šādos gadījumos autors informē visus attiecīgā dokumenta adresātus;

b) ja to ir sagatavojuši ārpus Komisijas esoši autori, saglabā tās sākotnējo klasifikāciju un tādējādi to uzskata par līdzvērtīga līmeņa ES klasificēto informāciju, ja vien autors piekrīt informāciju deklasificēt vai pazemināt tās slepenības pakāpi.

▼B

*PIELIKUMS*

**NOTEIKUMI PAR DROŠĪBU**

**Saturs**

▼B

17.2. **Klasifikācijas piemērošana**

17.3. **Slepenības pakāpes pazemināšana un deklasificēšana**

18. FIZISKĀ DROŠĪBA

18.1. **Vispārīgi**

18.2. **Drošības prasības**

18.3. **Fiziskās drošības pasākumi**

18.3.1. *Drošības zonas*

18.3.2. *Administratīvā zona*

18.3.3. *Kontrole caurlaides punktos*

18.3.4. *Sargu posteņi*

18.3.5. *Drošības tvertnes un seifi*

18.3.6. *Slēdzenes*

18.3.7. *Atslēgu un kodu kombināciju kontrole*

18.3.8. *Ielaušanās detektori*

18.3.9. *Atļautais aprīkojums*

18.3.10. *Kopējamo mašīnu un telefaksu aizsardzība*

18.4. **Aizsardzība pret slēptu novērošanu un slepenu noklausīšanos**

18.4.1. *Slēpta novērošana*

18.4.2. *Slepena noklausīšanās*

18.4.3. *Elektroniskās un ieraksta aparatūras ieviešana*

18.5. **Tehniski drošas zonas**

19. VISPĀRĒJI NOTEIKUMI PAR NEPIECIEŠAMĪBU ZINĀT PRINCIPU UN DROŠĪBAS PIELAIDES IZSNIEGŠANU ES PERSONĀLAM

19.1. **Vispārīgi**

19.2. **Īpaši noteikumi par TRES SECRET UE/EU TOP SECRET informāciju**

19.3. **Īpaši noteikumi par piekļuvi SECRET UE un CONFIDENTIEL UE informācijai**

19.4. **Īpaši noteikumi par piekļuvi RESTREINT UEinformācijai**

19.5. **Pārcelšana citā amatā**

19.6. **Īpašas norādes**

20. DROŠĪBAS PIELAIDES IZSNIEGŠANAS PROCEDŪRA KOMISIJAS IERĒDŅIEM UN CITIEM DARBINIEKIEM

21. ES KLASIFICĒTU DOKUMENTU SAGATAVOŠANA, IZPLATĪŠANA, PĀRSŪTĪŠANA, KURJERU PERSONISKĀ DROŠĪBA UN PAPILDUS KOPIJAS VAI TULKOJUMI, KĀ ARĪ IZVILKUMI

21.1. **Sagatavošana**

21.2. **Izplatīšana**

21.3. **ES klasificētas informācijas pārsūtīšana**

21.3.1. *Iesaiņošana, paziņojumi par saņemšanu*

21.3.2. *Pārsūtīšana ēkas vai ēku grupas iekšienē*

21.3.3. *Pārsūtīšana pa valsti*

21.3.4. *Pārsūtīšana no vienas valsts uz otru*

21.3.5. *ES ierobežotai lietošanai dokumentu pārsūtīšana*

21.4. **Kurjerpasta darbinieku drošība**

21.5. **Tehniskās pārsūtīšanas elektroniskie un citi veidi**

21.6. **Papildu kopijas un tulkojumi, kā arī izvilkumi no ES klasificētas informācijas**

22. EUCI REĢISTRI, APVIENOŠANAS, PĀRBAUDES, ARHĪVU GLABĀŠANA UN EUCI IZNĪCINĀŠANA

▼B

22.1. *Vietējie EUCI reģistri*

22.2. **TRES SECRET UE/EU TOP SECRET informācijas reģistrs**

22.2.1. *Vispārīgi*

22.2.2. *Centrālais TRES SECRET UE/EU TOP SECRET informācijas reģistrs*

22.2.3. *TRES SECRET UE/EU TOP SECRET informācijas apakšreģistri*

22.3. **ES klasificētu dokumentu uzskaitījumi, apvienošanas un pārbaudes**

22.4. **ES klasificētu dokumentu uzglabāšana arhīvos**

22.5. **ES klasificētu dokumentu iznīcināšana**

22.6. **Iznīcināšana ārkārtas gadījumos**

23. DROŠĪBAS PASĀKUMI ĪPAŠĀS SANĀKSMĒS, KAS NOTIEK ĀRPUS KOMISIJAS TELPĀM UN KURĀS IR IESAISTĪTA ES KLASIFICĒTA INFORMĀCIJA

23.1. **Vispārīgi**

23.2. **Pienākumi**

23.2.1. ► **M2** Komisijas Drošības direktorāts ◄

23.2.2. *Sanāksmes drošības speciālists (MSO)*

23.3. **Drošības pasākumi**

23.3.1. *Drošības zonas*

23.3.2. *Caurlaides*

23.3.3. *Foto un audio aprīkojuma kontrole*

23.3.4. *Portfeļu, pārnēsājamo datoru un iepakojumu pārbaude*

23.3.5. *Tehniskā drošība*

23.3.6. *Delegācijas dokumenti*

23.3.7. *Dokumentu uzglabāšana seifos*

23.3.8. *Biroju pārbaude*

23.3.9. *ES klasificēto atkritumu iznīcināšana*

24. DROŠĪBAS PĀRKĀPUMS UN ES KLASIFICĒTAS INFORMĀCIJAS KOMPROMITĒŠANA

24.1. **Definīcijas**

24.2. **Paziņošana par drošības pārkāpumiem**

24.3. **Tiesiska darbība**

25. ES KLASIFICĒTAS INFORMĀCIJAS AIZSARDZĪBA, KO APSTRĀDĀ AR INFORMĀCIJAS TEHNOLOĢIJU UN KOMUNIKĀCIJAS SISTĒMU PALĪDZĪBU

25.1. **Ievads**

25.1.1. *Vispārīgi*

25.1.2. *Draudi drošības sistēmām un to neaizsargātība*

25.1.3. *Drošības pasākumu galvenais mērķis*

25.1.4. *Sistēmas drošības prasību izklāsts (SSRS)*

25.1.5. *Drošības ekspluatācijas metodes*

25.2. **Definīcijas**

25.3. **Atbildība par drošību**

25.3.1. *Vispārīgi*

25.3.2. *Drošības akreditācijas iestāde, SAA*

25.3.3. *INFOSEC iestāde (IA)*

25.3.4. *Tehniskās sistēmas īpašnieks (ISO)*

25.3.5. *Informācijas īpašnieks (IO)*

▼B

25.3.6. *Lietotāji*

25.3.7. *Apmācība par INFOSEC*

25.4. **Drošības pasākumi, kas nav tehniski**

25.4.1. *Personāla drošība*

25.4.2. *Fiziskā drošība*

25.4.3. *Piekļuves sistēmai kontrole*

25.5. **Tehniski drošības pasākumi**

25.5.1. *Informācijas drošība*

25.5.2. *Informācijas kontrole un uzskatāmība*

25.5.3. *Maināmo datu nesēju apstrāde un kontrole*

25.5.4. *Datu nesēju deklasificēšana un iznīcināšana*

25.5.5. *Komunikācijas drošība*

25.5.6. *Instalāciju un radiācijas drošība*

25.6. **Drošība apstrādes laikā**

25.6.1. *Drošības ekspluatācijas procedūras (SecOPs)*

25.6.2. *Programmatūras aizsardzība/konfigurāciju pārvaldība*

25.6.3. *Ļaunprātīgas programmatūras/datorvīrusu esamības pārbaude*

25.6.4. *Uzturēšana*

25.7. **Datu iegūšana**

25.7.1. *Vispārīgi*

25.7.2. *Akreditācija*

25.7.3. *Izvērtēšana un sertifikācija*

25.7.4. *Drošības iezīmju parastās pārbaudes akreditācijas pagarināšanas nolūkos*

25.8. **Pagaidu un neregulāra lietošana**

25.8.1. *Mikrodatoru/personālo datoru drošība*

25.8.2. *Personiskajā īpašumā esošā IT aprīkojuma izmantošana oficiālā Komisijas darbā*

25.8.3. *Līgumdarbinieku īpašumā esoša vai valsts piegādāta IT aprīkojuma izmantošana oficiālā Komisijas darbā*

26. ES KLASIFICĒTAS INFORMĀCIJAS NODOŠANA TREŠĀM VALSTĪM VAI STARPTAUTISKĀM ORGANIZĀCIJĀM

26.1.1. *ES klasificētas informācijas nodošanu regulējoši principi*

26.1.2. *Līmeņi*

26.1.3. *Drošības līgumi*

1. PAPILDINĀJUMS: **Nacionālo drošības klasifikāciju salīdzinājums**

2. PAPILDINĀJUMS: **Praktisks klasifikācijas ceļvedis**

3. PAPILDINĀJUMS: **Pamatnostādnes par ES klasificētas informācijas nodošanu trešām valstīm vai starptautiskām organizācijām: 1. līmeņa sadarbība**

4. PAPILDINĀJUMS: **Pamatnostādnes par ES klasificētas informācijas nodošanu trešām valstīm vai starptautiskām organizācijām: 2. līmeņa sadarbība**

5. PAPILDINĀJUMS: **Pamatnostādnes par ES klasificētas informācijas nodošanu trešām valstīm vai starptautiskām organizācijām: 3. līmeņa sadarbība**

6. PAPILDINĀJUMS: **Saīsinājumu saraksts**

▼B

## I DAĻA: DROŠĪBAS PAMATPRINCIPI UN MINIMĀLIE STANDARTI

### 1. IEVADS

Šie noteikumi paredz drošības pamatprincipus un minimālos standartus, kas pienācīgi jāievēro Komisijai visās tās darba vietās, kā arī *EUCI* saņēmējiem, lai aizsargātu drošību un pārliecinātu ikvienu par kopēju aizsardzības standartu izveidi.

### 2. VISPĀRĪGI PRINCIPI

Komisijas drošības politika ir viena no tās vispārējās iekšējās pārvaldības politikas sastāvdaļām un tādējādi pamatota ar principiem, kas attiecas uz to vispārējo politiku.

Šie principi iekļauj likumību, pārredzamību, politisko atbildību un subsidiaritāti (proporcionalitāti).

Likumība norāda nepieciešamību stingri ievērot likumus drošības funkciju veikšanā un nepieciešamību atbilst tiesiskajām prasībām. Tā nozīmē arī to, ka saistībām par drošību domēnā jāpamatojas ar atbilstošām tiesību normām. Civildienesta noteikumus piemēro pilnībā, jo īpaši to 17. pantu par personāla pienākumiem veikt darbu, ņemot vērā Komisijas informāciju un VI sadaļu par disciplinārajiem pasākumiem. Visbeidzot tas nozīmē to, ka drošības noteikumu pārkāpumi, par ko atbild Komisija, tiek izskatīti atbilstoši Komisijas nostājai par disciplināro atbildību un sadarbību ar dalībvalstīm kriminālatbildību jomā.

Pārredzamība norāda skaidrības nepieciešamību attiecībā uz visiem drošības noteikumiem un nosacījumiem, lai līdzsvarotu dažādus pakalpojumus un dažādus domēnus (fiziskā drošība pret informācijas aizsardzību u.c.) un nepieciešamību pēc viendabīgas un strukturizētas drošības izpratnes politikas. Turklāt tā nosaka nepieciešamību attiecībā uz skaidrām rakstiskām pamatnostādnēm drošības pasākumu ieviešanai.

Politiskā atbildība nozīmē to, ka atbildība drošības domēnā tiks skaidri sadalīta. Turklāt tā norāda nepieciešamību regulāri pārbaudīt minēto saistību pareizu pildīšanu.

Subsidiaritāte vai proporcionalitāte nozīmē to, ka drošību organizē zemākā iespējamā līmenī un pēc iespējas ciešākā saiknē ar ģenerāldirektorātiem un Komisijas dienestiem. Tā nozīmē arī to, ka drošības darbībās iekļauj tikai tos elementus, kas tai patiešām ir nepieciešami. Visbeidzot tā nozīmē to, ka drošības pasākumiem jābūt proporcionāliem aizsargājamām interesēm un faktiskiem vai potenciāliem minēto interešu draudiem, sniedzot tādu aizsardzību, kas izraisa vismazāko potenciālo traucējumu.

### 3. DROŠĪBAS PAMATI

Pareizas drošības pamati ir:

a) katrā dalībvalstī valsts drošības iestāde ir atbildīga par:

   1) ziņu savākšanu un ierakstīšanu par spiegošanu, sabotāžu, terorismu un citām graujošām darbībām, un

   2) informācijas un padomu sniegšanu tās valdībai un ar tās starpniecību — Komisijai — par draudiem drošībai un veidiem, kā pret tiem aizsargāties;

b) katrā dalībvalstī un Komisijā tehniskā *INFOSEC* iestāde *(IA)*, kas atbild par sadarbību ar attiecīgo drošības iestādi, sniedz informāciju un ieteikumus par tehniskiem draudiem drošībai un veidiem, kā pret tiem aizsargāties;

c) regulāra sadarbība starp valdības departamentiem un attiecīgiem Eiropas institūciju dienestiem, lai attiecīgā gadījumā izveidotu un ieteiktu:

   1) kādas personas, informāciju un resursus ir jāaizsargā un

   2) vienotus aizsardzības standartus;

▼B

d) cieša sadarbība starp ►M2 Komisijas Drošības direktorātu ◄ un citiem Eiropas institūciju drošības dienestiem, un NATO drošības biroju (*NOS*).

4. INFORMĀCIJAS DROŠĪBAS PRINCIPI

4.1. **Mērķi**

Informācijas drošībai ir šādi galvenie mērķi:

a) aizsargāt ES klasificēto informāciju (*EUCI*) no spiegošanas, kompromitēšanas vai neatļautas atklāšanas;

b) aizsargāt ES informāciju, ko apstrādā komunikāciju un informācijas sistēmās un tīklos, no draudiem tās konfidencialitātei, integritātei un pieejamībai;

c) aizsargāt Komisijas telpas, kurās atrodas ES informācija, no sabotāžas un ar nodomu nodarīta ļaunuma;

d) neveiksmes gadījumā izvērtēt nodarīto kaitējumu, ierobežot tā sekas un veikt nepieciešamos pasākumus stāvokļa uzlabošanai.

4.2. **Definīcijas**

Šajos noteikumos:

a) termins "ES klasificēta informācija" (*EUCI*) ir jebkura informācija un materiāli, kuru neatļauta atklāšana var dažādās pakāpes apdraudētu ES, vienas vai vairāku tās dalībvalstu intereses, atkarībā no tā, vai šāda informācija nāk no ES vai ir saņemta no dalībvalstīm, trešām valstīm vai starptautiskām organizācijām;

b) termins "dokuments" ir jebkura vēstule, ziņa, pieraksts, ziņojums, memorands, signāls/paziņojums, skečs, fotogrāfija, diapozitīvs, filma, karte, tabula, plāns, piezīmju grāmatiņa, trafarets, kopējamais papīrs, rakstāmmašīnas vai printera izdruka, lente, kasete, datora disks, CD–ROM vai cits fizisks informācijas ierakstīšanas līdzeklis;

c) termins "materiāls" ir "dokuments", kā tas ir definēts b) punktā un arī jebkura iekārta, kas ir vai nu izgatavota, vai atrodas izgatavošanas procesā;

d) termins "nepieciešamība zināt" ir individuāla darbinieka vajadzība piekļūt ES klasificētai informācijai, lai spētu veikt darbu vai pildīt pienākumus;

e) "atļauja" ir ►M2 Komisijas Drošības direktorāta direktora ◄ lēmums sniegt individuālu piekļuvi *EUCI* līdz noteiktam līmenim, pamatojoties uz pārmeklēšanu (drošības pārbaudi), ko veic valsts drošības iestāde saskaņā ar valsts tiesību aktiem;

f) termins "klasificēt" ir noteiktas slepenības pakāpes piemērošana informācijai, kuras neatļauta atklāšana var radīt konkrētu kaitējumu Komisijas vai dalībvalstu interesēm;

g) termins "slepenības pakāpes pazemināšana" (*déclassement*) ir klasifikācijas līmeņa pazemināšana;

h) termins "deklasifikācija" (*déclassification*) ir jebkādas klasifikācijas atcelšana;

i) termins "autors" ir pienācīgi pilnvarots klasificēta dokumenta autors. Komisijā departamentu vadītāji var atļaut to darbiniekiem sagatavot *EUCI*;

j) termins "Komisijas departamenti" ir Komisijas departamenti un dienesti, tostarp biroji, visas darba vietas, tostarp Kopīgais pētniecības centrs, pārstāvniecības un biroji Savienībā un delegācijas trešajās valstīs.

▼B

4.3. **Klasifikācija**

a) Attiecībā uz klasifikāciju nepieciešama rūpība un pieredze, izvēloties informāciju un materiālu, kas ir jāaizsargā, un izvērtējot tam piemērojamo aizsardzības pakāpi. Ir svarīgi, lai aizsardzības pakāpe atbilstu tās informācijas un materiāla drošībai, kas ir jāaizsargā. Lai nodrošinātu vienmērīgu informācijas plūsmu, veic pasākumus, lai izvairītos no pārlieku augstas vai zemas klasifikācijas pakāpes piešķiršanas;

b) klasifikācijas sistēma ir šo principu īstenošanas instruments; līdzīgu klasifikācijas sistēmu ievēro plānojot un organizējot veidus, lai apkarotu spiegošanu, sabotāžu, terorismu un citus draudus, lai attiecībā uz vissvarīgākajām telpām, kurās atrodas klasificēta informācija, un visjutīgākajām to vietām piemērotu vislielākos aizsardzības pasākumus;

c) par klasificētu informāciju ir atbildīgs vienīgi tās autors;

d) klasifikācijas līmeni var pamatot tikai ar minētās informācijas saturu;

e) ja ir grupētas vairākas ziņas, klasifikācijas pakāpe, ko piešķir visam kopumam, ir vismaz tik augsta kā visaugstākā klasifikācija. Informācijas kolekcijai tomēr var piešķirt augstāku klasifikāciju kā tās sastāvdaļām;

f) klasifikāciju piešķir tikai tad, kad tas ir nepieciešams, un tikai uz nepieciešamo laiku.

4.4. **Drošības pasākumu mērķi**

Drošības pasākumi:

a) attiecas uz visām personām, kam ir piekļuve klasificētai informācijai, klasificētas informācijas nesējiem, visām telpām, kurās atrodas šāda informācija, un svarīgām iekārtām;

b) ir izveidoti tā, lai atpazītu personas, kuru stāvoklis var apdraudēt klasificētas informācijas drošību un svarīgas iekārtas, kas satur klasificētu informāciju un kas paredzētas to izslēgšanai vai iznīcināšanai;

c) liegt jebkurai personai, kurai tas nav atļauts, piekļūt klasificētai informācijai vai iekārtām, kas to satur;

d) nodrošināt to, ka klasificētu informāciju izplata tikai pamatojoties uz nepieciešamības zināt principu, kas ir visu drošības aspektu pamatā;

e) nodrošināt integritāti (piemēram, korupcijas novēršana vai neatļautu izmaiņu veikšanas, vai neatļautas izdzēšanas novēršana) un pieejamību (piemēram, piekļuve netiek liegta tiem, kam ir nepieciešama piekļuve un kuriem tā ir atļauta) visai informācijai, vai tā ir klasificēta vai nav, jo īpaši tādai informācijai, kas ir uzglabāta, apstrādāta vai pārsūtīta elektromagnētiskā formā.

5. DROŠĪBAS ORGANIZĒŠANA

5.1. **Kopējie minimālie standarti**

Komisija nodrošina to, ka kopējos minimālos drošības standartus ievēro visi *EUCI* saņēmēji iestādē un tās kompetencēs esošās iestādēs, piemēram, visi departamenti un līgumdarbinieki, lai ES klasificēto informāciju nodotu ar pārliecību, ka to apstrādās ar pienācīgu rūpību. Šādi minimālie standarti iekļauj kritērijus atļauju izsniegšanai personālam un procedūrām ES klasificētas informācijas aizsardzībai.

Komisija ļauj piekļuvi *EUCI* ārpus esošām struktūrām, ja vien tās nodrošina *EUCI* apstrādes laikā ievērot tādus noteikumus, kas ir vismaz tikpat stingri kā šie minimālie standarti.

▼M3

Šādus minimālos standartus piemēro arī tajos gadījumos, kad Komisija, izmantojot līgumus vai subsīdiju līgumus, uztic rūpniecības vai cita veida uzņēmumiem uzdevumus, kas ietver, ietekmē un/vai satur ES

▼M3

klasificēto informāciju; šie kopējie minimālie standarti ir ietverti II daļas 27. iedaļā.

▼B

5.2. **Organizācija**

Komisijā drošība ir organizēta divos līmeņos:

a) visas Komisijas līmenī ir ►M2 Komisijas Drošības direktorāts ◄ ar drošības akreditācijas iestādi (*SAA*), kas darbojas arī kā Kriptogrāfijas iestāde (*CrA*) un kā *TEMPEST* iestāde, un ar *INFOSEC* iestādi (*IA*) un vienu vai vairākiem Centrāliem *EUCI* reģistriem, katrā no kuriem ir viens vai vairāki Reģistra kontrolieri (*RCO*);

b) Komisijas departamentu drošības līmenī par drošību atbild viens vai vairāki vietējie drošības speciālisti (*LSO*), viens vai vairāki galvenie IT drošības speciālisti (*CISO*), vietējie IT drošības speciālisti (*LISO*) un vietējie ES klasificētas informācijas reģistri, kuros ir viens vai vairāki reģistra kontrolieri;

c) centrālie drošības dienesti vada vietējo drošības dienestu darbību.

6. PERSONĀLA DROŠĪBA

6.1. **Atļauju izsniegšana personālam**

Visām personām, kurām nepieciešama piekļuve ►M1 CONFIDENTIEL UE ◄ informācijai vai augstākas drošības pakāpes informācijai, pirms šādas piekļuves sniegšanas pienācīgā kārtā jāsaņem atļauja. Līdzīgu atļauju vajag tādām personām, kuru pienākumos ir klasificētas informācijas saturošu komunikāciju un informāciju sistēmu tehniskā darbība vai uzturēšana. Šādas atļaujas piešķiršana ir domāta, lai noteiktu, vai šādas personas:

a) ir neapšaubāmi uzticīgas;

b) tām piemīt tāds raksturs un diskrētums, kas neizraisa šaubas par savu integritāti klasificētas informācijas apstrādē, vai

c) tās var ietekmēt ārzemju vai citi avoti.

Pārbaudes procedūrās īpaša uzmanība jāievērš personām, kam:

d) tiks sniegta piekļuve ►M1 TRES SECRET UE/EU TOP SECRET ◄ informācijai;

e) ir amati, kuri paredz regulāru piekļuvi apjomīgai ►M1 SECRET UE ◄ informācijai;

f) savu pienākumu dēļ ir īpaša piekļuve slepenai komunikācijai vai informācijas sistēmām un tādējādi iespēja iegūt neatļautu piekļuvi apjomīgai ES klasificētai informācijai vai radīt nopietnus zaudējumus, veicot tehnisko sabotāžu.

Pēc iespējas vairāk jāizmanto cēloņu izmeklēšanas tehnika d), e) un f) punktos izklāstītajos apstākļos.

Ja personas, kam nav pamatota "nepieciešamība zināt", tiks nodarbinātas apstākļos, kuros tām var būt piekļuve ES klasificētai informācijai (piemēram, kurjeri, drošības aģenti, apkalpojošais personāls un apkopēji u.c.), vispirms pienācīgi jāpārbauda to drošība.

6.2. **Personālam izsniegto atļauju uzskaite**

Visi Komisijas departamenti, kas apstrādā ES klasificētu informāciju vai glabā slepenu komunikāciju vai informācijas sistēmas, veic ierakstu par atļauju, kura ir izsniegta attiecīgajam personālam. Katru atļauju pārbauda atkarībā no apstākļiem, pārliecinoties, vai tā ir adekvāta personas pašreizējam darbam; to pārskata prioritārā kārtā katru reizi, kad tiek saņemta jauna informācija, kas norāda uz to, ka klasificēta darba turpināšana vairs nav drošības interesēs. Vietējais Komisijas departamenta drošības kontrolieris uztur ierakstu par atļauju viņa vai viņas pārziņā.

▼B

6.3. **Personāla informēšana par drošības jautājumiem**

Visu personālu, kas ir nodarbinātas amatos, saistībā ar kuriem tiem var būt piekļuve klasificētai informācijai, informē par šāda darba uzsākšanu un par drošībai nepieciešamajiem laika intervāliem, kā arī procedūrām, kas nepieciešamas tā pabeigšanai. Šādam personālam rakstiski jāapliecina, ka tas ir izlasījis un pilnīgi saprot pašreizējos drošības noteikumus.

6.4. **Atbildība par pārvaldību**

Pārvaldnieku pienākums ir apzināt tās personas, kuras ir iesaistītas darbā ar klasificētu informāciju vai kurām ir piekļuve slepenai komunikācijai vai informācijas sistēmām, kā arī reģistrēt un paziņot jebkurus starpgadījumus vai acīmredzamus trūkumus, kas potenciāli var apdraudēt drošību.

6.5. **Personāla drošības statuss**

Izveido procedūras, lai nodrošinātu to, ka uzzinot negatīvu informāciju par indivīdu, tiek noteikts, vai indivīds ir nodarbināts darbā ar klasificētu informāciju vai tam ir piekļuve slepenai komunikācijai vai informācijas sistēmām, par ko informē ►M2 Komisijas Drošības direktorātu ◄. Ja nosaka, ka šāds indivīds apdraud drošību, to atceļ no tādiem darbiem vai liedz tos darīt, kuros tas var apdraudēt drošību.

7. FIZISKĀ DROŠĪBA

7.1. **Vajadzība pēc aizsardzības**

Fiziskās drošības pasākumu līmenis, ko piemēro, lai nodrošinātu ES klasificētas informācijas aizsardzību ir proporcionāls klasifikācijai, rīcībā esošās informācijas un materiāla apjomam, kā arī pastāvošajiem draudiem. Visi ES klasificētas informācijas turētāji ievēro vienotu praksi attiecībā uz šādas informācijas klasificēšanu un atbilstību kopējiem standartiem par aizsardzību pret informācijas un materiāla arestu, pārsūtīšanu un iznīcināšanu, kurai ir nepieciešama aizsardzība.

7.2. **Pārbaudes**

Pirms tādu zonu atstāšanas, kurās bez uzraudzības atrodas ES klasificēta informācija, attiecīgās pārraugošās personas nodrošina to, ka tā ir droši novietota un ka visi drošības rīki ir aktivizēti (slēdzenes, signalizācijas u.c.). Citu neatkarīgu pārbaudi veic pēc darba dienas beigām.

7.3. **Ēku drošība**

Ēkas, kurās atrodas ES klasificēta informācija vai slepenas komunikācijas un informācijas sistēmas aizsargā pret neatļautu piekļuvi. Veiktie ES klasificētas informācijas aizsardzības pasākumi, piemēram, logu bloķēšana, durvju slēdzenes, sargi pie ieejamām, automātiskas piekļuves kontroles sistēmas, drošības pārbaudes un patruļas, signalizācijas sistēmas, ielaušanās identificēšanas sistēmas un sargsuņi ir atkarīgi no:

a) aizsargājamās informācijas un materiāla klasifikācijas, apjoma un izvietojuma ēkā;

b) minētās informācijas un materiāla drošības konteineru kvalitātes un

c) ēkas fiziskajām īpašībām un novietojuma.

Tāpat komunikācijas un informācijas sistēmām piešķirtā aizsardzība ir atkarīga no to vērtības izvērtēšanas un potenciālo seku izvērtēšanas, kas rastos drošības kompromitēšanas dēļ, ēkas fiziskajām īpašībām un novietojuma, kurā atrodas sistēmas, un no sistēmu novietojuma ēkā.

7.4. **Ārkārtas rīcības plāni**

Iepriekš izstrādā sīki izstrādātus plānus klasificētas informācijas aizsardzībai vietējas vai valsts ārkārtas situācijās.

8. INFORMĀCIJAS DROŠĪBA

Informācijas drošība (*INFOSEC*) attiecas uz drošības pasākumu identificēšanu un piemērošanu, lai aizsargātu ES klasificēto informāciju, kas

▼B

tiek apstrādāta, uzglabāta vai pārsūtīta komunikācijas, informācijas un citās elektroniskās sistēmās, pret konfidencialitātes zaudēšanu, integritāti vai pieejamību, vai tā ir nejauša vai ar iepriekšēju nodomu. Lai novērstu neatļautu lietotāju piekļuvi ES klasificētai informācijai, lai novērstu piekļuves atteikumu ES klasificētai informācijai autorizētiem lietotājiem un lai novērstu korupciju vai neatļautu ES klasificētas informācijas sagrozīšanu vai dzēšanu, nodrošina atbilstošus pretpasākumus.

9. SABOTĀŽAS PROFILAKSE UN CITU TĪŠA KAITĒJUMA VEIDU KONTROLE

Fiziski aizsardzības pasākumi svarīgu tādu iekārtu aizsargāšanai, kas satur klasificētu informāciju, ir labākie drošības pasākumi pret sabotāžu un citu tīšu kaitējumu; to nevar aizvietot tikai ar atļauju izsniegšanu personālam. Kompetentu valsts iestādi aicina sniegt ziņas par spiegošanu, sabotāžu, terorismu un citām graujošām darbībām.

10. KLASIFICĒTAS INFORMĀCIJAS NODOŠANA TREŠAJĀM VALSTĪM VAI STARPTAUTISKĀM ORGANIZĀCIJĀM

Komisija kā kolēģija pieņem lēmumu par Komisijā sagatavotas ES klasificētas informācijas nodošanu trešai valstij vai starptautiskai organizācijai. Ja informācijas autors, kura informāciju ir vēlams atklāt, nav Komisija, Komisija vispirms cenšas saņemt autora atļauju informācijas nodošanai. Ja autoru nevar noteikt, Komisija uzņemas iepriekšējā atbildību.

Ja Komisija saņem klasificētu informāciju no trešajām valstīm, no starptautiskām organizācijām vai citām trešajām pusēm, minēto informāciju aizsargā atbilstoši tās klasifikācijai un atbilstoši standartiem ES klasificētai informācijai, ko nosaka šie noteikumi, vai citiem augstākiem standartiem, kurus var pieprasīt trešā puse, kas ir atklājusi informāciju. Var vienoties par savstarpējām pārbaudēm.

Iepriekšminētos principus ievieš saskaņā ar sīki izklāstītiem noteikumiem, kas ir minēti II daļā, 26. iedaļā un 3., 4. un 5. papildinājumā.

**II DAĻA: DROŠĪBAS ORGANIZĒŠANA KOMISIJA**

11. KOMISIJAS LOCEKLIS, KAS ATBILD PAR DROŠĪBAS JAUTĀJUMIEM

Komisijas loceklis, kas atbild par drošības jautājumiem:

a) īsteno Komisijas drošības politiku;

b) izskata drošības problēmas, kuras tam ir paziņojusi Komisija vai tās kompetentās struktūras;

c) izskata jautājumus, kuri iekļauj izmaiņas Komisijas drošības politikā, ciešā sadarbībā ar dalībvalstu valsts drošības (vai citām atbilstošām) iestādēm (še turpmāk — *NSA*).

Jo īpaši Komisijas loceklis, kas atbild par drošības jautājumiem, atbild par:

a) visu drošības jautājumu, kuri attiecas uz Komisijas darbībām, koordinēšanu;

b) pieprasījumu nosūtīšanu atbildīgām dalībvalstu iestādēm par to, lai *NSA* sniedz drošības pielaides personālam, kurš ir nodarbināts Komisijā atbilstoši 20. iedaļai;

c) jebkuras ES klasificētas informācijas noplūdes, kura ir notikusi Komisijā, izmeklēšanu vai izmeklēšanas pasūtīšanu;

d) pieprasījuma nosūtīšanu atbilstošām drošības iestādēm uzsākt izmeklēšanu, ja ES klasificētas informācijas noplūde ir notikusi ārpus Komisijai, un par pieprasījumu koordinēšanu, ja ir iesaistīta vairāk kā viena drošības iestāde;

e) periodisku pārbaužu veikšanu par drošības pasākumiem ES klasificētas informācijas aizsardzībai;

f) ciešas sadarbības uzturēšanu ar visām attiecīgajām drošības iestādēm, lai panāktu vispārēju drošības koordināciju;

▼B

g) Komisijas drošības politikas un procedūru pastāvīgu pārskatīšanu un atbilstošu ieteikumu sagatavošanu nepieciešamības gadījumā. Šajā sakarā Komisijas loceklis, kas atbild par drošības jautājumiem, iesniedz Komisijai gadskārtēju pārbaudes plānu, kuru ir sagatavojis ►M2 Komisijas Drošības direktorāts ◄.

12. KOMISIJAS DROŠĪBAS POLITIKAS KONSULTATĪVĀ GRUPA

Izveido Komisijas drošības politikas konsultatīvo grupu. Tajā ir Komisijas loceklis, kas atbild par drošības jautājumiem, vai tā pārstāvis, kurš vada sapulci, un katras dalībvalsts *NSA* pārstāvis. Var ielūgt arī citu Eiropas institūciju pārstāvjus. Attiecīgo EK un ES decentralizēto aģentūru pārstāvjus var aicināt piedalīties tad, ja tiek izskatīti jautājumi, kas uz tiem attiecas.

Komisijas drošības politikas konsultatīvā grupa tiekas pēc tās priekšsēdētāja vai jebkura tās locekļa pieprasījuma. Grupas uzdevums ir izskatīt un izvērtēt visus svarīgos drošības jautājumus, un attiecīgā gadījumā sniegt ieteikumus Komisijai.

▼M2

13. KOMISIJAS DROŠĪBAS PADOME

Tiek izveidota Komisijas Drošības padome. Tā sastāv no Pārvaldes un personāla ģenerāldirektora, kas ir šīs padomes priekšsēdētājs, par drošības jautājumiem atbildīgā komisāra kabineta locekļa, priekšsēdētāja kabineta locekļa, ģenerālsekretāra vietnieka, kas vada Komisijas krīzes vadības grupu, Juridiskā, Ārējo sakaru, Tieslietu, Brīvības un drošības dienestu, Kopīgā pētniecības centra, Informātikas un Iekšējās revīzijas dienestu ģenerāldirektoriem un Komisijas Drošības direktorāta direktora vai viņu pārstāvjiem. Var pieaicināt citus Komisijas ierēdņus. Tās uzdevums ir izvērtēt drošības pasākumus Komisijā un sniegt ieteikumus šajā jomā Komisijas loceklim, kas atbild par drošības jautājumiem.

▼B

14. ►M2 KOMISIJAS DROŠĪBAS DIREKTORĀTS ◄

Lai izpildītu pienākumus, kuri ir minēti 11. iedaļā, Komisijas locekļa, kas atbild par drošības jautājumiem, rīcībā ir ►M2 Komisijas Drošības direktorāts ◄ drošības pasākumu koordinēšanai, pārraudzīšanai un īstenošanai.

►M2 Komisijas Drošības direktorāta direktors ◄ ir Komisijas locekļa, kas atbild par drošības jautājumiem, galvenais padomdevējs un pilda Komisijas drošības politikas konsultatīvās grupas sekretāra pienākumus. Šajā sakarā viņš vai viņa vada drošības noteikumu atjaunināšanu un koordinē drošības pasākumus ar kompetentām dalībvalstu iestādēm un attiecīgā gadījumā ar starptautiskām organizācijām, kurām ar Komisiju ir drošības vienošanās. Tādēļ viņš/viņa darbojas kā sadarbības koordinators.

►M2 Komisijas Drošības direktorāta direktors ◄ atbild par IT sistēmu akreditāciju un to tīkliem Komisijā. ►M2 Komisijas Drošības direktorāta direktors ◄ lemj, sadarbojoties ar attiecīgo *NSA*, par IT sistēmu un tīklu akreditāciju, kurā ir iesaistīta Komisija, no vienas puses, un jebkurš ES klasificētas informācijas saņēmējs, no otras puses.

15. DROŠĪBAS PĀRBAUDES

►M2 Komisijas Drošības direktorāts ◄ veic periodiskas pārbaudes par drošības pasākumiem ES klasificētas informācijas aizsardzībai.

Veicot šo uzdevumu, ►M2 Komisijas Drošības direktorāts ◄ var saņemt palīdzību no citas ES institūcijas, kuras rīcībā ir *EUCI* vai no dalībvalsts valsts drošības iestādes ([1]).

([1]) Neierobežojot 1961. gada Vīnes konvenciju par diplomātiskajām attiecībām un 1965. gada 8. aprīļa Protokolu par Eiropas Kopienu privilēģijām un imunitāti.

▼B

Pēc dalībvalsts pieprasījuma *EUCI* pārbaudi var veikt tās *NSA* kopā ar ►M2 Komisijas Drošības direktorātu ◄, savstarpēji vienojoties.

16. KLASIFIKĀCIJAS, DROŠĪBAS APZĪMĒJUMI UN MARĶĒJUMS

16.1. **Klasifikācijas līmeņi ([1])**

Informāciju klasificē šādos līmeņos (skatīt arī 2. papildinājumu).

►M1 TRES SECRET UE/EU TOP SECRET ◄: šo klasifikāciju piemēro tikai informācijai un materiāliem, kuru neatļauta publiskošana var izraisīt būtiskus traucējumus ES vai vienas vai vairāku tās dalībvalstu interesēm.

►M1 SECRET UE ◄: šo klasifikāciju piemēro tikai informācijai un materiāliem, kuru neatļauta publiskošana var radīt nopietnu kaitējumu ES vai vienas vai vairāku tās dalībvalstu interesēm.

►M1 CONFIDENTIEL UE ◄: šo klasifikāciju piemēro tikai informācijai un materiāliem, kuru neatļauta publiskošana var kaitēt ES vai vienas vai vairāku tās dalībvalstu interesēm.

►M1 RESTREINT UE ◄: šo klasifikāciju piemēro tikai informācijai un materiāliem, kuru neatļauta publiskošana var būt neizdevīga ES vai vienas vai vairāku tās dalībvalstu interesēm.

Citas klasifikācijas nav atļautas.

16.2. **Drošības apzīmējumi**

Lai ierobežotu klasifikācijas derīgumu (klasificētai informācijai, kas paredz automātisku slepenības pakāpes pazemināšanu vai deklasificēšanu), var izmantot norunātus drošības apzīmējumus. Šādi apzīmējumi ir vai nu "LĪDZ… (laiks/diena)" vai "LĪDZ… (notikums)".

Piemēro papildu drošības apzīmējumus, tādus kā *CRYPTO* vai jebkuru citu ES atzītu drošības apzīmējumu, ja ir nepieciešams ierobežot izplatīšanu un īpašu apstrādi papildus tai, kas ir norādīta drošības klasifikācijā.

Drošības apzīmējumus izmanto tikai kopā ar klasifikāciju.

16.3. **Marķējumi**

Marķējumu var izmantot, lai norādītu jomu, uz ko attiecas dokumenti, vai īpašu izplatīšanu, pamatojoties uz nepieciešamību zināt, vai (neklasificētai informācijai) lai norādītu embargo beigas.

Marķējumu neklasificē un to savstarpēji neaizvieto.

*EDAP* marķējumu piemēro dokumentiem un to kopijām, kas attiecas uz Savienības un vienas vai vairāku tās dalībvalstu drošību un aizsardzību, vai kas attiecas uz militāro un nemilitāro krīžu vadību.

16.4. **Klasifikācijas piešķiršana**

Klasifikāciju piešķir šādi:

a) ►M1 RESTREINT UE ◄ dokumentiem mehāniski vai elektroniski;

b) ►M1 CONFIDENTIEL UE ◄ dokumentiem mehāniski vai ar roku, vai drukājot uz iepriekš apzīmogota, reģistrēta papīra;

c) ►M1 SECRET UE ◄ un ►M1 TRES SECRET UE/EU TOP SECRET ◄ dokumentiem mehāniski vai ar roku.

16.5. **Drošības apzīmējumu piešķiršana**

Drošības apzīmējumus piešķir tieši zem klasifikācijas tādā pašā veidā kā tos, ar kuriem norāda klasifikāciju.

([1]) Skatīt ES, NATO, RES un dalībvalstu drošības klasifikāciju salīdzinošo tabulu 1. papildinājumā.

▼B

17. KLASIFIKĀCIJAS PĀRVALDĪBA

17.1. **Vispārīgi**

Informāciju klasificē tikai tad, kad tas ir nepieciešams. Klasifikācija ir skaidra un pareizi norādīta, un to patur tikai tik ilgi, kamēr informācijai nepieciešama aizsardzība.

Par informācijas klasificēšanu un tās tālāku slepenības pakāpes pazemināšanu vai deklasificēšanu atbild tās autors.

Komisijas ierēdņi un citi darbinieki klasificē, pazemina slepenības pakāpi vai deklasificē informāciju, saskaņojot to ar savas struktūrvienības vadītāju vai pēc tā norādījuma.

Sīki izstrādāta procedūra klasificētu dokumentu apstrādei ir izstrādāta tā, lai nodrošinātu tajos esošās informācijas saturam atbilstošu aizsardzību.

Personu skaitu, kurām ir atļauts izstrādāt ►M1 TRES SECRET UE/EU TOP SECRET ◄ dokumentus, pēc iespējas vairāk ierobežo un to vārdus ieraksta ►M2 Komisijas Drošības direktorāta ◄ sagatavotajā sarakstā.

17.2. **Klasifikācijas piemērošana**

Dokumenta klasifikāciju nosaka pēc dokumenta satura jutības pakāpes saskaņā ar 16. iedaļā izklāstīto definīciju. Ir svarīgi, lai klasifikāciju izmantotu pareizi un ierobežoti. Jo īpaši tas attiecas uz ►M1 TRES SECRET UE/EU TOP SECRET ◄ klasifikāciju.

Tāda dokumenta autors, kuram tiks piešķirta klasifikācija, patur prātā iepriekš izklāstītos noteikumus un ierobežo jebkuru tendenci piešķirt augstāku vai zemāku klasifikāciju.

Klasificēšanas praktiskā rokasgrāmata ir iekļauta 2. papildinājumā.

Atsevišķām konkrēta dokumenta lappusēm, daļām, iedaļām, pielikumiem un papildinājumiem var būt nepieciešama atšķirīga klasifikācija un tos klasificē atbilstoši. Visa dokumenta klasifikācija atbilst tai, kas ir tā visaugstāk klasificētajai daļai.

Vēstules vai ziņas, kas iekļauj pielikumus, klasifikācijas pakāpe ir tāda, kāda ir tās visaugstāk klasificētajam pielikumam. Autors skaidri norāda, kāds klasifikācijas līmenis tai jāpiešķir, kad to nodaļas nodala no tās pielikumiem.

Regula (EK) Nr. 1049/2001 joprojām attiecas uz publiskumu.

17.3. **Slepenības pakāpes pazemināšana un deklasificēšana**

ES klasificētus dokumentus var deklasificēt vai pazemināt to slepenības pakāpi tikai ar autora atļauju un vajadzības gadījumā pēc apspriešanās ar citām ieinteresētajām pusēm. Slepenības pakāpes pazemināšanu vai deklasificēšanu apstiprina rakstiski. Autors atbild par izmaiņu paziņošanu adresātiem; savukārt tie atbild par izmaiņu paziņošanu citiem tālākajiem adresātiem, kuriem tie ir nosūtījuši vai nokopējuši dokumentu.

Ja iespējams, autori uz klasificētiem dokumentiem norāda datumu, laika posmu vai notikumu, pēc kuriem to saturu var deklasificēt vai pazemināt to slepenību. Citā gadījumā, tie pārskata dokumentus, vēlākais, ik pēc pieciem gadiem, lai pārliecinātos, ka sākotnējā klasifikācija ir nepieciešama.

18. FIZISKĀ DROŠĪBA

18.1. **Vispārīgi**

Fiziskās drošības pasākumu galvenais mērķis ir novērst neatļautu personu piekļuvi ES klasificētai informācijai un/vai materiāliem, novērst zādzību, iekārtu vai cita īpašuma bojāšanu un novērst uzmākšanos vai citu tipu agresiju, kas vērsta pret personālu, citiem darbiniekiem un apmeklētājiem.

▼B

18.2. **Drošības prasības**

Visas ēkas, zonas, būves, telpas, komunikācijas un informācijas sistēmas utt., kurās atrodas un/vai tiek apstrādāta ES klasificēta informācija, aizsargā ar atbilstošiem fiziskiem drošības pasākumiem.

Lemjot par nepieciešamo fiziskās drošības aizsardzības pakāpi, ņem vērā tādus svarīgus faktorus kā:

a) informācijas un/vai materiālu klasifikāciju;

b) informācijas apjomu un formu (piemēram, cietā kopija, elektroniski informācijas nesēji);

c) uz vietas izvērtētus draudus no izlūkdienestiem, kuru mērķis ir ES, dalībvalstis, un/vai citas institūcijas vai trešās puses, kuru rīcībā ir ES klasificēta informācija, proti, sabotāžu, terorismu un citas graujošas un/vai krimināls odāmas darbības.

Piemērotie fiziskās drošības līdzekļi ir domāti, lai:

a) liegtu slepenu vai vardarbīgu iebrucēja iekļūšanu;

b) atturētu, aizkavētu un atklātu neuzticama personāla darbības;

c) aizkavētu tos, kam nav nepieciešamības zināt, piekļūt ES klasificētai informācijai.

18.3. **Fiziskās drošības pasākumi**

18.3.1. *Drošības zonas*

Zonas, kurās uzglabā vai apstrādā informāciju, kurai ir piešķirta ►**M1** CONFIDENTIEL UE ◄ vai augstāka klasifikācijas pakāpe, ir organizētas un strukturizētas tā, lai atbilstu vienai no turpmāk minētajām.

a) I līmeņa drošības zona: zona, kurā ►**M1** CONFIDENTIEL UE ◄ vai augstākas klasifikācijas informāciju apstrādā vai uzglabā tā, ka ienākšana šādā zonā praktiski ir piekļuve klasificētai informācijai. Šādai zonai nepieciešams:

   i) skaidri noteikts un aizsargāts perimetrs, kurā tiek kontrolēta visa ienākšana un iziešana;

   ii) ienākšanas kontroles sistēma, saskaņā ar kuru tikai tie drīkst ienākt, kam ir pienācīga piekļuves atļauja;

   iii) tās informācijas klasifikācijas specifikācija, kas atrodas minētajā zonā, proti, informācija, kurai var piekļūt pēc ienākšanas zonā.

b) II līmeņa drošības zona: zona, kurā ►**M1** CONFIDENTIEL UE ◄ vai augstāka klasifikācijas informācija tiek apstrādāta un uzglabāta tā, ka to var aizsargāt no neatļautu personas piekļuves ar iekšēju kontroli, proti, telpas, kurās atrodas dienesti, kas regulāri apstrādā un uzglabā ►**M1** CONFIDENTIEL UE ◄ vai augstākas klasifikācijas informāciju. Šādai zonai nepieciešams:

   i) skaidri noteikts un aizsargāts perimetrs, kurā tiek kontrolēta visa ienākšana un iziešana;

   ii) ienākšanas kontroles sistēma, saskaņā ar kuru tikai tie drīkst ienākt, kam ir pienācīga piekļuves atļauja; citās personas nodrošina ar pavadoņiem vai līdzvērtīgu kontroli, lai novērstu neatļautu piekļuvi ES klasificētai informācijai un nekontrolētu ienākšanu zonās, uz kurām attiecas tehniskās drošības pārbaudes.

   Tās zonas, kurās drošības personāls neuzturas 24 stundas diennaktī, pārbauda nekavējoties pēc parastā darba laika beigām, lai nodrošinātu to, ka ES klasificēta informācija ir atbilstoši aizsargāta.

18.3.2. *Administratīvā zona*

Apkārt I vai II līmeņa drošības zonām var izveidot administratīvu zonu ar mazāku drošības līmeni. Šādā zonā nepieciešams skaidri noteikts perimetrs, kas ļauj pārbaudīt personālu un transporta līdzekļus. Šādās

▼B

zonās apstrādā un uzglabā tikai ►M1 RESTREINT UE ◄ un neklasificētu informāciju.

18.3.3. *Kontrole caurlaides punktos*

Ienākšanu I un II līmeņa drošības zonās un iziešanu no tām kontrolē pēc pases vai personu atpazīšanas sistēmas, ko piemēro visiem darbiniekiem, kuri parasti strādā šajās zonās. Papildus izveido apmeklētāju pārbaudes sistēmu, lai liegtu neatļautu piekļuvi ES klasificētai informācijai. Caurlaižu sistēmu var papildināt ar automātisku identificēšanu, kas papildina, taču pilnīgi neaizvieto sargus. Izmaiņas draudu izvērtējumā var izraisīt caurlaides kontroles pasākumu pastiprināšanu, piemēram, ievērojamu cilvēku apmeklējumu laikā.

18.3.4. *Sargu posteņi*

I un II līmeņa drošības zonu patrulēšanu veic ārpus parastā darba laika, lai aizsargātu ES īpašumu no kompromitēšanas, bojājumiem vai zudumiem. Patruļu biežumu nosaka saskaņā ar vietējiem apstākļiem, tomēr ir ieteicams tās veikt ik pēc 2 stundām.

18.3.5. *Drošības tvertnes un seifi*

ES klasificētas informācijas uzglabāšanai izmanto trīs veidu tvertnes:

— A kategorija: tvertnes, ko valsts ir atļāvusi izmantot ►M1 TRES SECRET UE/EU TOP SECRET ◄ informācijas uzglabāšanai I vai II līmeņa drošības zonās;

— B kategorija: tvertnes, ko valsts ir atļāvusi izmantot ►M1 SECRET UE ◄ un ►M1 CONFIDENTIEL UE ◄ informācijas uzglabāšanai I un II līmeņa drošības zonās;

— C kategorija: dienesta mēbeles, kas ir piemērotas tikai ►M1 RESTREINT UE ◄ informācijas uzglabāšanai.

Seifus, kas atrodas I un II līmeņa drošības zonās, un visas I drošības zonas, kurās ►M1 CONFIDENTIEL UE ◄ vai augstāk klasificētu informāciju, uzglabā atklātos plauktos vai izstāda shēmās, uz kartēm utt., sienas, grīdas, griestus, durvis ar slēdzenēm apstiprina Drošības akreditācijas iestāde, tādējādi apliecinot, ka tās sniedz aizsardzību, kas ir līdzvērtīga tai, ko sniedz drošības tvertne, kurā ir atļauts uzglabāt tādas pašas klasifikācijas informāciju.

18.3.6. *Slēdzenes*

Slēdzenes, ko izmanto drošības tvertnēs un seifos, kuros uzglabā ES klasificētu informāciju, atbilst šādiem standartiem:

— A grupa: valsts apstiprinātām A kategorijas tvertnēm;

— B grupa: valsts apstiprinātām B kategorijas tvertnēm;

— C grupa: piemēro tikai C grupas dienesta mēbelēm.

18.3.7. *Atslēgu un kodu kombināciju kontrole*

Seifu atslēgas neiznes ārpus Komisijas ēkām. Seifu kodu kombinācijas iegaumē tās personas, kurām tās ir nepieciešams zināt. Ārkārtas gadījumiem attiecīgā Komisijas struktūrvienības atbildīgais par drošību glabā rezerves atslēgas un pierakstus par katru kodu kombināciju; pēdējo glabā atsevišķās aizzīmogotās necaurspīdīgās aploksnēs. Darba atslēgas, rezerves drošības atslēgas un kodu kombinācijas glabā atsevišķās drošības tvertnēs. Minētās atslēgas un kodu kombinācijas aizsargā ne mazāk kā materiālu, kuram tie sniedz piekļuvi.

Seifu kodu kombinācijas dara zināmas pēc iespējas mazāk cilvēkiem. Kombinācijas nomaina:

a) saņemot jaunu tvertni;

b) mainoties personālam;

c) ja ir notikusi vai draud notikt kompromitēšana;

▼B

d) vēlams, ik pēc sešiem mēnešiem, un vismaz katrus divpadsmit mēnešus.

18.3.8. *Ielaušanās detektori*

Kad signalizācijas sistēmas, videonovērošanas kameras un citas elektriskas ierīces aizsargā ES klasificētu informāciju, ir pieejama ārkārtas elektroapgāde, lai nodrošinātu sistēmas nepārtrauktu darbību, ja enerģijas piegāde ir pārtraukta. Vēl viena pamatprasība ir tā, ka šādas sistēmas darbības traucējumu vai manipulāciju gadījumā drošības personālam paziņo ar signalizāciju vai citu uzticamu brīdinājumu.

18.3.9. *Atļautais aprīkojums*

►M2 Komisijas Drošības direktorāts ◄ uztur atjauninātus sarakstus par drošības iekārtām pēc to tipa un modeļa, ko tas ir apstiprinājis klasificētas informācijas aizsardzībai dažādos noteiktos apstākļos un ar dažādiem noteiktiem nosacījumiem. ►M2 Komisijas Drošības direktorāts ◄ sagatavo šādus sarakstus, pamatojoties uz *inter alia* informāciju no nacionālajām drošības iestādēm.

18.3.10. *Kopējamo mašīnu un telefaksu fiziskā aizsardzības*

Kopējamās mašīnas un telefaksus fiziski aizsargā tiktāl, cik tas ir nepieciešams, lai nodrošinātu to, ka tikai tās personas, kurām tas ir atļauts, var tos izmantot klasificētas informācijas apstrādāšanai un visus klasificētos produktus atbilstoši kontrolē.

18.4. **Aizsardzība pret slēptu novērošanu un slepenu noklausīšanos**

18.4.1. *Slēpta novērošana*

Visus piemērotus pasākumus veic gan dienā, gan naktī, lai nodrošinātu to, lai neatļauta persona pat nejauši neierauga ES klasificētu informāciju.

18.4.2. *Slepena noklausīšanās*

Dienestus vai zonas, kurās ►M1 SECRET UE ◄ vai augstākas klasifikācijas informāciju regulāri pārrunā, aizsargā pret pasīvu un aktīvu slepenu noklausīšanos, ja vien pastāv tāds risks. Par šādas noklausīšanās risku izvērtēšanu atbild ►M2 Komisijas Drošības direktorāts ◄, nepieciešamības gadījumā konsultējoties ar nacionālajām drošības iestādēm.

18.4.3. *Elektroniskās un ieraksta aparatūras ieviešana*

Ir aizliegts ienest mobilos telefonus, personiskos datorus, ierakstīšanas ierīces, kameras un citas elektroniskas vai ieraksta ierīces drošības zonās vai tehniski drošās zonās bez iepriekšējas ►M2 Komisijas Drošības direktorāta direktora ◄ atļaujas.

Lai noteiktu aizsardzības pasākumus, ko veic telpās, kuras ir jutīgas pret pasīvu slepenu noklausīšanos (piemēram, sienu, grīdu, durvju un griestu izolācija, kompromitētu noplūžu izvērtēšana) un pret aktīvu slepenu noklausīšanos (piemēram, mikrofonu meklēšana), ►M2 Komisijas Drošības direktorāts ◄ var lūgt palīdzību no nacionālajām drošības iestādēm.

Turklāt, ja apstākļi to atļauj, telekomunikāciju aprīkojumu un elektronisko vai elektrisko biroju aprīkojumu, ko izmanto ►M1 SECRET UE ◄ līmeņa vai augstākas klasifikācijas sanāksmēs, var pārbaudīt nacionālo drošības dienestu tehniskās drošības speciālisti pēc ►M2 Komisijas Drošības direktorāta direktora ◄ pieprasījuma.

18.5. **Tehniski drošas zonas**

Konkrētas zonas var norādīt kā tehniski drošas zonas. Veic īpašas iekļūšanas pārbaudes. Kad šādas zonas neizmanto, tās aizslēdz, izmantojot atļautu metodi, un visas atslēgas uzskata par drošības atslēgām. Šādas zonas regulāri fiziski pārbauda; pārbaudi veic arī pēc katras neatļautas iekļūšanas vai esot aizdomām par šādu iekļūšanu.

▼B

Par iekārtām un mēbelēm sagatavo detalizētu uzskaitījumu, lai uzraudzītu to pārvietošanos. Nevienu iekārtu vai mēbeli neienes drošības zonā, kamēr īpaši apmācīts drošības personāls to nav rūpīgi pārbaudījis, lai atklātu noklausīšanās ierīces. Pēc vispārēja noteikuma nav atļauts bez iepriekšējas atbilstošu iestāžu atļaujas ierīkot komunikāciju līnijas tehniski drošās zonās.

19. VISPĀRĒJI NOSACĪJUMI PAR NEPIECIEŠAMĪBU ZINĀT PRINCIPU UN DROŠĪBAS PIELAIDES IZSNIEGŠANU ES PERSONĀLAM

19.1. **Vispārīgi**

Piekļuvi ES klasificētai informācijai atļauj tikai tām personām, kam ir "nepieciešamība zināt", lai veiktu to pienākumus vai misijas. Piekļuvi ►M1 TRES SECRET UE/EU TOP SECRET ◄, ►M1 SECRET UE ◄ un ►M1 CONFIDENTIEL UE ◄ informācijai atļauj tikai personām, kurām ir atbilstoša drošības pielaide.

"Nepieciešamību zināt" nosaka tā struktūrvienība, kurā attiecīgā persona ir nodarbināta.

Par atļaujas izsniegšanas personālam pieprasīšanu atbild katra struktūrvienība.

No tā izriet "ES personiskās drošības sertifikāta" izsniegšana, kurā ir norādīts informācijas klasifikācijas līmenis, kam var piekļūt attiecīgā persona, un atļaujas derīguma termiņš.

ES personiskās drošības sertifikāts noteiktam klasifikācijas līmenim var sniegt tā turētājam piekļuvi informācijai ar zemāku klasifikācijas pakāpi.

Personām, kas nav ierēdņi vai citi darbinieki, piemēram, līgumdarbiniekiem, ekspertiem vai konsultantiem, ar kuriem var būt nepieciešams pārrunāt vai kuriem var būt nepieciešams parādīt ES klasificētu informāciju, jābūt ES personiskai drošības pielaidei attiecībā uz ES klasificētu informāciju un tiem jābūt instruētiem par atbildību par drošību.

Regula (EK) Nr. 1049/2001 joprojām attiecas uz publicitāti.

19.2. **Īpaši noteikumi par piekļuvi** ►M1 TRES SECRET UE/EU TOP SECRET ◄ informācijai

Par visām personām, kurām ir piekļuve ►M1 TRES SECRET UE/EU TOP SECRET ◄ informācijai, vispirms pārbauda, vai tām var sniegt piekļuvi šādai informācijai.

Visas personas, kurām jāpiekļūst ►M1 TRES SECRET UE/EU TOP SECRET ◄ informācijai, ieceļ Komisijas loceklis, kas atbild par drošības jautājumiem, un to vārdus ievada atbilstošā ►M1 TRES SECRET UE/EU TOP SECRET ◄ reģistrā. ►M2 Komisijas Drošības direktorāts ◄ izveido un uzglabā šādu reģistru.

Pirms piekļuves ►M1 TRES SECRET UE/EU TOP SECRET ◄ informācijai, visas personas paraksta apliecinājumu par to, ka tās ir iepazīstinātas ar Komisija drošības procedūru un pilnīgi saprot savu īpašo atbildību aizsargāt ►M1 TRES SECRET UE/EU TOP SECRET ◄ informāciju, un sekas, kas izklāstītas ES tiesību aktos un valsts likumdošanā vai administratīvajos noteikumos par klasificētas informācijas nonākšanu svešās rokās, vai nu apzināti, vai nejauši.

Ja personām ir piekļuve ►M1 TRES SECRET UE/EU TOP SECRET ◄ informācijai sapulcēs u.c., tā dienesta vai struktūras kompetents kontrolieris, kurā persona ir nodarbināta, paziņo struktūrai, kas organizē sanāksmi par to, ka attiecīgajai personai ir šāda atļauja.

Visu to personu vārdus, kas vairs nav nodarbinātas darbā, kurā nepieciešama piekļuve ►M1 TRES SECRET UE/EU TOP SECRET ◄ informācijai, izslēdz no ►M1 TRES SECRET UE/EU TOP SECRET ◄ saraksta. Turklāt minēto personu uzmanību atkal pievērš to īpašai atbildībai aizsargāt ►M1 TRES SECRET UE/EU TOP SECRET ◄ informāciju. Tās paraksta deklarāciju par to, ka tās

▼B

nekad neizmantos vai nenodos citiem ►M1 TRES SECRET UE/EU TOP SECRET ◄ informāciju, kas ir to rīcībā.

19.3. **Īpaši noteikumi par piekļuvi** ►M1 SECRET UE ◄ un ►M1 CONFIDENTIEL UE ◄ informācijai

Visas personas, kurām tiks sniegta piekļuve ►M1 SECRET UE ◄ vai ►M1 CONFIDENTIEL UE ◄ informācijai, vispirms atbilstoši pārbauda.

Visas personas, kurām tiks sniegta piekļuve ►M1 SECRET UE ◄ vai ►M1 CONFIDENTIEL UE ◄ informācijai, iepazīstina ar atbilstošiem drošības noteikumiem un dara tām zināmas neuzmanības sekas.

Ja personām ir piekļuve ►M1 SECRET UE ◄ vai ►M1 CONFIDENTIEL UE ◄ informācijai sanāksmēs u.c., tās struktūras drošības kontrolieris, kurā minētā persona ir nodarbināta, paziņo struktūrai, kas organizē sanāksmi, par to, ka attiecīgajai personai ir šāda atļauja.

19.4. **Īpaši noteikumi par piekļuvi** ►M1 RESTREINT UE ◄ informācijai

Personām, kurām ir piekļuve ►M1 RESTREINT UE ◄ informācijai, dara zināmus šos drošības noteikumus un neuzmanības sekas.

19.5. **Pārcelšana citā amatā**

Pārceļot darbinieku no amata, kura pienākumos ir ES klasificēta materiāla apstrāde, reģistrs pārrauga to, lai aizejošais ierēdnis šādu materiālu atbilstoši nodotu jaunajam ierēdnim.

Ja darbinieku pārceļ citā amatā, kura pienākumos ir ES klasificēta materiāla apstrāde, vietējais drošības kontrolieris sniedz tam atbilstošus norādījumus.

19.6. **Īpašas norādes**

Personām, kurām jāapstrādā ES klasificēta informācija, pirmo reizi uzņemoties šādus pienākumus un regulāri pēc tām, sniedz norādes par:

a) draudiem drošībai, kas izriet no neapdomīgām sarunām;

b) piesardzību, ar kādu tām jāizturas pret presi un īpašu interešu grupu pārstāvjiem;

c) draudiem, kas izriet no izlūkdienestu darbībām, kuru mērķis ir ES un dalībvalstis attiecībā uz ES klasificētu informāciju un darbībām;

d) pienākumu nekavējoties ziņot atbilstošām drošības iestādēm par jebkuru mēģinājumu tuvoties vai manevru, kas rada aizdomas par spiegošanu vai citiem neparastiem ar drošību saistītiem apstākļiem.

Visām personām, kas parasti bieži kontaktējas ar tādu valstu pārstāvjiem, kuru izlūkdienestu mērķis ir ES un dalībvalstis saistībā ar ES klasificētu informāciju un darbībām, sniedz norādes par metodēm, kuras parasti izmanto dažādi izlūkdienesti.

Nav tādu Komisijas drošības noteikumu, kas attiecas uz personāla, kuram ir sniegta piekļuve ES klasificētai informācijai, privātiem ceļojumiem uz jebkuru galapunktu. ►M2 Komisijas Drošības direktorāts ◄ tomēr iepazīstina šādus ierēdņus un citus darbiniekus, kas ir viņu pakļautībā, ar ceļošanas noteikumiem, kuri uz tiem var attiekties.

20. DROŠĪBAS PIELAIDES IZSNIEGŠANAS PROCEDŪRA KOMISIJAS IERĒDŅIEM UN CITIEM DARBINIEKIEM

a) Piekļuve šādai informācijai ir tikai Komisijas ierēdņiem un citiem darbiniekiem vai personām Komisijā, kam saistībā ar to pienākumiem vai darba prasībām ir nepieciešamība zināt vai izmantot klasificētu informāciju, kura ir Komisijas rīcībā.

b) Lai piekļūtu informācijai, kurai ir piešķirta " ►M1 TRES SECRET UE/EU TOP SECRET ◄", " ►M1 SECRET UE ◄" un " ►M1 CONFIDENTIEL UE ◄" klasifikācija, a) punktā minētajām

▼B

personām, jābūt piešķirtai atļaujai atbilstoši procedūrai, kas ir minētas šīs iedaļas c) un d) punktos.

c) Atļauju piešķir tikai tām personām, kuras ir pārbaudījusi kompetenta dalībvalsts iestāde (nacionālais drošības dienests) saskaņā ar procedūru, kas minēta no i) līdz n) punktam.

d) ►M2 Komisijas Drošības direktorāta direktors ◄ atbild par a), b) un c) punktos minēto atļauju piešķiršanu.

e) Viņš/viņa piešķir atļauju pēc kompetentu dalībvalsts nacionālo iestāžu atzinuma, kas pamatojas uz drošības pārbaudi, kura ir veikta saskaņā ar i) līdz n) punktiem.

f) ►M2 Komisijas Drošības direktorāts ◄ uzglabā visu jutīgo posteņu dienu sarakstu, ko ir snieguši attiecīgās Komisijas struktūrvienības, un visu to personu sarakstu, kuriem ir piešķirta (pagaidu) atļauja.

g) Atļauja, kas ir derīga piecus gadus, nedrīkst pārsniegt to pienākumu termiņu, uz kuru pamata to piešķīra. To var pagarināt saskaņā ar e) punktā minēto procedūru.

h) ►M2 Komisijas Drošības direktorāta direktors ◄ atsauc atļauju, kad viņš/viņa uzskata, ka tam ir pamatoti iemesli. Visi lēmumi atsaukt atļauju ir jādara zināmi attiecīgajai personai, kura var lūgt, lai to uzklausa ►M2 Komisijas Drošības direktorāta direktors ◄ un kompetentā valsts iestāde.

i) Drošības pārbaudi veic ar attiecīgās personas palīdzību un pēc ►M2 Komisijas Drošības direktorāta direktora ◄ pieprasījuma. Pārbaudes jautājumos kompetenta nacionālā iestāde ir tāda, kas atrodas dalībvalstī, kuras pilsonis ir persona, kam tiek piešķirta atļauja. Ja attiecīgā persona nav ES dalībvalsts pilsonis, ►M2 Komisijas Drošības direktorāta direktors ◄ pieprasa drošības pārbaudi vienai no ES dalībvalstīm, kurā personai ir parastā dzīvesvieta vai kurā tā parasti uzturas.

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

k) ►M2 Komisijas Drošības direktorāta direktors ◄ savā pieprasījumā norāda klasificētās informācijas tipu un līmeni, kas jādara pieejams attiecīgajai personai, lai kompetentās nacionālās iestādes spētu veikt pārbaudes procedūras un sniegt savus atzinumus par atļaujas līmeni, kuru varētu piešķirt attiecīgajai personai.

l) Uz visu drošības pārbaudes procedūru kopumā ar iegūtajiem rezultātiem attiecas atbilstīgas tiesību normas, kas ir spēkā attiecīgajā dalībvalstī, tostarp tiesību normas par pārsūdzēšanu.

m) Ja dalībvalsts kompetenta nacionālā drošības iestāde sniedz pozitīvu atzinumu, ►M2 Komisijas Drošības direktorāta direktors ◄ var sniegt personai attiecīgo atļauju.

n) Par negatīvu kompetentu nacionālo iestāžu atzinumu paziņo attiecīgajai personai, kas var lūgt tikšanos ar ►M2 Komisijas Drošības direktorāta direktoru ◄. Ja viņš to uzskata par nepieciešamu, ►M2 Komisijas Drošības direktorāta direktors ◄ var lūgt kompetentas nacionālās iestādes sniegt tālākus paskaidrojumus, ko tās arī dara. Ja negatīvu atzinumu apstiprina, atļauju nepiešķir.

o) Visas personas, kurām ir piešķirta atļauja d) un e) punkta izpratnē, atļaujas piešķiršanas laikā un turpmāk regulāri saņem visas vajadzīgās instrukcijas par slepenas informācijas aizsargāšanu un šādas aizsardzības nodrošināšanas līdzekļiem. Šādas personas paraksta deklarāciju par instrukciju saņemšanu un apņemas tās ievērot.

p) ►M2 Komisijas Drošības direktorāta direktors ◄ veic visus nepieciešamos pasākumus, lai īstenotu šo iedaļu, jo īpaši attiecībā uz noteikumiem par piekļuvi atļauto personu sarakstam.

▼B

q) Izņēmuma gadījumā, ja to pieprasa dienests, ►M2 Komisijas Drošības direktorāta direktors ◄ pēc tā paziņošanas kompetentām nacionālajām iestādēm un ar nosacījumu, ka no tām mēneša laikā nav saņemta atbilde, sniedz pagaidu atļauju uz laika posmu, kurš nepārsniedz sešus mēnešus, kamēr i) punktā minētā pārbaude nav beigusies.

r) Šādi piešķirta pagaidu atļauju nesniedz piekļuvi ►M1 TRES SECRET UE/EU TOP SECRET ◄ informācijai; atbilstoši i) punktam šāda piekļuve ir tikai tiem ierēdņiem, kas efektīvās pārbaudēs ir saņēmušas pozitīvu rezultātu. Kamēr atbilde par pārbaudi nav saņemta, ierēdņiem, kas ir lūguši pārbaudi, lai saņemtu piekļuvi ►M1 TRES SECRET UE/EU TOP SECRET ◄ informācijai, var atļaut, pagaidām un īslaicīgi, piekļūt informācijai, kura ir klasificēta līdz un tostarp — ►M1 SECRET UE ◄.

21. ES KLASIFICĒTU DOKUMENTU SAGATAVOŠANA, IZPLATĪŠANA, PĀRSŪTĪŠANA, KURJERU PERSONISKĀ DROŠĪBA UN PAPILDUS KOPIJAS VAI TULKOJUMI, KĀ ARĪ IZVILKUMI

21.1. **Sagatavošana**

1. ES klasifikācijas piemēro tā, kā noteikts 16. iedaļā, un ►M1 CONFIDENTIEL UE ◄ un augstākas klasifikācijas pakāpes informācijai to norāda katras lappuses apakšas vidū, katru lappusi numurējot. Katram ES klasificētam dokumentam ir reģistrācijas numurs un datums. ►M1 TRES SECRET UE/EU TOP SECRET ◄ un ►M1 SECRET UE ◄ dokumentos minēto reģistrācijas numuru norāda katrā lappusē. Ja tos izplata vairākās kopijās, katrai norāda numuru, kas atrodas pirmajā lappusē, un kopējo lappušu skaitu. Visus pielikumus un papildinājumus uzskaita tāda dokumenta pirmajā lappusē, kam ir piešķirta ►M1 CONFIDENTIEL UE ◄ vai augstāka klasifikācija.

2. Dokumentus, kam ir piešķirta ►M1 CONFIDENTIEL UE ◄ un augstāka klasifikācija, drukā, tulko, uzglabā, pavairo, magnētiski reproducē vai mikrofilmē tikai tās personas, kurām ir piekļuves atļauja ES klasificētai informācijai līdz pat zemākajam pieļaujamajam attiecīgā dokumenta klasifikācijas līmenim.

3. Noteikumi, kas attiecas uz datorizētu klasificētu dokumentu sagatavošanu ir izklāstīti 25. iedaļā.

21.2. **Izplatīšana**

1. ES klasificētu informāciju izplata tikai starp tām personām, kurām ir nepieciešamība zināt un kurām ir atbilstoša drošības pielaide. Autors norāda sākotnējo izplatīšanu.

2. ►M1 TRES SECRET UE/EU TOP SECRET ◄ dokumentus izplata ar ►M1 TRES SECRET UE/EU TOP SECRET ◄ reģistru starpniecību (skatīt 22. iedaļas 2. punktu). Attiecībā uz ►M1 TRES SECRET UE/EU TOP SECRET ◄ ziņām kompetents reģistrs var atļaut komunikāciju centra vadītājam pavairot dokumentu tik eksemplāros, cik norādīts adresātu sarakstā.

3. Dokumentus ar ►M1 SECRET UE ◄ un zemāku klasifikācijas pakāpi sākotnējie adresāti var pārsūtīt citiem adresātiem, pamatojoties uz nepieciešamību zināt. Tomēr sākotnējā dokumenta autoru iestāde skaidri norāda visus brīdinājumus, ko tie vēlas iekļaut. Šādu brīdinājumu iekļaušanas dēļ adresāti var pārsūtīt dokumentus tikai ar dokumenta autora iestādes atļauju.

4. Reģistrē vietējā *EUCI* reģistrā katru dokumentu ar ►M1 CONFIDENTIEL UE ◄ un augstāku klasifikācijas pakāpi pēc tā iesūtīšanas ģenerāldirektorātā vai nosūtīšanas no ģenerāldirektorāta departaments. Dati, kas jāiekļauj (atsauces, datums un, vajadzības gadījumā, kopijas numurs) ir tādi, lai dokumentu varētu identificēt, un tos norāda žurnālā vai īpašā aizsargātā datorizētā informācijas nesējā (skatīt 22. iedaļas 1. punktu).

▼B

21.3. **ES klasificētas informācijas pārsūtīšana**

21.3.1. *Iesaiņošana, paziņojumi par saņemšanu*

1. Dokumentus ar ►M1 CONFIDENTIEL UE ◄ vai augstāku klasifikācijas pakāpi pārsūta īpaši izturīgā, necaurspīdīgā dubultā aploksnē. Uz iekšējās aploksnes norāda attiecīgo ES klasifikācijas pakāpi, kā arī, ja tas ir iespējams, sīku aprakstu par saņēmēja amatu un adresi.

2. Tikai reģistra kontrolieris (skatīt 22. iedaļas 1. punktu) vai tā aizstājējs var atvērt iekšējo aploksni un apstiprināt iekļauto dokumentu saņemšanu, ja vien aploksne nav adresēta konkrētai personai. Šādā gadījumā, attiecīgais reģistrs (skatīt 22. iedaļas 1. punktu) iegrāmato vēstules ienākšanu un tikai tā persona, kurai ir adresēta vēstule, var atvērt iekšējo aploksni un apstiprināt to dokumentu saņemšanu, kas tajā ir iekļauti.

3. Iekšējā aploksnē ievieto pavadrakstu. Paziņojumā par saņemšanu, kas nav klasificēts, norāda reģistrācijas numuru, datumu un dokumenta kopijas numuru, tomēr nekad nenorāda tā saturu.

4. Iekšējā aploksne ir ievietota ārējā aploksne, uz kuras paziņojuma par saņemšanu nolūkos ir norādīts iepakojuma numurs. Drošības klasifikācija nekādā gadījumā nedrīkst parādīties uz ārējās aploksnes.

5. Kurjeri pieprasa paziņojumu par saņemšanu par katru iepakojuma numuru par dokumentiem ar klasifikācijas pakāpi ►M1 CONFIDENTIEL UE ◄ un augstāku.

21.3.2. *Pārsūtīšana ēkas vai ēku grupas iekšienē*

Attiecīgajā ēkā vai ēku grupā klasificētus dokumentus var pārnēsāt aizzīmogotā aploksnē, uz kuras ir norādīts tikai adresāta vārds, ja to pārnes persona, kam ir piekļuves atļauja dokumentiem ar attiecīgo klasifikācijas pakāpi.

21.3.3. *Pārsūtīšana pa valsti*

1. Valstī ►M1 TRES SECRET UE/EU TOP SECRET ◄ dokumentu pārsūta tikai ar oficiālo kurjerpakalpojumu starpniecību vai ar to personu starpniecību, kuriem ir piekļuve ►M1 TRES SECRET UE/EU TOP SECRET ◄ informācijai.

2. Ja ►M1 TRES SECRET UE/EU TOP SECRET ◄ dokumentu pārsūtīšanai izmanto kurjerpakalpojumus ārpus ēkas vai ēku grupas, ievēro noteikumus par iesaiņošanu un paziņojumu par saņemšanu, kas ir izklāstīti šajā iedaļā. Piegādes dienesti organizē darbu tā, lai nodrošinātu, ka iepakojumi, kuros ir ►M1 TRES SECRET UE/EU TOP SECRET ◄ dokumenti, jebkurā laikā nonāk tiešā atbildīgā ierēdņa pārraudzībā.

3. Izņēmuma gadījumos, ►M1 TRES SECRET UE/EU TOP SECRET ◄ dokumentus var paņemt ierēdņi, kas nav kurjeri, vietējai izmantošanai sanāksmēs un diskusijās ārpus ēkas vai ēku grupas, ja:

   a) turētājam ir piekļuve minētajiem ►M1 TRES SECRET UE/EU TOP SECRET ◄ dokumentiem;

   b) transportēšanas veids atbilst noteikumiem, kas attiecas uz ►M1 TRES SECRET UE/EU TOP SECRET ◄ dokumentu pārsūtīšanu;

   c) ierēdnis nekādā gadījumā neatstāj ►M1 TRES SECRET UE/EU TOP SECRET ◄ dokumentus bez uzraudzības;

   d) par šādi pārnēsātu dokumentu, kas ir iekļauts ►M1 TRES SECRET UE/EU TOP SECRET ◄ dokumentu reģistrā, minētajā reģistrā veic piezīmi, kuru pārbauda pēc dokumenta atgriešanas.

4. Attiecīgajā valstī ►M1 SECRET UE ◄ un ►M1 CONFIDENTIEL UE ◄ dokumentus var pārsūtīt vai nu pa pastu, ja šādu

▼B

pārsūtīšanu atļauj valsts tiesību akti un tā atbilst minēto tiesību aktu noteikumiem, vai ar kurjerpastu, vai ar tādu personu starpniecību, kurām ir piekļuve ES klasificētiem dokumentiem.

5. Pamatojoties uz šiem noteikumiem, ►M2 Komisijas Drošības direktorāts ◄ izstrādā norādījumus par personisku ES klasificētu dokumentu pārnēsāšanu. Turētājam jāizlasa un jāparaksta minētos norādījumus. Jo īpaši, norādījumos ir skaidri pateikts, ka nekādā gadījumā:

   a) turētājs nedrīkst atstāt dokumentus bez uzraudzības, ja vien tie neatrodas seifā saskaņā ar 18. iedaļā izklāstītajiem noteikumiem;

   b) turētājs nedrīkst atstāt dokumentus bez uzraudzības sabiedriskajos transportlīdzekļos vai personiskajos transportlīdzekļos, vai tādās vietās kā restorāni vai viesnīcas. Minētos dokumentus nedrīkst uzglabāt viesnīcu seifos vai atstāt bez uzraudzības viesnīcu numuros;

   c) dokumentus nedrīkst lasīt sabiedriskās vietās, piemēram, lidmašīnās vai vilcienos.

21.3.4. *Pārsūtīšana no vienas valsts uz otru*

1. Materiālus ar klasifikācijas pakāpi ►M1 CONFIDENTIEL UE ◄ vai augstāku nogādā ar ES diplomātisko vai militāro kurjerpakalpojumu palīdzību.

2. Tomēr materiālu ar klasifikācijas pakāpi ►M1 SECRET UE ◄ vai ►M1 CONFIDENTIEL UE ◄ personisku pārnēsāšanu var atļaut, ja pārnēsāšanas noteikumi nodrošina to, ka minētie dokumenti nevar nokļūt neatļautu personu rokās.

3. Komisijas loceklis, kas atbild par drošības jautājumiem, var atļaut personisku dokumentu pārnēsāšanu, ja diplomātiskie vai militārie kurjeri nav pieejami vai šādu kurjeru izmantošana izraisītu aizkavēšanos, kura savukārt kaitīgi ietekmētu ES darbības, un materiāls ir steidzami nepieciešams paredzētajam saņēmējam. ►M2 Komisijas Drošības direktorāts ◄ sagatavo norādījumus, kas iekļauj tādu materiālu starptautisku personisku pārvadāšanu, kuru klasifikācijas pakāpe ir līdz un tostarp — ►M1 SECRET UE ◄, ko veic personas, kuras nav diplomātiskie vai militārie kurjeri. Instrukcijās pieprasa to, ka:

   a) turētājam ir atbilstoša drošības pielaide;

   b) attiecīgajā struktūrvienībā vai reģistrā par šādi pārvadātiem materiāliem ir atbilstošs ieraksts;

   c) uz iepakojumiem vai somām, kuros ir ES materiāli, ir oficiāls zīmogs, lai liegtu tos pārbaudīt muitā, un marķējumu ar identifikāciju un norādījumiem atradējam;

   d) turētājam ir kurjera apliecība un/vai misijas apliecība, ko atzīst visās ES dalībvalstīs un ar ko tam ir atļauts pārvadāt norādītos iepakojumus;

   e) ceļojot pa sauszemi, netiek šķērsota valsts, kas nav ES dalībvalsts, robeža, ja vien pārvadātājai valstij nav īpašas garantijas no valsts, kura nav ES dalībvalsts;

   f) turētāja ceļošanas noteikumi, kas attiecas uz maršrutiem, galamērķi un izmantojamajiem transporta veidiem, atbilst ES noteikumiem vai — ja valsts tiesību akti attiecībā uz šādiem jautājumiem ir stingrāki — saskaņā ar šādiem noteikumiem;

   g) turētājs nedrīkst atstāt materiālu bez uzraudzības, ja vien tas netiek uzglabāts saskaņā ar 18. iedaļā izklāstītajiem noteikumiem par seifiem;

   h) turētājs nedrīkst atstāt dokumentus bez uzraudzības sabiedriskajos transportlīdzekļos vai personiskajos transportlīdzekļos, vai tādās

▼B

vietās kā restorāni vai viesnīcas. Minētos dokumentus nedrīkst uzglabāt viesnīcu seifos vai atstāt bez uzraudzības viesnīcu numuros;

i) ja pārvadājamajā materiālā ir dokumenti, tos nedrīkst lasīt sabiedriskās vietās (piemēram, lidmašīnās, vilcienos u.c.).

4. Personām, kas ir ieceltas pārvadāt klasificētu materiālu, jāizlasa un jāparaksta drošības noteikumus, kuros ir iekļauti, mazākais, iepriekšminētie norādījumi un procedūra, kas jāievēro ārkārtas gadījumos vai tad, ja iepakojumu, kurā atrodas klasificēts materiāls, vēlas apskatīt muita vai lidostas drošības amatpersonas.

21.3.5. *ES ierobežotai lietošanai dokumentu pārsūtīšana*

Par ►M1 RESTREINT UE ◄ dokumentu pārvadāšanu īpašu noteikumu nav, izņemot to, ka tiem jābūt tādiem, lai nodrošinātu to, ka dokumenti nenonāk nepilnvarotu personu rokās.

21.4. **Kurjerdienesta darbinieku drošība**

Visiem kurjeriem, kas ir nodarbināti ►M1 SECRET UE ◄ un ►M1 CONFIDENTIEL UE ◄ dokumentu pārvadāšanai, ir atbilstoša drošības pielaide.

21.5. **Tehniskās pārsūtīšanas elektroniskie un citi veidi**

1. Komunikāciju drošības pasākumi ir vērsti uz to, lai nodrošinātu ES klasificētas informācijas drošu pārsūtīšanu. Sīki izstrādāti noteikumi, ko piemēro šādas ES klasificētas informācijas pārsūtīšanai, ir izklāstīti 25. iedaļā.

2. Tikai akreditēti komunikāciju centri un tīkli un/vai termināļi un sistēmas drīkst pārsūtīt informāciju ar klasifikācijas pakāpi ►M1 CONFIDENTIEL UE ◄ un ►M1 SECRET UE ◄.

21.6. **Papildu kopijas un tulkojumi, kā arī izvilkumi no ES klasificētas informācijas**

1. Tikai autors var atļaut kopēt vai tulkot ►M1 TRES SECRET UE/EU TOP SECRET ◄ dokumentus.

2. Ja personas, kurām nav piekļuves ►M1 TRES SECRET UE/EU TOP SECRET ◄ informācijai pieprasa informāciju, kas nav šādi klasificēta, lai arī tā ir iekļauta ►M1 TRES SECRET UE/EU TOP SECRET ◄ dokumentā, ►M1 TRES SECRET UE/EU TOP SECRET ◄ reģistra vadītājam (skatīt 22. iedaļas 2. punktu) var atļaut sniegt nepieciešamo skaitu minētā dokumenta izvilkumu. Vienlaicīgi viņš/viņa veic nepieciešamos pasākumus, lai nodrošinātu to, ka minētajiem izvilkumiem piešķir attiecīgu drošības klasifikāciju.

3. Dokumentus ar klasifikācijas pakāpi ►M1 SECRET UE ◄ un zemāku to adresāts var atveidot un tulkot atbilstoši šiem drošības noteikumiem un ar noteikumu, ka tas stingri ievēro nepieciešamības zināt principu. Drošības pasākumus, ko piemēro dokumenta oriģinālam, piemēro arī tā atveidojumiem un/vai tulkojumiem.

22. ***EUCI*** REĢISTRI, APVIENOŠANAS, PĀRBAUDES, ARHĪVU GLABĀŠANA UN ***EUCI*** IZNĪCINĀŠANA

22.1. **Vietējie *EUCI* reģistri**

1. Komisijā, katrā struktūrvienībā, kā tas ir pieprasīts, viens vai vairāki vietējie *EUCI* reģistri atbild par dokumentu ar klasifikācijas pakāpi ►M1 SECRET UE ◄ un ►M1 CONFIDENTIEL UE ◄ reģistrāciju, atveidošanu, nosūtīšanu, arhivēšanu un iznīcināšanu.

2. Ja struktūrvienībai nav vietējā *EUCI* reģistra, *EUCI* reģistra funkcijas pilda ģenerālsekretariāta vietējais *EUCI* reģistrs.

▼B

3. Vietējie *EUCI* reģistri ziņo tās struktūrvienības vadītājam, no kura tie saņem norādījumus. Šādu reģistru vadītājs ir Reģistra kontrolieris (*RCO*).

4. Vietējais drošības speciālists tos pārrauga tiktāl, cik tas attiecas uz noteikumiem par *EUCI* dokumentu apstrādi un attiecīgo drošības pasākumu ievērošanu.

5. Ierēdņiem, kas ir norīkoti darbam vietējā *EUCI* reģistrā, ir atļauta piekļuve *EUCI* saskaņā ar 20. iedaļu.

6. Vietējie *EUCI* reģistri attiecīgās struktūrvienības vadītāja pārraudzībā:

   a) pārvalda darbības, kas attiecas uz šādas informācijas reģistrāciju, atveidošanu, tulkošanu, pārsūtīšanu, nosūtīšanu un iznīcināšanu;

   b) atjaunina datu sarakstu par klasificētu informāciju;

   c) periodiski izskata jautājumus par nepieciešamību paturēt informācijas klasifikāciju.

7. Vietējie *EUCI* reģistri uztur reģistru par šādiem datiem:

   a) klasificētās informācijas sagatavošanas datumu;

   b) klasifikācijas pakāpi;

   c) klasifikācijas derīguma termiņu;

   d) izsniedzēja vārdu un struktūrvienību;

   e) saņēmēju vai saņēmējus ar kārtas numuru;

   f) tematu;

   g) numuru;

   h) izplatīto kopiju skaitu;

   i) uzskaitījumu sagatavošanu par struktūrvienībām iesniegto klasificēto informāciju;

   j) klasificētās informācijas slepenības pakāpes pazemināšanai vai deklasifikācijas reģistru.

8. Uz Komisijas vietējiem *EUCI* reģistriem attiecas vispārējie noteikumi, kas ir izklāstīti 21. iedaļā, ja vien tie nav pārgrozīti ar īpašajiem noteikumiem, kuri ir izklāstīti šajā iedaļā.

22.2. ►**M1** TRES SECRET UE/EU TOP SECRET ◄ informācijas reģistrs

22.2.1. *Vispārīgi*

1. Centrālais ►**M1** TRES SECRET UE/EU TOP SECRET ◄ reģistrs nodrošina ►**M1** TRES SECRET UE/EU TOP SECRET ◄ dokumentu reģistrāciju, apstrādi un izplatīšanu saskaņā ar šiem drošības noteikumiem. ►**M1** TRES SECRET UE/EU TOP SECRET ◄ reģistra vadītājs ir ►**M1** TRES SECRET UE/EU TOP SECRET ◄ Reģistra kontrolieris.

2. Centrālais ►**M1** TRES SECRET UE/EU TOP SECRET ◄ reģistrs darbojas kā galvenā Komisijas saņēmēja un nosūtītāja iestāde attiecībā uz citām ES iestādēm, dalībvalstīm, starptautiskām organizācijām un trešām valstīm, ar kuru Komisijai ir nolīgumi par drošības procedūru, ko piemēro klasificētai informācijai.

3. Nepieciešamības gadījumā izveido apakšreģistrus, kas atbild par ►**M1** TRES SECRET UE/EU TOP SECRET ◄ dokumentu iekšēju pārvaldību; tajos uzglabā atjauninātus ierakstus par katra dokumenta apriti, kas atrodas apakšreģistrā.

4. ►**M1** TRES SECRET UE/EU TOP SECRET ◄ apakšreģistrus izveido atbilstoši 22. iedaļas 2.3. punktā noteiktajam, ievērojot ilgtermiņa vajadzības, un tos pievieno centrālajam ►**M1** TRES SECRET UE/EU TOP SECRET ◄ reģistram. Ja ir nepieciešamība

▼B

tikai pagaidām un neregulāri apskatīt ►M1 TRES SECRET UE/EU TOP SECRET ◄ dokumentus, minētos dokumentus var izlaist, neizveidojot ►M1 TRES SECRET UE/EU TOP SECRET ◄ apakšreģistru, ja vien ir izstrādāti noteikumi, kas nodrošina to, ka šādi dokumenti ir atbilstošā ►M1 TRES SECRET UE/EU TOP SECRET ◄ reģistra kontrolē un ka visi fiziskās un personiskās drošības pasākumi ir ievēroti.

5. Apakšreģistri nedrīkst tieši pārsūtīt ►M1 TRES SECRET UE/EU TOP SECRET ◄ dokumentus citiem tā paša centrālā ►M1 TRES SECRET UE/EU TOP SECRET ◄ reģistra apakšreģistriem bez skaidri izteiktas ►M1 TRES SECRET UE/EU TOP SECRET ◄ reģistra atļaujas.

6. Visu ►M1 TRES SECRET UE/EU TOP SECRET ◄ dokumentu apmaiņu starp apakšreģistriem, kas nav pievienoti tam pašam centrālajam reģistram, veic ar centrālā ►M1 TRES SECRET UE/EU TOP SECRET ◄ reģistra starpniecību.

22.2.2. *Centrālais* ►M1 *TRES SECRET UE/EU TOP SECRET* ◄ *informācijas reģistrs*

Centrālā ►M1 TRES SECRET UE/EU TOP SECRET ◄ reģistra vadītājs kā kontrolieris atbild par:

a) ►M1 TRES SECRET UE/EU TOP SECRET ◄ dokumentu pārsūtīšanu atbilstoši noteikumiem, kas ir izklāstīti 21. iedaļas 3. punktā;

b) ►M1 TRES SECRET UE/EU TOP SECRET ◄ apakšreģistru saraksta uzturēšanu kopā ar norīkoto kontrolieru un to atļauto vietnieku vārdiem un parakstiem;

c) paziņojumu par centrālā reģistra izplatīto ►M1 TRES SECRET UE/EU TOP SECRET ◄ dokumentu saņemšanu no reģistriem;

d) ierakstu uzturēšanu par rīcībā esošajiem un izplatītajiem ►M1 TRES SECRET UE/EU TOP SECRET ◄ dokumentiem;

e) atjauninātа saraksta uzturēšanu par visiem centrālajiem ►M1 TRES SECRET UE/EU TOP SECRET ◄ reģistriem, ar kuriem viņš/viņa regulāri uztur saraksti, kā arī par kontrolieru un to atļauto vietnieku vārdiem un parakstiem;

f) fizisku visu ►M1 TRES SECRET UE/EU TOP SECRET ◄ dokumentu aizsardzību, kas atrodas reģistrā atbilstoši 18. iedaļā izklāstītajiem noteikumiem.

22.2.3. ►M1 *TRES SECRET UE/EU TOP SECRET* ◄ *informācijas apakšreģistri*

Centrālā ►M1 TRES SECRET UE/EU TOP SECRET ◄ apakšreģistra vadītājs kā kontrolieris atbild par:

a) ►M1 TRES SECRET UE/EU TOP SECRET ◄ dokumentu pārsūtīšanu atbilstoši noteikumiem, kas ir izklāstīti 21. iedaļas 3. punktā;

b) atjauninātа saraksta uzturēšanu par visām tām personām, kurām ir atļauta piekļuve viņa kontrolē esošai ►M1 TRES SECRET UE/EU TOP SECRET ◄ informācijai;

c) ►M1 TRES SECRET UE/EU TOP SECRET ◄ dokumentu izplatīšanu atbilstoši šādu dokumentu autora norādījumiem vai nepieciešamībai zināt, vispirms pārbaudot to, ka adresātam ir nepieciešamā drošības pielaide;

d) atjauninātu sarakstu uzglabāšanu par visiem ►M1 TRES SECRET UE/EU TOP SECRET ◄ dokumentiem, kas atrodas viņa kontrolē vai cirkulē viņa pārraudzībā, vai kas ir nodoti citiem ►M1 TRES SECRET UE/EU TOP SECRET ◄ reģistriem un visu attiecīgo paziņojumu par saņemšanu uzglabāšanu;

e) atjauninātа saraksta uzturēšanu par tiem ►M1 TRES SECRET UE/EU TOP SECRET ◄ reģistriem, ar kuriem tam ir atļauja apmainīties ar ►M1 TRES SECRET UE/EU TOP SECRET ◄ dokumen-

▼B

tiem, kopā ar to kontrolieru un viņu atļauto vietnieku vārdiem un parakstiem;

f) fizisku visu ►M1 TRES SECRET UE/EU TOP SECRET ◄ dokumentu aizsardzību, kas atrodas apakšreģistrā atbilstoši 18. iedaļā izklāstītajiem noteikumiem.

22.3. **ES klasificētu dokumentu uzskaitījumi, apvienošanas un pārbaudes**

1. Katru gadu katrs ►M1 TRES SECRET UE/EU TOP SECRET ◄ reģistrs, kas ir minēts šajā iedaļā, veic detalizētu ►M1 TRES SECRET UE/EU TOP SECRET ◄ dokumentu uzskaitījumu. Dokumentu uzskata par uzskaitītiem, ja reģistrs fiziski ir apskatījis un pārbaudījis dokumentu, vai tam ir paziņojums par saņemšanu no ►M1 TRES SECRET UE/EU TOP SECRET ◄ reģistra, kuram dokuments ir nodots, apliecinājums par dokumenta iznīcināšanu vai norādījums deklasificēt dokumentu vai pazemināt tā slepenības pakāpi. Vēlākais līdz katra gada 1. aprīlim gada uzskaitījumu atzinumus nosūta Komisijas loceklim, kas atbild par drošības jautājumiem.

2. ►M1 TRES SECRET UE/EU TOP SECRET ◄ apakšreģistri pārsūta savu gada uzskaitījumu atzinumus Centrālajam reģistram, pēc kura pieprasījuma tās ir veiktas, līdz datumam, ko ir norādījis Centrālais reģistrs.

3. Par ES klasificētiem dokumentiem, kuru klasifikācijas pakāpe ir zemāka par ►M1 TRES SECRET UE/EU TOP SECRET ◄, veic iekšējās pārbaudes atbilstoši norādījumiem, kurus sniedz Komisijas loceklis, kas atbild par drošības jautājumiem.

4. Šādas darbības sniedz turētājam iespēju pārliecināties par:

   a) konkrētu dokumentu deklasifikāciju vai slepenības pakāpes pazemināšanu;

   b) dokumentiem, kas jāiznīcina.

22.4. **ES klasificētu dokumentu uzglabāšana arhīvos**

1. *EUCI* uzglabā atbilstoši nosacījumiem, kas ir saskaņā ar visām atbilstošajām prasībām, kuras ir uzskaitītas 18. iedaļā.

2. Lai mazinātu uzglabāšanas problēmas, visu reģistru kontrolieriem ir atļauts uzglabāt ►M1 TRES SECRET UE/EU TOP SECRET ◄, ►M1 SECRET UE ◄ un ►M1 CONFIDENTIEL UE ◄ dokumentus uz mikrofilmām vai citā veidā magnētiskajos vai optiskajos informācijas nesējos arhivēšanas nolūkos, ja:

   a) mikrofilmēšanu/uzglabāšanu veic personāls, kam ir atļauja piekļūt attiecīgās klasifikācijas pakāpes dokumentiem;

   b) mikrofilmu/uzglabājošos informācijas nesējus aizsargā tāpat kā dokumentu oriģinālus;

   c) par ►M1 TRES SECRET UE/EU TOP SECRET ◄ dokumenta mikrofilmēšanu/uzglabāšanu paziņo dokumenta autoram;

   d) filmiņas vai citi atbalsta veidi satur dokumentus ar vienādu ►M1 TRES SECRET UE/EU TOP SECRET ◄, ►M1 SECRET UE ◄ vai ►M1 CONFIDENTIEL UE ◄ klasifikāciju;

   e) ►M1 TRES SECRET UE/EU TOP SECRET ◄ vai ►M1 SECRET UE ◄ dokumenta mikrofilmēšana/uzglabāšana ir skaidri norādīta ierakstā, ko izmanto gada uzskaitījumam;

   f) dokumentu oriģināli, kas ir mikrofilmēti vai citādi saglabāti, iznīcina saskaņā ar 22. iedaļas 5. punktā izklāstītajiem noteikumiem.

3. Šos noteikumus piemēro arī citiem atļautas uzglabāšanas veidiem, tādiem kā elektromagnētiskie informācijas nesēji un optiskais disks.

▼B

22.5. **ES klasificētu dokumentu iznīcināšana**

1. Lai novērstu nevajadzīgu ES klasificētu dokumentu uzkrāšanu, dokumentus, kurus tā departamenta vadītājs, kā rīcībā tie atrodas, uzskata par novecojušiem un vairākās kopijās pēc iespējas ātrāk iznīcina šādi:

   a) ►M1 TRES SECRET UE/EU TOP SECRET ◄ dokumentus iznīcina tikai tas Centrālais reģistrs, kas par tiem atbild. Katru iznīcināto dokumentu uzskaita apliecībā par iznīcināšanu, ko ir parakstījis ►M1 TRES SECRET UE/EU TOP SECRET ◄ kontrolieris un ierēdnis, kurš ir iznīcināšanas liecinieks; šādai personai jābūt piekļuvei ►M1 TRES SECRET UE/EU TOP SECRET ◄ informācijai. Par iznīcināšanu žurnālā ieraksta piezīmi;

   b) reģistrs 10 gadus glabā apliecības par iznīcināšanu un aprites veidlapas; Kopijas nosūta dokumenta autoram vai atbilstošam centrālajam reģistram tikai pēc skaidra pieprasījuma;

   c) ►M1 TRES SECRET UE/EU TOP SECRET ◄ dokumenti, tostarp visus ES klasificētas informācijas atkritumus, kas rodas no ►M1 TRES SECRET UE/EU TOP SECRET ◄ dokumentu sagatavošanas, piemēram, bojātas kopijas, darba melnrakstus, drukātas piezīmes, disketes, iznīcina ►M1 TRES SECRET UE/EU TOP SECRET ◄ Reģistra kontroliera klātbūtnē, tos sadedzinot, sasmalcinot, saplēšot vai citādi pārveidojot līdz neatpazīstamai un neatjaunojamai formai.

2. ►M1 SECRET UE ◄ dokumentus iznīcina reģistrs, kas par tiem atbild, tādas personas klātbūtnē, kurai ir drošības pielaide, izmantojot vienu no 1. punkta c) apakšpunktā izklāstītajiem veidiem. Iznīcinātos ►M1 SECRET UE ◄ dokumentus uzskaita parakstītās apliecībās par iznīcināšanu, kuras vismaz trīs gadus uzglabā reģistrs, tām pievienojot aprites veidlapas.

3. ►M1 CONFIDENTIEL UE ◄ dokumentus iznīcina reģistrs, kas par tiem atbild, tādas personas klātbūtnē, kurai ir drošības pielaide, izmantojot vienu no 1. punkta c) apakšpunktā izklāstītajiem veidiem. To iznīcināšanu reģistrē saskaņā ar norādījumiem, kurus sniedz Komisijas loceklis, kas atbild par drošības jautājumiem.

4. ►M1 RESTREINT UE ◄ dokumentus iznīcina reģistrs, kas par tiem atbild, vai lietotājs atbilstoši norādījumiem, kurus sniedz Komisijas loceklis, kas atbild par drošības jautājumiem.

22.6. **Iznīcināšana ārkārtas gadījumos**

1. Pamatojoties uz vietējiem noteikumiem, Komisijas struktūrvienības izstrādā plānus ES klasificēta materiāla pasargāšanai krīzes gadījumos, tostarp, vajadzības gadījumā, iznīcināšanu ārkārtas gadījumos un evakuācijas plānus. Ar tiem izsludina norādījumus, kas ir nepieciešami, lai novērstu ES klasificētas informācijas nokļūšanu neatļautu personu rokās.

2. Pasākumi ►M1 SECRET UE ◄ un ►M1 CONFIDENTIEL UE ◄ materiāla aizsardzībai un/vai iznīcināšanai krīzes gadījumā nekādā veidā nedrīkst negatīvi ietekmēt ►M1 TRES SECRET UE/EU TOP SECRET ◄ materiāla aizsargāšanu vai iznīcināšanu, tostarp šifrēšanas aprīkojumu, kura aizsargāšana vienmēr ir prioritāra.

3. Īpašos norādījumos ir izklāstīti pasākumi, ko veic šifrēšanas aprīkojuma aizsardzībai un iznīcināšanai ārkārtas gadījumos.

4. Norādījumi ir pieejami uz vietas aizzīmogotās aploksnēs. Jābūt pieejamiem iznīcināšanas veidiem/iekārtām.

▼B

23. DROŠĪBAS PASĀKUMI ĪPAŠĀS SANĀKSMĒS, KAS NOTIEK ĀRPUS KOMISIJAS TELPĀM UN KURĀS TIEK IZSKATĪTA ES KLASIFICĒTA INFORMĀCIJA

23.1. **Vispārīgi**

Ja Komisijas vai citas svarīgas sanāksmes notiek ārpus Komisijas telpām un to pamato īpašas drošības prasības, kas attiecas uz izskatāmo jautājumu vai informācijas augsto jutīgumu, veic turpmāk izklāstītos drošības pasākumus. Šie pasākumi attiecas tikai uz ES klasificētas informācijas aizsardzību; var plānot citus drošības pasākumus.

23.2. **Pienākumi**

23.2.1. ►M2 Komisijas Drošības direktorāts ◄

►M2 Komisijas Drošības direktorāts ◄ sadarbojas ar citām dalībvalstu kompetentām iestādēm, kuru teritorijā notiks sanāksmes (uzņēmēju dalībvalsti), lai nodrošinātu Komisijas vai citu svarīgu tikšanos drošību un delegātu un to darbinieku drošību. Attiecībā uz drošības aizsardzību tas jo īpaši nodrošina:

a) plānu izstrādi, kas izskata draudus drošībai un ar drošību saistītus starpgadījumus, attiecīgos pasākumus, kuri jo īpaši iekļauj ES klasificētu dokumentu uzglabāšanu biroju seifos;

b) pasākumu veikšanu, lai sniegtu piekļuvi Komisijas komunikāciju sistēmai ES klasificētu ziņojumu saņemšanas un pārsūtīšanas nolūkiem. Uzņēmējai dalībvalstij pēc pieprasījuma jānodrošina piekļuve drošām tālruņu sistēmām.

►M2 Komisijas Drošības direktorāts ◄ darbojas kā padomdevējs drošības jautājumos sanāksmes sagatavošanas procesā; tas ir pārstāvēts sanāksmēs, lai nepieciešamības gadījumā palīdzētu un sniegtu padomus sanāksmes drošības speciālistam (*MSO*) un delegācijām.

Katra sanāksmes delegācija ieceļ drošības speciālistu, kas atbild par drošības jautājumiem savā delegācijā un par sadarbību ar sanāksmes drošības speciālistu, kā arī ar ►M2 Komisijas Drošības direktorāta ◄ pārstāvi.

23.2.2. *Sanāksmes drošības speciālists (MSO)*

Sanāksmes drošības speciālists ir norīkots un atbild par vispārēju sagatavošanu un vispārēju iekšēju drošības pasākumu kontroli, un par koordināciju ar citām attiecīgajām drošības iestādēm. Sanāksmes drošības speciālista veiktie pasākumi parasti attiecas uz:

a) aizsardzības pasākumiem sanāksmes vietā, lai nodrošinātu to, ka sanāksme norisinās bez starpgadījumiem, kuri var kompromitēt jebkuru ES klasificētu informāciju, ko var izmantot sanāksmē;

b) personāla pārbaudi, kuriem ir atļauta piekļuve sanāksmes vietai, delegāciju atrašanās vietām un konferenču vietām, un jebkuru iekārtu pārbaudi;

c) pastāvīgu sadarbību ar uzņēmējas dalībvalsts kompetentām iestādēm un ar ►M2 Komisijas Drošības direktorātu ◄;

d) drošības norādījumu iekļaušanu sanāksmes dokumentācijā, ņemot vērā prasības, kas ir izklāstītas šajos drošības noteikumos un jebkuros citos drošības noteikumos, kurus uzskata par nepieciešamiem.

23.3. **Drošības pasākumi**

23.3.1. *Drošības zonas*

Izveido šādas drošības zonas:

a) II līmeņa drošības zona, ko veido telpas dokumentu izstrādāšanai, Komisijas biroji un pavairošanas iekārtas, kā arī attiecīgā gadījumā delegāciju biroji;

▼B

b) I līmeņa drošības zona, ko veido konferenču telpas un tulku un skaņu inženieru kabīnes;

c) administratīvā zona, ko veido telpas presei un tās sanāksmes vietas daļas, kuras izmanto administrācijai, ēdināšanai un izmitināšanai, kā arī zona, kas ir tieši savienota ar preses centru un sanāksmes vietu.

23.3.2. *Caurlaides*

Sanāksmes drošības speciālists izsniedz piemērotas personas kartes, kuras ir pieprasījušas delegācijas, pamatojoties uz to vajadzībām. Pēc pieprasījuma tās var izšķirt pēc piekļuves dažādām drošības zonām.

Sanāksmes drošības norādes iekļauj prasību visām attiecīgajām personām valkāt un uzrādīt to personas kartes sanāksmes vietās, lai drošības personāls nepieciešamības gadījumā varētu tās pārbaudīt.

Papildus personas karšu turētājiem sanāksmes vietā ielaiž pēc iespējas mazāk cilvēku. Sanāksmes drošības speciālists atļauj valstu delegācijām uzņemt apmeklētājus sanāksmes laikā tikai pēc to pieprasījuma. Apmeklētājiem izsniedz apmeklētāja karti. Aizpilda apmeklētāja karti, uz kuras ir norādīts viņa/viņas vārds un apmeklējamās personas vārds. Apmeklētājus visu laiku pavada apsargs vai apmeklējamā persona. Apmeklētāja caurlaides veidlapa atrodas pie pavadošās personas, kas to atdod kopā ar apmeklētāja karti drošības personālam pēc tam, kad apmeklētājs ir atstājis sanāksmes vietu.

23.3.3. *Foto un audio aprīkojuma kontrole*

I līmeņa drošības zonā nedrīkst ienest kameras vai ieraksta aparatūru, izņemot to aprīkojumu, ko ienes fotogrāfi un skaņu inženieri, kuriem ir atbilstošas sanāksmes drošības speciālista atļaujas.

23.3.4. *Portfeļu, pārnēsājamo datoru un iepakojumu pārbaude*

Personas karšu turētāji, kuriem ir piekļuve drošības zonai, parasti var ienest portfeļus un pārnēsājamos datorus (tikai ar savu barošanas bloku) bez pārbaudes. Attiecībā uz delegācijām adresētu iepakojumu delegācijas var pieņemt iepakojumus, ko ir pārbaudījis vai nu delegācijas drošības speciālists, vai kas ir pārbaudītas ar īpaša aprīkojuma palīdzību, vai ko pārbaudes nolūkos ir atvēris drošības personāls. Ja sanāksmes drošības speciālists uzskata to par vajadzīgu, portfeļu un iepakojumu pārbaudei var pieņemt stingrākus noteikumus.

23.3.5. *Tehniskā drošība*

Tehniskās drošības vienība var padarīt sanāksmes telpu tehniski drošu un sanāksmes laikā var veikt elektronisku novērošanu.

23.3.6. *Delegācijas dokumenti*

Delegācijas atbild par ES klasificētu dokumentu ienešanu sanāksmēs un aiznešanu no tās. Tās atbild arī par minēto dokumentu pārbaudi un drošību to izmantošanas laikā telpās, kas ir tiem piešķirtas. Uzņēmēja dalībvalsts var pieprasīt klasificētu dokumentu pārvadāšanu uz sanāksmes vietu un no tās.

23.3.7. *Dokumentu uzglabāšana seifos*

Ja Komisija vai delegācijas nespēj uzglabāt to klasificētos dokumentus saskaņā ar apstiprinātajiem standartiem, tās var iesniegt dokumentus aizzīmogotā aploksnē sanāksmes drošības speciālistam pret izziņu par saņemšanu, lai sanāksmes drošības speciālists varētu uzglabāt dokumentus atbilstoši apstiprinātajiem standartiem.

23.3.8. *Biroju pārbaude*

Sanāksmes drošības speciālists iekārto Komisijas un delegāciju birojus, ko pārbauda katras darba dienas beigās, lai nodrošinātu ES klasificētu dokumentu uzglabāšanu drošā vietā. Ja tas tā nav, viņš/viņa veic atbilstošus pasākumus.

▼B

23.3.9. *ES klasificēto atkritumu iznīcināšana*

Visus atkritumus uzskata par ES klasificētiem; papīrgrozus vai maisus atdod Komisijai un delegācijām šādu atkritumu iznīcināšanai. Pirms telpu atstāšanas, kas ir tiem piešķirtas, Komisija un delegācijas nodod atkritumus sanāksmes drošības speciālistam, kurš organizē to iznīcināšanu atbilstoši noteikumiem.

Pēc sanāksmes visus dokumentus, kuri ir Komisijas vai delegāciju rīcībā, taču kurus tās neuzskata par vajadzīgiem, uzskata par atkritumiem. Pirms atceļ sanāksmei noteiktos drošības pasākumus, visas Komisijas un delegāciju telpas kārtīgi pārmeklē. Dokumentus, par kuriem ir parakstīta izziņa par saņemšanu, ciktāl to var piemērot, iznīcina atbilstoši 22. iedaļas 5. punktā izklāstītajam.

## 24. DROŠĪBAS PĀRKĀPUMS UN ES KLASIFICĒTAS INFORMĀCIJAS KOMPROMITĒŠANA

### 24.1. **Definīcijas**

Drošība tiek pārkāpta, ja tādas darbības vai bezdarbības rezultātā, kas ir pretrunā ar Komisijas drošības noteikumiem, tiek apdraudēta vai kompromitēta ES klasificēta informācija.

ES klasificēta informācija tiek kompromitēta, kad tā pilnīgi vai daļēji nokļūst neatļautu personu rokās, piemēram, tādu personu rokās, kam nav atbilstošas drošības pielaides vai nepieciešamās vajadzības zināt, vai ir iespēja, ka šāds gadījums ir noticis.

ES klasificēta informācija var būt kompromitēta paviršības, neuzmanības vai neapdomības rezultātā, kā arī tādu dienestu darbību rezultātā, kuru mērķis ir ES vai tās dalībvalstis attiecībā uz ES klasificētu informāciju un darbībām, vai graujošu organizāciju darbības rezultātā.

### 24.2. **Paziņošana par drošības pārkāpumiem**

Visas personas, kurām jāapstrādā ES klasificēta informācija, pilnīgi informē par to atbildību. Tās nekavējoties ziņo par jebkuru drošības pārkāpumu, kas tām ir tapis zināms.

Kad vietējais drošības speciālists vai sanāksmes drošības speciālists atklāj vai tiek informēts par drošības pārkāpumu attiecībā uz ES klasificētu informāciju vai ES klasificētu materiālu pazaudēšanu vai pazušanu, viņš vai viņa nekavējoties veic pasākumus, lai:

a) pasargātu pierādījumus;

b) noskaidrotu faktus;

c) izvērtētu un mazinātu radušos zaudējumus;

d) novērstu šādu notikumu atkārtošanos;

e) paziņotu atbilstošām iestādēm par drošības pārkāpumu sekām.

Šajā sakarā sniedz šādu informāciju:

i) iesaistītās informācijas aprakstu, tostarp tās klasifikāciju, atsauci un kopijas numuru, datumu, autoru, tematu un darbības jomu;

ii) īsu aprakstu par apstākļiem, kuros noticis drošības pārkāpums, tostarp datumu un laika posmu, kurā informācija tika atklāta kompromitēšanai;

iii) paziņojumu par to, vai informācijas autors ir informēts.

Katras drošības iestādes pienākums, tiklīdz tai ir paziņots par šādu drošības pārkāpumu, ir nekavējoties ziņot ►**M2** Komisijas Drošības direktorātam ◄.

Ja ir iesaistīta ►**M1** RESTREINT UE ◄ informācija, ziņo tikai tad, ja šādai informācijai ir neparastas iezīmes.

Pēc informācijas saņemšanas par šādu drošības pārkāpumu, Komisijas loceklis, kas atbild par drošības jautājumiem:

▼B

a) paziņo iestādei, kura ir izstrādājusi attiecīgo klasificēto informāciju;

b) lūdz atbilstošām drošības iestādēm sākt izmeklēšanu;

c) koordinē pieprasījumus, ja ir iesaistīta vairāk kā viena drošības iestāde;

d) iegūst ziņojumu par apstākļiem, kuros ir noticis pārkāpums, datumu vai laika posmu, kurā tas varēja notikt vai tika atklāts, kā arī sīku aprakstu par iesaistītā materiāla saturu un klasifikāciju. Tiek paziņoti arī zaudējumi, kas nodarīti ES vai vienai vai vairākām tās dalībvalstīm, un darbības, kuras ir veiktas, lai novērstu atkārtošanos.

Iestāde, kas ir dokumenta autors, informē adresātus un sniedz tiem atbilstošus norādījumus.

24.3. **Tiesiska darbība**

Katra persona, kas ir atbildīga par ES klasificētas informācijas kompromitēšanu, ir disciplināri atbildīga atbilstoši attiecīgajiem noteikumiem, jo īpaši Civildienesta noteikumu VI nodaļai. Šāda tiesvedība neierobežo jebkuru citu tiesisku darbību.

Attiecīgos gadījumos, pamatojoties uz 24. iedaļas 2. punktā minēto ziņojumu, Komisijas loceklis, kas atbild par drošības jautājumiem, veic nepieciešamos pasākumus, lai ļautu kompetentām valsts iestādēm sākt kriminālvajāšanu.

25. ES KLASIFICĒTAS INFORMĀCIJAS AIZSARDZĪBA, KO APSTRĀDĀ AR INFORMĀCIJAS TEHNOLOĢIJU UN KOMUNIKĀCIJAS SISTĒMU PALĪDZĪBU

25.1. **Ievads**

25.1.1. *Vispārīgi*

Drošības politiku un prasības piemēro visām komunikācijas un informācijas sistēmām un tīkliem (še turpmāk — sistēmām), kas apstrādā informāciju ar klasifikācijas pakāpi ►M1 CONFIDENTIEL UE ◄ vai augstāku. Tos piemēro papildus Komisijas 1995. gada 23. novembra galīgajam Lēmumam C (95) 1510 par informātikas sistēmu aizsardzību.

Sistēmām, kas apstrādā ►M1 RESTREINT UE ◄ informāciju, piemēro drošības pasākumus, lai aizsargātu šādas informācijas konfidencialitāti. Visām sistēmām nepieciešami drošības pasākumi, lai aizsargātu šādu sistēmu un informācijas, ko tās satur, integritāti un pieejamību.

IT drošības politikai, ko piemēro Komisija, ir šādas iezīmes:

— tā ir neatņemama drošības sastāvdaļa un papildina visus informācijas drošības elementus, personāla drošību un fizisko drošību,

— tā sadala atbildību starp tehnisko sistēmu īpašniekiem, *EUCI* īpašniekiem, ko uzglabā vai apstrādā tehniskajās sistēmās, IT drošības speciālistiem un lietotājiem,

— tā apraksta drošības principus un prasības katrai IT sistēmai,

— tā apstiprina šādus principus un atbildīgās iestādes prasības,

— tā ņem vērā īpašus draudus un IT sistēmu neaizsargātību.

25.1.2. *Draudi sistēmām un to neaizsargātība*

Draudus var raksturot kā nejaušu vai apzinātu drošības kompromitēšanu. Attiecībā uz sistēmu šāda kompromitēšana iekļauj vienu vai vairāku konfidencialitātes, integritātes un pieejamības iezīmju zaudēšanu. Neaizsargātību var raksturot kā vājību vai kontroles neesamību, kas veicina vai pieļauj draudus noteiktai lietai vai mērķim.

ES klasificēta un neklasificēta informācija, ko apstrādā sistēmās koncentrētā formā, kura ir domāta ātrai iegūšanai, komunikācijai un izmantošanai ir neaizsargāta pret daudziem draudiem. Tie iekļauj neatļautu personu piekļuvi informācijai vai, otrādi, piekļuves liegšanu atļautām personām. Turklāt pastāv neatļautas informācijas atklāšanas, bojāšanas,

▼B

pārveidošanas vai izdzēšanas draudi. Turklāt sarežģītais un dažreiz trauslais aprīkojums ir dārgs un bieži vien to ir grūti salabot vai aizvietot.

25.1.3. *Drošības pasākumu galvenais mērķis*

Šajā iedaļā izklāstīto drošības pasākumu galvenais mērķis ir sniegt aizsardzību pret neatļautu ES klasificētas informācijas atklāšanu (konfidencialitātes zaudēšanu) un pret integritātes vai informācijas pieejamības zaudēšanu. Lai sasniegtu atbilstošu tādu sistēmu aizsardzību, kurās apstrādā ES klasificētu informāciju, ►**M2** Komisijas Drošības direktorāts ◄ nosaka atbilstošus parastos drošības standartus, kā arī atbilstošas īpašas drošības procedūras un metodes, kas ir izstrādātas katrai sistēmai.

25.1.4. *Sistēmas drošības prasību izklāsts (SSRS)*

Visām sistēmām, kas apstrādā informāciju ar klasifikācijas pakāpi ►**M1** CONFIDENTIEL UE ◄ vai augstāku, nepieciešams izstrādāt sistēmas drošības prasību izklāstu (*SSRS*), kuru veic tehniskais sistēmas īpašnieks (*TSO*, skatīt 25. iedaļas 3.4. punktu) un informācijas īpašnieks (skatīt 25. iedaļas 3.5. punktu), kas sadarbojas un kam palīdz projekta personāls un ►**M2** Komisijas Drošības direktorāts ◄ (kā *INFOSEC* iestāde, skatīt 25. iedaļas 3.3. punktu), un ko apstiprina Drošības akreditācijas iestāde (*SAA*, skatīt 25. iedaļas 3.2. punktu).

*SSRS* ir nepieciešams arī tad, ja Drošības akreditācijas iestāde uzskata, ka ►**M1** RESTREINT UE ◄ vai neklasificētas informācijas pieejamība un integritāte ir kritiska.

*SSRS* formulē projekta uzsākšanas sākumā un attīsta un uzlabo projekta gaitā; *SSRS* dažādos projekta posmos un sistēmas aprites ciklā ir dažādas lomas.

25.1.5. *Drošības ekspluatācijas metodes*

Visas sistēmas, kas apstrādā informāciju ar klasifikācijas līmeni ►**M1** CONFIDENTIEL UE ◄ vai augstāku, ir akreditētas darbībai vienā vai, ja to nodrošina prasības dažādos laika posmos, vairāk nekā vienā sekojošā drošības ekspluatācijas metodēsvai līdzvērtīgā valsts sistēmā:

a) specializētā,

b) augstā drošības sistēmā un

c) daudzpakāpju.

25.2. **Definīcijas**

"Akreditācija" ir autorizācija un apstiprinājums, ko piešķir sistēmai, lai apstrādātu ES klasificētu informāciju tās darbības vidē.

Piezīme:

šādu akreditāciju piešķir pēc visu atbilstošo drošības procedūru ieviešanas un pēc tam, kad ir sasniegts pietiekošs sistēmas resursu aizsardzības līmenis. Parasti akreditāciju piešķir, pamatojoties uz *SSRS*, tostarp:

a) paziņojumu par sistēmas akreditācijas mērķi; jo īpaši, kāda klasifikācijas līmeņa informācija tiks apstrādāta un kāds drošības režīms ir piedāvāts sistēmas darbībai;

b) riska pārvaldības pārskata izstrādi, lai noteiktu draudus un neaizsargātību, kā arī pasākumus to novēršanai;

c) drošības ekspluatācijas procedūras (*SecOPs*) ar sīku aprakstu par ieteikto darbību (piemēram, veidi, pakalpojumi, kas tiks sniegti) un tostarp aprakstu par sistēmas drošības iezīmēm, ar kurām pamatota akreditācija;

d) plānu drošības iezīmju īstenošanai un uzturēšanai;

e) plānu sākotnējai un turpmākai sistēmas drošībai vai tīkla drošības pārbaudei, izvērtēšanai un sertifikācijai, un

▼B

f) sertifikāciju, ja pieprasa, kopā ar citiem akreditācijas elementiem.

“Centrālais informācijas drošības speciālists” (*CISO*) ir ierēdnis centrālajā IT dienestā, kas koordinē un pārrauga drošības pasākumus centralizēti organizētām sistēmām.

“Sertifikācija” ir oficiāla paziņojuma izsniegšana, ko papildina neatkarīgs pārskats par izvērtēšanas gaitu un rezultātiem, sistēmas atbilstības drošības prasībām līmenis vai datordrošības atbilstības iepriekšnoteiktām drošības prasībām līmenis.

“Komunikācijas drošība” (*COMSEC*) ir drošības pasākumu piemērošana telekomunikācijām, lai liegtu neatļautām personām piekļuvi vērtīgai informāciju, kas var izrietēt no šādu telekomunikāciju turēšanas vai izpētes, vai lai nodrošinātu šādu telekomunikāciju autentiskumu.

Piezīme:

Šādi pasākumi iekļauj kriptogrāfijas, pārsūtīšanas un izsūtīšanas drošību; kā arī procesuālo, personisko, dokumentu un datoru drošību.

“Datoru drošība” (*COMPUSEC*) ir datortehnikas, programmaparatūras un programmatūras drošības iezīmju piemērošana datorsistēmai, lai aizsargātu vai novērstu neatļautu informācijas atklāšanu, manipulāciju, sagrozīšanu/izdzēšanu vai pakalpojumu liegšanu.

“Datoru drošība produkts” ir vispārējs datoru drošības priekšmets, kas ir domāts ievietošanai IT sistēmā un kas uzlabo vai sniedz apstrādājamai informācijai konfidencialitāti, integritāti vai pieejamību.

“Darbība specializētā drošības režīmā” ir darbības režīms, kurā visām personām, kam ir piekļuve sistēmai, ir atļauja piekļūt augstākās klasifikācijas informācijai, kuru apstrādā sistēmā, kā arī kopīga nepieciešamība zināt visu informāciju, ko apstrādā sistēmā.

Piezīmes:

1) Kopīga nepieciešamība zināt norāda uz obligātu prasību neesamību datoru drošības iezīmēm, lai tās nodalītu informāciju, kas atrodas sistēmā.

2) Citas drošības iezīmes (piemēram, fiziskās, personiskās un procesuālās) atbilst augstākā klasifikācijas līmeņa prasībām un visiem sistēmā apstrādātās informācijas kategoriju apzīmējumiem.

“Izvērtēšana” ir sīka sistēmas vai kriptogrāfijas vai datoru drošības produkta drošības aspektu tehniska pārbaude, ko veic atbilstoša iestāde.

Piezīmes:

1) Izvērtēšanā pārbauda prasītās drošības darbības esamību un šādu darbību kompromitējošu blakus efektu neesamību, kā arī izvērtē šādas darbības neuzpērkamību.

2) Izvērtēšana nosaka, ciktāl ir izpildītas sistēmas drošības prasības vai datoru drošības produkta drošības prasības, kā arī nosaka sistēmai vai kriptogrāfijai, vai datoru drošības produktam uzticētās funkcijas nodrošinājuma līmeni.

“Informācijas īpašnieks” (*IO*) ir iestāde (struktūrvienības vadītājs), kas atbild par informācijas izstrādāšanu, apstrādi un izmantošanu, tostarp lēmumu pieņemšanu par to, kuram ir piekļuve informācijai.

“Informācijas drošība” (*INFOSEC*) ir drošības pasākumu piemērošana, lai aizsargātu komunikācijas, informācijas un citās elektroniskās sistēmās apstrādāto, uzglabāto vai pārsūtīto informāciju no konfidencialitātes, integritātes vai pieejamības zaudēšanas, neskatoties uz to, vai tā ir nejauša vai tīša, kā arī novērst pašu sistēmu integritātes un pieejamības zaudēšanu.

“*INFOSEC pasākumi*” iekļauj datoru, pārsūtīšanas, izsniegšanas un kriptogrāfijas drošību, kā arī informācijas un sistēmu draudu noteikšanu, reģistrēšanu un novēršanu.

▼B

"IT zona" ir zona, kurā atrodas viens vai vairāki datori, to vietējās perifērās un uzglabāšanas iekārtas, kontroles iekārtas un specializēts tīkls, un komunikāciju aprīkojums.

Piezīme:

Tā neiekļauj atsevišķu zonu, kurā atrodas attālas perifērās iekārtas vai termināļi/darbstacijas, lai arī šādas iekārtas ir savienotas ar iekārtām, kas atrodas IT zonā.

"IT tīkls" ir ģeogrāfiski izkliedēta IT sistēmu organizācija, kas ir savienotas ar datu apmaiņu, un iekļauj savstarpēji savienotās IT sistēmas un to pieslēgumus kopā ar to datiem vai komunikāciju tīkliem.

Piezīmes:

1) IT tīkls var izmantot viena vai vairāku tādu komunikācijas tīklu pakalpojumus, kas ir savienoti ar datu apmaiņu; vairāki IT tīkli var izmantot kopīga komunikācijas tīkla pakalpojumus.

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

"IT tīkla drošības iezīmes" iekļauj atsevišķu IT sistēmu drošības iezīmes, kas kopā ar papildu sastāvdaļām un iezīmēm, kuras piemīt tīklam (piemēram, tīkla komunikācija, drošības noteikšana un marķējuma mehānismi un procedūra, piekļuves kontrole, programmas un auditācijas pieraksts) veido tīklu, kas ir nepieciešams, lai sniegtu apmierinošu aizsardzību klasificētai informācijai.

"IT sistēma" ir iekārtu, metožu un procedūru un, vajadzības gadījumā, personāla savienojums, kas ir izveidots, lai apstrādātu informāciju.

Piezīmes:

1) Tā nozīmē tādu ierīču savienojumu, kas ir pielāgotas informācijas apstrādei sistēmā.

2) Šādas sistēmas var papildināt konsultējošās, pavēlošās, kontroles, komunikāciju, zinātniskās vai administratīvās lietojumprogrammas, tostarp tekstapstrādi.

3) Sistēmas robežas parasti ir tie elementi, ko kontrolē viens tehniskās sistēmas īpašnieks.

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

"IT sistēmas drošības iezīmes" iekļauj visas datortehnikas/programmaparatūras/programmatūras darbības un iezīmes; darbības procedūras, pārskatu sniegšanas procedūras un piekļuves kontroles, IT zona, attālais terminālis/darbstacija, pārvaldības ierobežojumi, fiziskā drošība un iekārtas, personāla un komunikācijas kontroles sniedz apmierinošu tādas klasificētas informācijas aizsardzību, kas tiks apstrādāta IT sistēmā.

"Vietējais IT drošības speciālists" (*LISO*) ir ierēdnis Komisijas struktūrvienībā, kas atbild par tā pārziņā esošu drošības pasākumu koordinēšanu un pārraudzīšanu.

"Darbība daudzpakāpju drošības režīmā" ir darbības režīms, kurā ne visām personām, kam ir piekļuve sistēmai, ir atļauja piekļūt augstākās klasifikācijas informācijai, kuru apstrādā sistēmā, kā arī ne visām personām, kam ir piekļuve sistēmai, ir kopīga nepieciešamība zināt informāciju, kuru apstrādā sistēmā.

Piezīmes:

1) Šis darbības režīms pašlaik atļauj dažādu klasifikācijas līmeņu informācijas apstrādi un jauktus informācijas kategoriju apzīmējumus.

2) Tas, ka ne visām personām ir piekļuve augstākās klasifikācijas pakāpēm, kas izriet no tā, ka nav nepieciešamības zināt, nozīmē,

▼B

ka datoru drošības iezīmēm jāsniedz atšķirīga piekļuve informācijai, kura atrodas sistēmā, un šāda informācija ir jānodala.

"Attāla termināļa/darbstacijas zona" ir no IT zonas nodalīta zona, kurā atrodas atsevišķs datoraprīkojums, tā perifērās ierīces vai termināļi/darbstacijas un jebkuras saistītās iekārtas.

"Drošības ekspluatācijas procedūras" ir procedūras, ko izstrādā tehniskās sistēmas īpašnieks un kas nosaka principus, kurus piemēro drošības jautājumiem, darbības procedūru un personāla pienākumus.

"Darbība augstā sistēmas drošības režīmā" ir darbības režīms, kurā visām personām, kam ir piekļuve sistēmai, ir atļauja piekļūt augstākās klasifikācijas informācijai, kuru apstrādā sistēmā, tomēr ne visām personām, kam ir piekļuve sistēmai, ir kopīga nepieciešamība zināt informāciju, kuru apstrādā sistēmā.

Piezīmes:

1) Tas, ka nav kopīgas nepieciešamības zināt, norāda uz prasību neesamību attiecībā uz datoru drošības iezīmēm, lai tās izšķirtu piekļuvi informācijai un nodalītu šādu informāciju.

2) Citas drošības iezīmes (piemēram, fiziskās, personiskās un procesuālās) atbilst augstākā klasifikācijas līmeņa prasībām un visiem sistēmā apstrādātās informācijas kategoriju apzīmējumiem.

3) Visu informāciju, ko apstrādā vai kas ir pieejama sistēmā šajā drošības režīmā, kā arī sagatavotos rezultātus aizsargā kā tādu, kurai potenciāli ir informācijas kategorijas apzīmējums un augstākais klasifikācijas līmenis, kamēr nav noteikts citādi, ja vien ir pietiekoši ticams, ka to var aizvietot jebkurā esošā marķējuma darbībā.

"Sistēmas drošības prasību izklāsts" (*SSRS*) ir pilnīgs un skaidrs ievērojamo drošības principu izklāsts un sīks izpildāmo drošības prasību apraksts. Tas pamatojas ar Komisijas drošības politiku un risku izvērtējumu, vai to norāda parametri, kas iekļauj darbības vidi, zemāko personāla drošības pielaidi, augstāko apstrādātās informācijas klasifikācijas līmeni, darbības drošības režīmu vai prasības lietotājiem. *SSRS* ir neatņemama projekta dokumentācijas sastāvdaļa, ko iesniedz atbilstošām iestādēm tehniskas, budžeta un drošības apstiprināšanas nolūkos. Savā galīgajā veidolā *SSRS* ir pilnīgs sistēmas drošības būtības izklāsts.

"Tehniskās sistēmas īpašnieks" (*TSO*) ir iestāde, kas atbild par sistēmas izveidošanu, uzturēšanu, darbību un slēgšanu.

"Tempest" pretpasākumi ir drošības pasākumi, kas aizsargā iekārtas un komunikācijas infrastruktūru no klasificētas informācijas kompromitēšanas netīšas elektromagnētiskas noplūdes un vadītspējas rezultātā.

25.3. **Atbildība par drošību**

25.3.1. *Vispārīgi*

Komisijas drošības politikas konsultatīvās grupas atbildība par drošību, kas ir izklāstīta 12. iedaļā, iekļauj *INFOSEC* jautājumus. Grupa organizē darbību tā, lai tā spētu sniegt ekspertu viedokli iepriekšminētajos jautājumos.

►M2 Komisijas Drošības direktorāts ◄ atbild par *INFOSEC* noteikumu sīku izstrādi, kas pamatota ar šīs iedaļas noteikumiem.

Attiecībā uz drošības problēmām (starpgadījumi, pārkāpumi u.c.), ►M2 Komisijas Drošības direktorāts ◄ nekavējoties veic pasākumus.

►M2 Komisijas Drošības direktorātā ◄ ir *INFOSEC* vienība.

25.3.2. *Drošības akreditācijas iestāde (SAA)*

►M2 Komisijas Drošības direktorāta direktors ◄ ir Drošības akreditācijas iestāde (*SAA*) Komisijā. *SAA* atbild vispārīgi par drošības jomu un par specializētām *INFOSEC* jomām, komunikāciju drošību, Kripto drošību un Tempest drošību.

▼B

*SAA* atbild par sistēmas atbilstības Komisijas drošības politikai nodrošināšanu. Viens no tās uzdevumiem ir sniegt atļauju sistēmai apstrādāt ES klasificētu informāciju līdz noteiktam klasifikācijas līmenim tās darbības vidē.

Komisijas *SAA* jurisdikcija iekļauj visas sistēmas, kas darbojas Komisijas telpās. Ja Komisijas *SAA* un citu *SAA* jurisdikcijā nonāk dažādas sistēmas sastāvdaļas, visas iesaistītās puses var norīkot vienotu akreditācijas padomi, ko koordinē Komisijas *SAA*.

25.3.3. *INFOSEC iestāde (IA)*

►M2 Komisijas Drošības direktorātā ◄ *INFOSEC* vienības vadītājs ir *INFOSEC* iestāde Komisijā. *INFOSEC* iestāde:

— sniedz tehniska rakstura padomus un palīdzību *SAA*,

— palīdz attīstīt *SSRS*,

— pārskata *SSRS*, lai nodrošinātu atbilstību šiem drošības noteikumiem un *INFOSEC* politikai un arhitektūras dokumentiem,

— nepieciešamības gadījumā piedalās akreditācijas padomēs un sniedz *INFOSEC* ieteikumus par *SAA* akreditāciju,

— atbalsta *INFOSEC* darbības apmācību un izglītošanas jomā,

— sniedz tehniska rakstura padomus tādu starpgadījumu izmeklēšanā, kas saistīti ar *INFOSEC*,

— izveido tehniskās politikas konsultācijas, lai nodrošinātu tikai atļautas programmatūras izmantošanu.

25.3.4. *Tehniskās sistēmas īpašnieks (TSO)*

Par sistēmas kontroles un īpašu drošības iezīmju īstenošanu un darbību atbild šādas sistēmas īpašnieks, tehniskās sistēmas īpašnieks (*TSO*). Galvenajām sistēmām norīko galveno IT drošības speciālistu (*CISO*). Attiecīgā gadījumā katra struktūrvienība norīko vietējo IT drošības speciālistu (*LISO*). Tehniskās sistēmas īpašnieka pienākums ir izstrādāt drošības ekspluatācijas procedūras (*SecOps*), kas iekļauj visu sistēmas darbības laiku no projekta uzsākšanas līdz galīgai iznīcināšanai.

*TSO* norāda drošības standartus un praksi, kas jāievēro sistēmas piegādātājam.

Attiecīgā gadījumā *TSO* var deleģēt daļu no saviem pienākumiem vietējam IT drošības speciālistam. Viena persona var veikt dažādas *INFOSEC* funkcijas.

25.3.5. *Informācijas īpašnieks (IO)*

Informācijas īpašnieks (*IO*) atbild par *EUCI* (un citu informāciju), ko ievieš, apstrādā un izstrādā tehniskajās sistēmās. Viņš nosaka informācijas piekļuves prasības šādās sistēmās. Savā jomā tas var deleģēt pienākumus informācijas pārvaldniekam vai datubāzu pārvaldniekam.

25.3.6. *Lietotāji*

Visi lietotāji nodrošina to, ka to darbības negatīvi neietekmē to izmantotās sistēmas drošību.

25.3.7. *Apmācība par INFOSEC*

Izglītošana un apmācība par *INFOSEC* ir pieejama tam personālam, kam tā ir nepieciešama.

25.4. **Drošības pasākumi, kas nav tehniski**

25.4.1. *Personāla drošība*

Sistēmas lietotājiem ir atļauja un nepieciešamība zināt, ko attiecīgā gadījumā pieļauj klasifikācija un tādas informācijas saturs, kuru apstrādā attiecīgajā sistēmā. Piekļuvei konkrētām iekārtām vai informācijai, kas ir

▼B

raksturīga drošības sistēmām, nepieciešama īpaša atļauja, kura ir izsniegta atbilstoši Komisijas noteiktai procedūrai.

*SAA* norāda visus jutīgos amatus un atļaujas pakāpi un pārraudzību, kas nepieciešama personām, kuras strādā šādos amatos.

Sistēmas izstrādā un nosaka tā, lai veicinātu personāla pienākumu un atbildības sadalījumu, lai novērstu situāciju, kad vienai personai ir pilnīgas zināšanas vai kontrole pār sistēmas drošības galvenajām iezīmēm.

IT un attālos terminālos/darbstacijās, kuros var izmainīt sistēmas drošību, nestrādā tikai viena atļauta persona vai cits darbinieks.

Sistēmas drošības iestatījumus maina vismaz divas atļautas personas, kas strādā kopā.

25.4.2. *Fiziskā drošība*

IT un attālos terminālus/darbstacijas (atbilstoši 25. iedaļas 2. punktam), kuros ►M1 CONFIDENTIEL UE ◄ un informāciju ar augstāku klasifikācijas līmeni apstrādā ar IT palīdzību, vai kuros ir iespējama piekļuve šādai informācijai, attiecīgā gadījumā izveido kā ES I līmeņa vai II līmeņa drošības zonas.

25.4.3. *Piekļuves sistēmai kontrole*

Visu informāciju un materiālu, kas sniedz kontroli pār piekļuves sistēmu, aizsargā atbilstoši noteikumiem, kuri atbilst augstākajai klasifikācijai un tās informācijas kategorijas apzīmējumam, kam tās var sniegt piekļuvi.

Ja to vairs neizmanto šādam mērķim, informāciju un materiālus par piekļuvi kontrolei iznīcina saskaņā ar 25. iedaļas 5.4. punkta noteikumiem.

25.5. **Tehniski drošības pasākumi**

25.5.1. *Informācijas drošība*

Informācijas autors atbild par visu informāciju saturošu dokumentu identificēšanu un klasificēšanu, neatkarīgi no tā, vai tie ir uz papīra vai datorizētos datu uzglabāšanas līdzekļos. Katras papīra lapas augšā un apakšā norāda klasifikāciju. Rezultātam, neskatoties uz to, vai tas ir uz papīra vai atrodas datorizētos datu uzglabāšanas līdzekļos, ir klasifikācija, kas atbilst augstākajai klasifikācijai, kura ir piešķirta informācijai, ko izmanto tā izstrādei. Sistēmas darbības veids var ietekmēt šādas sistēmas rezultātu klasifikāciju.

Komisijas struktūrvienības un to informācijas turētāji atbild par problēmām, kas rodas, uzkrājoties atsevišķiem informācijas elementiem, un par secinājumiem, kas izriet no saistītiem elementiem, kā arī nosaka, vai augstāka klasifikācija atbilst visai informācijai.

Tas, ka informācija var būt saīsinājuma kods, pārraides kods vai jebkāds binārs atveidojums, nesniedz drošības aizsardzību un tādēļ neietekmē informācijas klasifikāciju.

Ja informāciju pārraida no vienas sistēmas uz otru, pārraides laikā informāciju aizsargā. Un saņēmēja sistēma atbilst sākotnējai klasifikācijai un informācijas kategorijai.

Ar visiem datorizētiem datu uzglabāšanas līdzekļiem darbojas tā, lai šāda darbība atbilstu uzglabātās informācijas vai līdzekļa marķējuma augstākajai klasifikācijai, un visu laiku atbilstoši aizsargātu.

Datorizēti datu uzglabāšanas līdzekļi, ko var atkārtoti izmantot ES klasificētas informācijas ierakstīšanai, patur augstāko klasifikāciju, kas tiem bija piešķirta pirms šāda informācija tika deklasificēta vai tās slepenības pakāpe tika pazemināta kopā ar uzglabāšanas līdzekli; to slepenības pakāpi var pazemināt vai tos var deklasificēt atbilstoši procedūrai, ko apstiprina *SAA* (skatīt 25. iedaļas 5.4. punktu).

▼B

25.5.2. *Informācijas kontrole un uzskaitāmība*

Par piekļuvi informācijai ar klasifikācijas pakāpi ►M1 SECRET UE ◄ un augstāku uzglabā automātiskus (auditācijas pieraksti) ierakstus vai ierakstus, kas veikti ar roku. Šādus ierakstus uzglabā atbilstoši šiem drošības noteikumiem.

ES klasificētus rezultātus, kas atrodas IT zonā, var apstrādāt kā vienu klasificētu lietu un tos nav jāreģistrē, ja vien materiāls ir identificēts, uz tā ir norādīta klasifikācija un to atbilstoši kontrolē.

Ja rezultātu ir izstrādājusi sistēma, kas apstrādā ES klasificētu informāciju, un to no IT zonas pārsūta attālam terminālim/darbstacijai, rezultātu kontrolei un reģistrācijai nosaka procedūru, kuru ir apstiprinājusi *SAA*. ►M1 SECRET UE ◄ un augstākas klasifikācijas informācijai šādā procedūrā iekļauj īpašas norādes par informācijas uzskaitāmību.

25.5.3. *Maināmo datu nesēju apstrāde un kontrole*

Visus maināmos datu nesējus ar klasifikācijas pakāpi ►M1 CONFIDENTIEL UE ◄ un augstāku apstrādā kā materiālu un tiem piemēro vispārējus noteikumus. Atbilstošu identificējošu un klasifikācijas marķējumu pielāgo datu nesēju īpašajam ārējam izskatam, lai tos varētu skaidri atpazīt.

Lietotāji nodrošina ES klasificētas informācijas uzglabāšanu datu nesējos ar atbilstošu klasifikācijas marķējumu un aizsardzību. Izveido procedūru, lai nodrošinātu visiem ES klasificētas informācijas līmeņiem informācijas tādu uzglabāšanu datu nesējos, kas atbilst šiem drošības noteikumiem.

25.5.4. *Datu nesēju deklasificēšana un iznīcināšana*

Datu nesēju, ko izmanto ES klasificētas informācijas ierakstīšanai, slepenības pakāpi var pazemināt vai tos var deklasificēt saskaņā ar procedūru, kuru apstiprina SAA.

Datu nesējus, kuros tika uzglabāta ►M1 TRES SECRET UE/EU TOP SECRET ◄ vai īpašas kategorijas informācija, nevar deklasificēt un izmantot atkārtoti.

Ja datu nesējus nevar deklasificēt vai tos nevar atkārtoti izmantot, tos iznīcina atbilstoši iepriekšnoteiktajai procedūrai.

25.5.5. *Komunikāciju drošība*

►M2 Komisijas Drošības direktorāta direktors ◄ ir Kripto iestāde.

Pārsūtot ES klasificētu informāciju elektromagnētiski, īsteno īpašus pasākumus, lai aizsargātu šādu pārsūtīšanu konfidencialitāti, integritāti un pieejamību. *SAA* nosaka prasības pārsūtījumu aizsardzībai pret atklāšanu un pārtveršanu. Informāciju, ko pārsūta komunikāciju sistēmā, aizsargā, pamatojoties uz prasībām par konfidencialitāti, integritāti un pieejamību.

Ja konfidencialitātes, integritātes un pieejamības nodrošināšanai nepieciešamas kriptogrāfijas metodes, šādas metodes un ar tām saistītos produktus īpaši apstiprina *SAA* kā Kripto iestāde.

Pārsūtīšanas laikā informācijas ar klasifikācijas pakāpi ►M1 SECRET UE ◄ un augstāku konfidencialitāti aizsargā ar kriptogrāfijas metodēm vai produktiem, kurus ir apstiprinājis Komisijas loceklis, kas atbild par drošības jautājumiem pēc konsultēšanās ar Komisijas drošības politikas konsultatīvo grupu. Pārsūtīšanas laikā informācijas ar klasifikācijas pakāpi ►M1 CONFIDENTIEL UE ◄ vai ►M1 RESTREINT UE ◄ aizsargā ar kriptogrāfijas metodēm vai produktiem, ko ir apstiprinājusi Komisijas Kripto iestāde pēc konsultēšanās ar Komisijas drošības politikas konsultatīvo grupu.

Sīki izstrādātus noteikumus, ko piemēro ES klasificētas informācijas pārsūtīšanai, iekļauj īpašos drošības norādījumos, kurus apstiprina

▼B

►M2 Komisijas Drošības direktorāts ◄ pēc konsultēšanās ar Komisijas drošības politikas konsultatīvo grupu.

Ārkārtas apstākļos informāciju ar klasifikācijas pakāpi ►M1 RESTREINT UE ◄, ►M1 CONFIDENTIEL UE ◄ un ►M1 SECRET UE ◄ var pārsūtīt skaidra teksta veidā, ja katru šādu gadījumu ir nepārprotami atļāvis un atbilstoši reģistrējis informācijas īpašnieks. Īpaši apstākļi ir šādi:

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

b) kad piegādes ātrums ir ārkārtīgi svarīgs un šifrēšana nav pieejama, un ir izvērtēts, ka pārsūtīto informāciju nevar izmantot tik ātri, lai tā negatīvi ietekmētu darbības.

Sistēma spēj liegt piekļuvi ES klasificētai informācijai jebkurā vai visās tās attālās darbstacijās vai terminālos, kad tas ir nepieciešams, vai nu ar fiziskas atslēgšanas palīdzību vai ar īpašām programmatūras iezīmēm, ko ir apstiprinājusi SAA.

25.5.6. *Instalāciju un radiācijas drošība*

Sākotnējo sistēmu instalāciju un jebkuras tās nozīmīgas izmaiņas organizē tā, lai instalāciju veiktu instalētāji, kuriem ir drošības pielaide, un kurus nepārtraukti pārrauga tehniski kvalificēts personāls, kam ir piekļuve tāda līmeņa ES klasificētai informācijai, kura atbilst augstākajai klasifikācijai, ko sistēma uzglabās un apstrādās.

Sistēmas, kas apstrādā informāciju ar klasifikācijas pakāpi ►M1 CONFIDENTIEL UE ◄ un augstāku, aizsargā tā, lai drošību nevarētu apdraudēt kompromitējošas noplūdes un/vai vadītspēja, kuru izpēti un kontroli sauc par "Tempest".

Tempest pretpasākumus pārskata un apstiprina Tempest iestāde (skatīt 25. iedaļas 3.2. punktu).

25.6. **Drošība apstrādes laikā**

25.6.1. *Drošības ekspluatācijas procedūras (SecOps)*

Drošības ekspluatācijas procedūras *(SecOPs)* nosaka principus, ko piemēro drošības jautājumos, darbības procedūru un personāla atbildību. Par *SecOPs* sagatavošanu atbild tehniskās sistēmas īpašnieks (*TSO*).

25.6.2. *Programmatūras aizsardzība/konfigurāciju pārvaldība*

Lietojumprogrammu drošības aizsardzību nosaka, pamatojoties uz programmas drošības klasifikācijas izvērtējumu, nevis uz to, kādas klasifikācijas pakāpes informāciju tā apstrādās. Izmantotās programmatūras versijas regulāri pārbauda, lai nodrošinātu to integritāti un uzlabotu to darbību.

Jaunas vai uzlabotas programmatūras versijas neizmanto ES klasificētas informācijas apstrādei, kamēr tās nav apstiprinājis *TSO*.

25.6.3. *Ļaunprātīgas programmatūras/datorvīrusu esamības pārbaude*

Ļaunprātīgas programmatūras/datorvīrusu esamības pārbaudi regulāri veic atbilstoši SAA prasībām.

Ļaunprātīgas programmatūras/datorvīrusu esamību pārbauda visos datu nesējus, kas nonāk Komisijas rīcībā pirms to ieviešanas jebkurā sistēmā.

25.6.4. *Uzturēšana*

Līgumos un procedūrās par regulāru sistēmu uzturēšanu un sistēmu uzturēšanu pēc pieprasījuma, kam ir izstrādāti *SSRS*, nosaka prasības un nosacījumus uzturēšanas personālam un ar to saistītam aprīkojumam, kuru ienes IT zonā.

Prasības ir skaidri izklāstītas *SSRS* un procedūras skaidri izklāsta *SecOPs*. Līgumuzturēšanu, kurai ir nepieciešamas attālas piekļuves diagnostikas procedūras, atļauj tikai ārkārtas gadījumos stingrā drošības kontrolē, un to atļauj tikai ar *SAA* apstiprinājumu.

▼B

25.7. **Datu iegūšana**

25.7.1. *Vispārīgi*

Jebkurš drošības produkts, ko izmantos sistēmā pēc tā iegūšanas, ir vai nu izvērtēts un sertificēts, vai pašlaik tiek izvērtēts un sertificēts; izvērtēšanu un sertificēšanu veic kādas no ES dalībvalstīm atbilstoša Izvērtēšanas vai Sertifikācijas struktūra, pamatojoties uz starptautiski atzītiem kritērijiem (piemēram, Vienoti informācijas tehnoloģiju drošības novērtējuma kritēriji, *re ISO 15408*). Lai saņemtu *ACPC* apstiprinājumu, nepieciešamas īpašas procedūras.

Lemjot, vai aprīkojumu, jo īpaši datu nesējus, jāiegādājas līzingā, nevis jāpērk, patur prātā to, ka šādu aprīkojumu, ja tas ir izmantots ES klasificētas informācijas apstrādei, nevar iznest ārpus atbilstoši drošas vides, kamēr tas ar SAA atļauju nav deklasificēts; šāda atļauja ne vienmēr ir iespējama.

25.7.2. *Akreditācija*

Visas sistēmas, kurām ir izstrādāti *SSRS*, pirms ES klasificētas informācijas apstrādes akreditē *SAA*, pamatojoties uz informāciju, kas ir sniegta *SSRS*, *SecOPs* vai citos atbilstošos dokumentos. Apakšsistēmas un attālus terminālus/darbstacijas akreditē kā daļu no visas sistēmas, ar ko tās ir savienotas. Ja sistēma darbojas gan Komisijā, gan citās organizācijās, Komisija un attiecīgās drošības iestādes savstarpēji vienojas par akreditāciju.

Akreditāciju var veikt atbilstoši akreditācijas stratēģijai, kas atbilst attiecīgajai sistēmai un ko ir noteikusi *SAA*.

25.7.3. *Izvērtēšana un sertifikācija*

Dažos gadījumos pirms akreditācijas sistēmas datortehnikas, programmaparatūras un programmatūras drošības iezīmes izvērtē un sertificē, apliecinot to spēju aizsargāt nodomātā klasifikācijas līmeņa informāciju.

Prasības izvērtēšanai un sertifikācijai iekļauj sistēmas plānošanā un skaidri norāda *SSRS*.

Izvērtēšanu un sertifikāciju veic atbilstoši apstiprinātām pamatnostādnēm; to veic tehniski kvalificēts personāls ar atbilstošām drošības atļaujām, kas darbojas *TSO* vārdā.

Ieteiktās dalībvalsts izvērtēšanas vai sertifikācijas iestāde var norīkot vienības vai tās pārstāvjus, piemēram, kompetentu līgumdarbinieku, kam ir drošības atļauja.

Iekļautās izvērtēšanas un sertifikācijas pakāpi var pazemināt (piemēram, tā var iekļaut tikai integrācijas aspektus), ja sistēma pamatojas uz esošiem datoru drošības produktiem, kas ir izvērtēti un sertificēti attiecīgajā valstī.

25.7.4. *Drošības iezīmju parastās pārbaudes akreditācijas pagarināšanas nolūkos*

*TSO* izveido parastu kontroles procedūru, kas pārliecinās par to, vai visas drošības iezīmes joprojām ir spēkā.

*SSRS* skaidri norāda izmaiņu veidus, kuru rezultātā veic atkārtotu akreditāciju vai kuru dēļ ir nepieciešams iepriekšējs *SAA* apstiprinājums. Pēc jebkuru izmaiņu veikšanas, labošanas vai defekta, kas var ietekmēt sistēmas drošības iezīmes, *TSO* nodrošina pārbaudes veikšanu, lai pārbaudītu drošības iezīmju pareizu darbību. Parasti sistēmas akreditācijas pagarināšana ir atkarīga no sekmīgiem pārbaužu rezultātiem.

Visas sistēmas, kurās ir iekļautas drošības iezīmes, regulāri pārbauda vai pārskata *SAA*. Attiecībā uz sistēmām, kurās apstrādā ►**M1** TRES SECRET UE/EU TOP SECRET ◄ informāciju, pārbaudes veic ne retāk kā reizi gadā.

▼B

25.8. **Pagaidu vai neregulāra lietošana**

25.8.1. *Mikrodatoru/personālo datoru drošība*

Mikrodatorus/personālos datorus ar fiksētiem diskiem (vai citu energoneatkarīgu atmiņu), kas darbojas vai nu autonomā režīmā, vai kā tīklā sasaistītas konfigurācijas, un pārnēsājamas datorierīces (piemēram, pārnēsājamus personālos datorus un elektroniskās piezīmju grāmatiņas) ar fiksētiem cietajiem diskiem, uzskata par informācijas nesējiem tāpat kā disketes vai citus maināmus datu nesējus.

Šādu aprīkojumu piekļuves, apstrādes, uzglabāšanas un pārvadāšanas ziņā aizsargā tādā līmenī, kas atbilst augstākajam klasifikācijas līmenim, kurš ir piešķirts informācijai, ko uzglabā vai apstrādā (līdz tās slepenības pakāpe ir pazemināta vai tā ir deklasificēta atbilstoši apstiprinātām procedūrām).

25.8.2. *Personiskā īpašumā esoša IT aprīkojuma izmantošana oficiālā Komisijas darbā*

Personiskā īpašumā esošu maināmu datu nesēju, programmatūras un IT datortehnikas (piemēram, personālo datoru un pārnēsājamu datorierīču), kuros var uzglabāt datus, izmantošana ES klasificētas informācijas apstrādei ir aizliegta.

Personiskā īpašumā esošu datortehniku, programmatūru un datu nesējus nedrīkst ienest I un II līmeņa zonās, kurās apstrādā ES klasificētu informāciju, bez iepriekšējas atļaujas no ►M2 Komisijas Drošības direktorāta direktora ◄. Šādu atļauju sniedz tehnisku iemeslu dēļ ārkārtas gadījumos.

25.8.3. *Līgumdarbinieku īpašumā esoša vai valsts piegādāta IT aprīkojuma izmantošana oficiālā Komisijas darbā*

►M2 Komisijas Drošības direktorāta direktors ◄ var atļaut līgumdarbinieku īpašumā esoša IT aprīkojuma vai programmatūras lietošanu organizācijās, kas palīdz Komisijai tās oficiālajā darbā. Arī valsts piegādāta IT aprīkojuma un programmatūras lietošanu var atļaut; šajā gadījumā IT aprīkojumu ienes attiecīga Komisijas reģistra kontrolē. Jebkurā gadījumā, ja IT aprīkojums tiks izmantots ES klasificētas informācijas apstrādei, konsultējas ar SAA, lai *INFOSEC* elementi, ko piemēro šāda aprīkojuma lietošanā, tiktu atbilstoši ņemti vērā un īstenoti.

26. ES KLASIFICĒTAS INFORMĀCIJAS NODOŠANA TREŠĀM VALSTĪM VAI STARPTAUTISKĀM ORGANIZĀCIJĀM

26.1.1. *ES klasificētas informācijas nodošanas regulējoši principi*

Komisija koleģiāli lemj par ES klasificētas informācijas nodošanu trešām valstīm vai starptautiskām organizācijām, pamatojoties uz:

— šādas informācijas veidu un saturu,

— saņēmēja ne pieciešamību zināt,

— šāda pasāk uma izdevību ES.

Tiek lūgta tādas ES klasificētas informācijas autora atļauja, kas tiks nodota.

Šādus lēmumus pieņem, katru gadījumu izvērtējot atsevišķi, atkarībā no:

— vēlamās sadarbības pakāpes ar attiecīgo trešo valsti vai starptautisko organizāciju;

— tiem parādītās uzticības, kas izriet no drošības līmeņa, kuru piemēros šīm valstīm vai organizācijām nodotajai ES klasificētai informācijai, un no šādās valstīs vai organizācijās piemēroto drošības noteikumu atbilstības drošības noteikumiem, ko piemēro ES. Šajā jautājumā Komisijas drošības politikas konsultatīvā grupa sniedz Komisijai savu tehnisko atzinumu.

Tas, ka trešās valstis vai starptautiskās organizācijas pieņem ES klasificētu informāciju, nozīmē to, ka informāciju neizmantos citiem

▼B

mērķiem kā tiem, kuri sekmē informācijas nodošanu vai apmaiņu ar informāciju, un ka tās sniegs aizsardzību, kuru pieprasa Komisija.

26.1.2. *Līmeņi*

Ja Komisija ir nolēmusi atklāt klasificētu informāciju vai apmainīties ar šādu informāciju ar attiecīgo valsti vai starptautisko organizāciju, tā lemj par iespējamo sadarbības līmeni. Līmenis jo īpaši ir atkarīgs no drošības politikas un noteikumiem, ko piemēro attiecīgā valsts vai organizācija.

Ir trīs sadarbības līmeņi:

1. līmenis

Sadarbība ar trešām valstīm vai starptautiskām organizācijām, kuru drošības politika un noteikumi saskan ar ES drošības politiku un noteikumiem.

2. līmenis

Sadarbība ar trešām valstīm vai starptautiskām organizācijām, kuru drošības politika un noteikumi izteikti atšķiras no ES drošības politikas un noteikumiem.

3. līmenis

Neregulāra sadarbība ar trešām valstīm vai starptautiskām organizācijām, kuru politiku un drošības noteikumus nevar izvērtēt.

Katrs sadarbības līmenis nosaka procedūru un drošības noteikumus, kas ir sīkāk izklāstīti 3., 4. un 5. papildinājumā.

26.1.3. *Drošības līgumi*

Kad Komisija ir nolēmusi, ka ir pastāvīga vai ilglaicīga nepieciešamība apmainīties ar klasificētu informāciju starp Komisiju un trešo valsti vai citu starptautisku organizāciju, tā sagatavo "vienošanos par drošības procedūrām klasificētas informācijas apmaiņām", nosakot sadarbības mērķi un savstarpējus noteikumus par apmainītās informācijas aizsardzību.

Attiecībā uz 3. līmeņa neregulāro sadarbību, kuras laiks un mērķis ir ierobežoti saskaņā ar definīciju, "vienošanās par drošības procedūrām klasificētas informācijai apmaiņai" vietu var ieņemt vienkāršs saprašanās memorands, kas nosaka apmaināmās klasificētās informācijas veidu un savstarpējās saistības attiecībā uz informāciju, ja šādas informācijas klasifikācijas līmenis nav augstāks par ►M1 RESTREINT UE ◄.

Vienošanās par drošības procedūrām klasificētas informācijas apmaiņai projektu pārrunā Komisijas drošības politikas konsultatīvajā grupā, pirms to iesniedz Komisijai lēmuma pieņemšanai.

Komisijas loceklis, kas atbild par drošības jautājumiem, pieprasa visu nepieciešamo palīdzību no dalībvalsts nacionālām drošības iestādēm, lai nodrošinātu to, ka nodoto informāciju izmantos un aizsargās atbilstoši noteikumiem, kuri ir izklāstīti vienošanās par drošības procedūrām vai saprašanās memorandos.

▼M3

27. KOPĒJIE MINIMĀLIE STANDARTI RŪPNIECISKAJAI DROŠĪBAI

27.1. **Ievads**

Šajā iedaļā iztirzāti rūpniecisko darbību drošības aspekti, kas ir būtiski, apspriežot un piešķirot līgumus vai subsīdiju līgumus, ar kuriem tiek uzticēti uzdevumi, kas ietver, ietekmē un/vai satur ES klasificēto informāciju, kā arī rūpniecības vai cita veida uzņēmumiem šos uzdevumus īstenojot, tostarp ES klasificētās informācijas paziņošana vai pieeja tai valsts iepirkuma un uzaicinājuma iesniegt priekšlikumus procedūras laikā (piedāvājuma izteikšanas periods un posms pirms līguma slēgšanas).

▼M3

27.2. **Definīcijas**

Minētajos kopējos minimālajos standartos piemēro šādas definīcijas:

a) "klasificēts līgums" – jebkurš līgums vai subsīdiju līgums par preču piegādi, darbu veikšanu, gatavu ēku nodošanu vai pakalpojumu sniegšanu, kura izpildei ir vajadzīga pieeja ES klasificētajai informācijai vai tās izveide vai kurā ir paredzēta šāda pieeja ES klasificētajai informācijai vai tās izveide;

b) "klasificēts apakšlīgums" – līgums, ko noslēdzis līgumdarbinieks vai subsīdijas saņēmējs ar citu līgumdarbinieku (proti, apakšuzņēmēju) par preču piegādi, darbu veikšanu, gatavu ēku nodošanu vai pakalpojumu sniegšanu, kura izpildei ir vajadzīga pieeja ES klasificētajai informācijai vai tās izveide vai kurā ir paredzēta šāda pieeja ES klasificētajai informācijai vai tās izveide;

c) "līgumdarbinieks" – uzņēmējs vai juridiska persona, kurai ir tiesībspēja slēgt līgumus vai saņemt subsīdiju;

d) "atbildīgā drošības iestāde (*DSA*)" – valsts drošības iestādei (*NSA*) attiecīgā dalībvalstī atbildīga iestāde, kas atbild par to, lai rūpniecības vai cita veida uzņēmumus informētu par valsts politiku visos jautājumos, kas attiecas uz rūpniecisko drošību, un sniegtu norādes un palīdzību tās īstenošanā. *NSA* var īstenot *DSA* funkcijas;

e) "objekta drošības pielaide (*FSC*)" – *NSA/DSA* administratīvs lēmums par to, ka drošības ziņā objektā var nodrošināt atbilstošu drošības aizsardzību īpaša drošības klasifikācijas līmeņa ES klasificētajai informācijai un ka tajā strādājošajam personālam, kuram nepieciešama pieeja ES klasificētajai informācijai, ir pienācīga drošības pielaide, un tas ir informēts par nepieciešamajām drošības prasībām attiecībā uz pieeju ES klasificētajai informācijai un tās aizsardzību;

f) "rūpniecības vai cita veida uzņēmums" – līgumdarbinieks vai apakšuzņēmējs, kas veic preču piegādi, darbu izpildi vai pakalpojumu sniegšanu; tie var būt uzņēmumi, kuru darbība saistīta ar rūpniecību, tirdzniecību, pakalpojumu sniegšanu, zinātni, izpēti, izglītību vai attīstību;

g) "rūpnieciskā drošība" – aizsardzības pasākumu un procedūru piemērošana, lai novērstu un konstatētu tādas ES klasificētās informācijas zudumu vai kompromitēšanu, ko apstrādā līgumdarbinieks vai apakšuzņēmējs sarunās pirms līguma slēgšanas, līguma apspriešanā un klasificētos līgumos, un pārvarētu šādas informācijas zaudēšanas vai kompromitēšanas sekas;

h) "valsts drošības iestāde (*NSA*)" – tāda valsts iestāde ES dalībvalstī, kuras galvenā atbildība ir aizsargāt ES klasificēto informāciju attiecīgajā dalībvalstī;

i) "līguma drošības klasifikācijas vispārējais līmenis" – drošības klasifikācijas noteikšana visam līgumam vai subsīdiju līgumam kopumā, pamatojoties uz tādas informācijas un/vai materiālu klasifikāciju, kas saistībā ar jebkuru punktu attiecīgajā līgumā vai subsīdiju līgumā kopumā jāsagatavo, jāizplata vai kurai jāpiekļūst, vai attiecībā uz kuru pastāv iespēja, ka to sagatavos, izplatīs vai piekļūs tai. Vispārējais līguma drošības klasifikācijas līmenis nedrīkst būt zemāks par jebkuras tā sastāvdaļas augstāko klasifikāciju, bet summēšanas rezultātā tas var būt augstāks;

j) "dokuments, kurā izklāstīti drošības aspekti (*SAL*)" – īpašu līgumslēdzējas iestādes noteiktu līguma nosacījumu kopums, kurš ir tāda klasificēta līguma sastāvdaļa, kas saistīts ar piekļuvi ES klasificētajai informācijai vai tās sagatavošanu, un kurā identificētas drošības prasības vai tās klasificēta līguma daļas, kurām vajadzīga drošības aizsardzība;

k) "drošības klasifikācijas rokasgrāmata (*SCG*)" – dokuments, kurā raksturotas programmas, līguma vai subsīdijas līguma klasificētās sastāvdaļas, norādot piemērojamos drošības klasifikācijas līmeņus.

▼M3

*SCG* var papildināt visā programmas, līguma vai subsīdiju līguma darbības laikā, turklāt iespējams informācijas sastāvdaļas pārklasificēt vai pazemināt to slepenības pakāpi. *SAL* ir jāietver *SCG*.

27.3. **Organizācija**

a) Komisija ar klasificētu līgumu var uzticēt dalībvalstī reģistrētiem rūpniecības vai cita veida uzņēmumiem veikt uzdevumus, kas ietver, ietekmē un/vai satur ES klasificēto informāciju.

b) Klasificētu līgumu piešķiršanā Komisijai ir jānodrošina visu to prasību ievērošana, kas izriet no minētajiem minimālajiem standartiem.

c) Komisija iesaista attiecīgo valsts drošības iestādi vai valsts drošības iestādes, lai rūpnieciskajai drošībai piemērotu minētos minimālos standartus. *NSA* var deleģēt minētos uzdevumus vienai vai vairākām *DSA*.

d) Par ES klasificēto informāciju rūpniecības vai cita veida uzņēmumos galvenokārt atbildīga ir šo uzņēmumu vadība.

e) Vienmēr, kad tiek piešķirts klasificēts līgums vai apakšlīgums, uz kuru attiecas minētie minimālie standarti, Komisija un/vai *NSA/DSA* attiecīgā gadījumā savlaicīgi informē tās dalībvalsts *NSA/DSA*, kurā līgumdarbinieks vai apakšuzņēmējs reģistrēts.

27.4. **Klasificēti līgumi un lēmumi par subsīdijām**

a) Klasificējot līgumu vai subsīdiju līgumu drošību, jāņem vērā šādi principi:

— Komisija attiecīgā gadījumā nosaka tos klasificēta līguma aspektus, kuriem nepieciešama aizsardzība un attiecīga drošības klasifikācija; veicot šādu klasifikāciju, tai ir jāņem vērā sākotnējā drošības klasifikācija, ko autors ir norādījis informācijai, kas sagatavota pirms klasificēta līguma piešķiršanas,

— līguma klasifikācijas kopējais līmenis nedrīkst būt zemāks par jebkuras tā sastāvdaļas augstāko klasifikāciju,

— ES klasificēto informāciju, kas sagatavota, īstenojot līguma darbības, klasificē atbilstoši Drošības klasifikācijas rokasgrāmatai,

— attiecīgā gadījumā Komisija ir atbildīga par līguma vispārējā klasifikācijas līmeņa maiņu vai visu tā sastāvdaļu drošības klasifikāciju, apspriežoties ar līguma autoru, un par visu ieinteresēto personu informēšanu,

— klasificēto informāciju, ko nodod līgumdarbiniekam vai apakšuzņēmējam vai kuru sagatavo saistībā ar līguma darbību, drīkst izmantot tikai tiem mērķiem, kas norādīti klasificētā līgumā, un to nedrīkst atklāt trešām personām bez autora iepriekš sniegtas rakstveida piekrišanas.

b) Komisija un attiecīgās dalībvalsts *NSA/DSA* atbild par to, lai nodrošinātu, ka līgumdarbinieki un apakšuzņēmēji, kam piešķir klasificētus līgumus, kuros ietverta informācija, kas klasificēta kā *CONFIDENTIEL UE* un augstāk, veic visus vajadzīgos pasākumus, lai nodrošinātu, ka atbilstoši valsts normatīvajiem aktiem tiek aizsargāta šāda ES klasificētā informācija, ko viņiem nodod vai ko viņi sagatavo, īstenojot klasificētu līgumu. Ja nav atbilstības drošības prasībām, klasificētu līgumu var izbeigt.

c) Visiem rūpnieciskajiem vai cita veida uzņēmumiem, kas piedalās tādu klasificētu līgumu izpildē, kuri ir saistīti ar pieeju informācijai, kas klasificēta kā *CONFIDENTIEL UE* vai augstāk, ir jābūt valsts *FSC*. Attiecīgās dalībvalsts *NSA/DSA* piešķir *FSC*, lai apstiprinātu, ka uzņēmums var nodrošināt un garantēt pienācīgu ES klasificētās informācijas drošības aizsardzību atbilstoši attiecīgam klasifikācijas līmenim.

▼M3

d) Piešķirot klasificētu līgumu, objekta drošības speciālists (*FSO*), ko šajā amatā iecēlusi līgumdarbinieka vai apakšuzņēmēja uzņēmuma vadība, ir atbildīgs par to, lai pieprasītu personāla drošības pielaidi (*PSC*) visām personām, kas nodarbinātas rūpnieciskos vai cita veida uzņēmumos ES dalībvalstī, kuru pienākumu veikšanai nepieciešama piekļuve informācijai, kas klasificēta kā *CONFIDENTIEL UE* vai augstāk, ievērojot klasificētu līgumu, ko piešķir attiecīgās dalībvalsts *NSA/DSA* saskaņā ar attiecīgās valsts noteikumiem.

e) Klasificētos līgumos ir jāiekļauj *SAL*, kā norādīts 27. panta b punkta j) apakšpunktā. *SCG* ir jābūt *SAL*.

f) Pirms sarunu procedūras uzsākšanas attiecībā uz klasificētu līgumu Komisija sazinās ar tās dalībvalsts *NSA/DSA*, kurā attiecīgais rūpnieciskais vai cita veida uzņēmums ir reģistrēts, lai pārliecinātos, ka tam ir derīgs *FSC*, kas atbilst līguma drošības klasifikācijas līmenim.

g) Līgumslēdzēja iestāde nedrīkst ierosināt klasificēta līguma slēgšanu ar izvēlēto uzņēmēju, pirms nav saņemts derīgs *FSC* sertifikāts.

h) Līgumiem, kas ietver informāciju, kura klasificēta kā *RESTRAINT UE*, *FSC* nav nepieciešama, ja vien nav pieprasīts dalībvalsts normatīvajos aktos.

i) Uzaicinājumos uz konkursu attiecībā uz klasificētiem līgumiem ir jāietver noteikums, saskaņā ar ko uzņēmējam, kas neiesniedz piedāvājumu vai kuru neizvēlas, noteiktā laikposmā ir jāatdod visi dokumenti.

j) Līgumdarbiniekiem var būt nepieciešams dažādos līmeņos apspriest klasificētus apakšlīgumus ar apakšuzņēmējiem. Līgumdarbinieks ir atbildīgs par to, lai nodrošinātu, ka visas apakšlīgumiskās darbības tiek veiktas saskaņā ar kopējiem minimālajiem standartiem, kas ietverti šajā iedaļā. Tomēr līgumdarbinieks nedrīkst nodot ES klasificēto informāciju vai materiālu apakšuzņēmējam bez autora iepriekš sniegtas rakstveida piekrišanas.

k) Konkursā vai uzaicinājumā iesniegt priekšlikumus un klasificētā līgumā ir jānosaka nosacījumi, saskaņā ar kuriem līgumdarbinieks var slēgt apakšlīgumu. Uzņēmumiem, kas reģistrēti valstī, kura nav ES dalībvalsts, nedrīkst piešķirt apakšlīgumus bez Komisijas skaidri izteiktas rakstveida atļaujas.

l) Visā klasificēta līguma darbības laikā Komisija saistībā ar attiecīgo *DSA/NSA* uzrauga atbilstību visiem tās drošības noteikumiem. Saskaņā ar noteikumiem, kas izklāstīti minēto drošības noteikumu II daļas 24. iedaļā, par visiem starpgadījumiem, kas skar drošību, tiek iesniegti ziņojumi. Par visām izmaiņām attiecībā uz *FSC* vai tās atsaukšanu tūlīt paziņo Komisijai un visām citām *NSA/DSA*, kuras ir informētas par attiecīgo *FSC*.

m) Beidzoties tāda klasificēta līguma vai klasificēta apakšlīguma darbības laikam, uz kuru attiecas minētie minimālie standarti, Komisija un/vai *NSA/DSA* attiecīgā gadījumā savlaicīgi informē tās dalībvalsts *NSA/DSA*, kurā līgumdarbinieks vai apakšuzņēmējs reģistrēts.

n) Līgumdarbinieki un apakšuzņēmēji pēc klasificēta līguma vai klasificēta apakšlīguma izbeigšanas vai noslēgšanas turpina ievērot šajā iedaļā ietvertos kopējos minimālos standartus, kā arī klasificētās informācijas konfidencialitāti.

o) Īpaši noteikumi par klasificētās informācijas izplatīšanu, beidzoties klasificēta līguma darbībai, būs izklāstīti *SAL* vai citos attiecīgos noteikumos, kuros nosaka drošības prasības.

p) Pienākumus un nosacījumus, kas minēti šajā iedaļā, ar attiecīgajām izmaiņām piemēro attiecībā uz procedūrām, ar kurām subsīdijas tiek piešķirtas, pamatojoties uz lēmumu un jo īpaši pamatojoties uz šādas subsīdijas saņēmējiem. Lēmumā par subsīdiju paredz saņēmēju nosacījumus.

▼M3

27.5. **Apmeklējumi**

Komisijas personāla apmeklējumi saistībā ar klasificētiem līgumiem tādos rūpnieciskos vai cita veida uzņēmumos dalībvalstīs, kuri pilda ES klasificētus līgumus, ir jāsaskaņo ar attiecīgo *NSA/DSA*. Attiecīgajām valsts drošības iestādēm/atbildīgajām drošības iestādēm ir jāsaskaņo rūpnieciska vai cita veida uzņēmuma darbinieku apmeklējumi saistībā ar ES klasificēto līgumu. Tomēr NSA/DSA, kas ir saistītas ar ES klasificētu līgumu var vienoties par kārtību, saskaņā ar kuru iespējams tieši organizēt rūpniecības vai cita veida uzņēmumu darbinieku apmeklējumus.

27.6. **ES klasificētās informācijas pārsūtīšana un transportēšana**

a) Attiecībā uz ES klasificētās informācijas pārsūtīšanu piemēro šo drošības noteikumu II daļas 21. iedaļu. Lai papildinātu šos nosacījumus, piemēro jebkuru procedūru, kas ir spēkā dalībvalstīs.

b) Tāda ES klasificētā materiāla starptautisku transportēšanu, kas saistīts ar klasificētiem līgumiem, veiks saskaņā ar valsts kārtību attiecīgajā dalībvalstī. Pārbaudot starptautiskas transportēšanas drošības pasākumus, piemēro šādus principus:

— drošību no sākumpunkta līdz galamērķim nodrošina visos transportēšanas posmos un jebkuros apstākļos,

— sūtījumam noteikto aizsardzības pakāpi nosaka, vadoties pēc tajā ietvertā materiāla visaugstākās klasifikācijas,

— attiecīgā gadījumā uzņēmumiem, kas sniedz transportēšanas pakalpojumus, ir jāsaņem *FSC*. Šādos gadījumos personālam, kas apstrādā sūtījumu, ir jābūt drošības pielaidei atbilstoši šajā iedaļā ietvertajiem kopējiem minimālajiem standartiem,

— pārvadājumi, cik iespējams, jāveic no viena punkta uz otru un pēc iespējas ātrāk,

— ja iespējams, maršrutiem jābūt tikai ES dalībvalstu robežās. Maršruti caur valstīm, kas nav ES dalībvalstis, ir jāveic tikai tad, ja to atļauj gan nosūtītājas valsts, gan saņēmējas valsts *NSA/DSA*,

— pirms jebkādas ES klasificētā materiāla pārvietošanas nosūtītājs izstrādā transportēšanas plānu, kuru attiecīgās *NSA/DSA* apstiprina.

▼M1

*1. papildinājums*

**VALSTU DROŠĪBAS KLASIFIKĀCIJAS SALĪDZINĀJUMS**

| ES klasifikācija | TRES SECRET UE/EU TOP SECRET | SECRET UE | CONFIDENTIEL UE | RESTREINT UE |
|---|---|---|---|---|
| RES klasifikācija | FOCAL TOP SECRET | WEU SECRET | WEU CONFIDENTIAL | WEU RESTRICTED |
| Euratom klasifikācija | EURA TOP SECRET | EURA SECRET | EURA CONFIDENTIAL | EURA RESTRICTED |
| NATO klasifikācija | COSMIC TOP SECRET | NATO SECRET | NATO CONFIDENTIAL | NATO RESTRICTED |
| Beļģija | Très Secret | Secret | Confidentiel | Diffusion restreinte |
| | Zeer Geheim | Geheim | Vertrouwelijk | Beperkte Verspreiding |
| Čehija | Přísně tajné | Tajné | Důvěrné | Vyhrazené |
| Dānija | Yderst hemmeligt | Hemmeligt | Fortroligt | Til tjenestebrug |
| Vācija | Streng geheim | Geheim | VS ([1]) — Vertraulich | VS — Nur für den Dienstgebrauch |
| Igaunija | Täiesti salajane | Salajane | Konfidentsiaalne | Piiratud |
| Grieķija | Άκρως Απόρρητο | Απόρρητο | Εμπιστευτικό | Περιορισμένης Χρήσης |
| | Abr: ΑΑΠ | Abr: (ΑΠ) | Abr: (ΕΜ) | Abr: (ΠΧ) |
| Spānija | Secreto | Reservado | Confidencial | Difusión Limitada |
| Francija | Très Secret Défense ([2]) | Secret Défense | Confidentiel Défense | |
| 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 |
| Ungārija | Szigorúan titkos ! | Titkos ! | Bizalmas ! | Korlátozott terjesztésű ! |
| Malta | L-Ghola Segretezza | Sigriet | Kunfidenzjali | Ristrett |
| Nīderlande | Stg ([3]). Zeer Geheim | Stg. Geheim | Stg. Confidentieel | Departementaalvertrouwelijk |
| Austrija | Streng Geheim | Geheim | Vertraulich | Eingeschränkt |
| Polija | Ściśle Tajne | Tajne | Poufne | Zastrzeżone |
| Portugāle | Muito Secreto | Secreto | Confidencial | Reservado |
| Slovēnija | Strogo tajno | Tajno | Zaupno | SVN Interno |
| Slovākija | Prísne tajné | Tajné | Dôverné | Vyhradené |

▼**M1**

| Somija | Erittäin salainen | Erittäin salainen | Salainen | Luottamuksellinen |
|---|---|---|---|---|
| Zviedrija | Kvalificerat hemlig | Hemlig | Hemlig | Hemlig |
| Apvienotā Karaliste | Top Secret | Secret | Confidential | Restricted |

([7]) VS = Verschlusssache.
([8]) *Très Secret Défense*, kas attiecas uz valdības prioritārajiem jautājumiem, drīkst mainīt tikai ar premjerministra atļauju.
([9]) Stg = staatsgeheim.

*2. papildinājums*

## PRAKTISKS KLASIFIKĀCIJAS CEĻVEDIS

Šis ceļvedis ir norādošs un tas neizmaina būtiskos noteikumus, kas ir izklāstīti 16., 17., 20. un 21. iedaļā.

| Klasifikācija | Kad | Kas | Piešķir | Slepenības pakāpes pazemināšana/deklasifikācija/iznīcināšana | |
|---|---|---|---|---|---|
| | | | | Kas | Kad |
| ►**M1** TRES SECRET UE/EU TOP SECRET ◄:<br>Šo klasifikāciju piemēro tikai tai informācijai un materiāliem, kuru neatļauta atklāšana var izraisīt ārkārtīgi smagus Eiropas Savienības vai vienas vai vairāku tās dalībvalstu vai tai draudzīgu valstu iekšējo stabilitāti | ►**M1** TRES SECRET UE/EU TOP SECRET ◄ lietu kompromitēšana:<br>— tieši apdraud Eiropas Savienības vai vienas vai vairāku tās dalībvalstu vai tai draudzīgu valstu iekšējo stabilitāti<br>— izraisa ārkārtīgi smagas sekas attiecībās ar draudzīgām valdībām<br>— tieši izraisa daudzu cilvēku nāvi<br>— nodara ārkārtīgi smagus zaudējumus drošības efektivitātei dalībvalstīs vai citos ieguldītāju spēkos, vai ārkārtīgi vērtīgām drošības vai ziņu ievākšanas darbībām<br>— nodara ilglaicīgus zaudējumus ES vai dalībvalstu ekonomikai | Personas ar atbilstošām atļaujām (autori), ģenerāldirektori, dienestu vadītāji (17. iedaļas 1. punkts).<br>Autori norāda datumu, laika posmu vai gadījumu, kad satura slepenības pakāpi var pazemināt vai to var deklasificēt (16. iedaļas 2. punkts).<br>Citādi tie pārskata dokumentus vismaz ik pēc pieciem gadiem, lai nodrošinātu sākotnējās klasifikācijas nepieciešamību (17. iedaļas 3. punkts). | ►**M1** TRES SECRET UE/EU TOP SECRET ◄ klasifikāciju piešķir ►**M1** TRES SECRET UE/EU TOP SECRET ◄ dokumentiem, un, vajadzības gadījumā, drošības marķējumu un/vai aizsardzības marķējumu — EDAP, vai nu mehāniski vai ar roku (16. iedaļas 4., 5. un 3. punkts).<br>ES klasifikāciju un drošības apzīmējumus norāda katras lappuses augšā, lejā un centrā, un katru lappusi numurē. Uz katra dokumenta norāda reģistrācijas numuru un datumu; reģistrācijas numuru norāda uz katras lappuses.<br>Ja dokumentus izdalīs vairākās kopijās, katrai norāda kopijas numuru, kas atrodas pirmajā lappusē, kā arī kopējo lappušu skaitu. Visus papildinājumus un pielikumus uzskaita pirmajā lapā (21. iedaļas 1. punkts). | Par deklasifikāciju vai slepenības pakāpes pazemināšanu atbild autors, kas informē par izmaiņām jebkuru tālāku adresātu, kuram tas ir nosūtījis vai kopējis dokumentu (17. iedaļas 3. punkts).<br>►**M1** TRES SECRET UE/EU TOP SECRET ◄ dokumentus iznīcina centrālais reģistrs vai tā pārraudzībā esoši apakšreģistri. Katru iznīcināto dokumentu uzskaita apliecībā par iznīcināšanu, ko paraksta ►**M1** TRES SECRET UE/EU TOP SECRET ◄ kontrolieris un ierēdnis, kas piedalās iznīcināšanā, kuram ir piekļuve ►**M1** TRES SECRET UE/EU TOP SECRET ◄ informācijai. Par to ieraksta piezīmi žurnālā. Reģistrs uzglabā apliecības par iznīcināšanu kopā ar nodošanas sarakstiem 10 gadus (22. iedaļas 5. punkts). | Iznīcina pāri palikušās kopijas un dokumentus, kas vairs nav vajadzīgi (22. iedaļas 5. punkts).<br>►**M1** TRES SECRET UE/EU TOP SECRET ◄ dokumentus, tostarp klasificētas informācijas atkritumus, kas rodas no ►**M1** TRES SECRET UE/EU TOP SECRET ◄ dokumentu sagatavošanas, piemēram, bojātām kopijām, darba melnrakstiem, drukātām piezīmēm un kopapīra, iznīcina ►**M1** TRES SECRET UE/EU TOP SECRET ◄ kontroliera pārraudzībā vai nu sadedzinot, saplēšot, sasmalcinot vai citā veidā samazinot līdz neatpazīstamai un neatjaunojamai formai (22. iedaļas 5. punkts). |

| Klasifikācija | Kad | Kas | Piešķir | Slepenības pakāpes pazemināšana/deklasifikācija/iznīcināšana | |
|---|---|---|---|---|---|
| | | | | Kas | Kad |
| ►M1 SECRET UE ◄:<br>Šo klasifikāciju piemēro tikai tai informācijai un materiāliem, kuru neatļauta atklāšana var nopietni kaitēt Eiropas Savienības vai vienas vai vairāku tās dalībvalstu interešu ierobežojumus (16. iedaļas 1. punkts). | ►M1 SECRET UE ◄ lietu kompromitēšana:<br>— izraisa starptautiskus saspīlējumus<br>— nopietni apdraud attiecības ar draudzīgām valdībām<br>— tieši apdraud cilvēku dzīvības vai nodara kaitējumu sabiedriskai kārtībai vai personiskai drošībai vai brīvībai<br>— nodara zaudējumus drošības efektivitātei dalībvalstīs vai citos ieguldītāju spēkos, vai ārkārtīgi vērtīgām drošības vai ziņu ievākšanas darbībām<br>— nodara nopietnus materiālos zaudējumus ES vai vienas no tās dalībvalstīm finanšu, monetārām, ekonomiskām un komerciālām interesēm. | Personas ar atbilstošām atļaujām (autori), ģenerāldirektori, dienestu vadītāji (17. iedaļas 1. punkts).<br>Autori norāda datumu, laika posmu, kad satura slepenības pakāpi var pazemināt vai to var deklasificēt (16. iedaļas 2. punkts).<br>Citādi tie pārskata dokumentus vismaz ik pēc pieciem gadiem, lai nodrošinātu sākotnējās klasifikācijas nepieciešamību (17. iedaļas 3. punkts). | ►M1 SECRET UE ◄ klasifikāciju piešķir ►M1 SECRET UE ◄ dokumentiem, un, vajadzības gadījumā, drošības marķējumu un/vai aizsardzības marķējumu — EDAP, vai nu mehāniski vai ar roku (16. iedaļas 4., 5. un 3. punkts).<br>ES klasifikāciju un drošības apzīmējumus norāda katras lappuses augšā, lejā un centrā, un katru lappusi numurē. Uz katra dokumenta norāda reģistrācijas numuru un datumu; reģistrācijas numuru norāda uz katras lappuses.<br>Ja dokumentus izdalīs vairākās kopijās, katrai norāda kopijas numuru, kas atrodas pirmajā lappusē, kā arī kopējo lappušu skaitu. Visus papildinājumus un pielikumus uzskaita pirmajā lapā (21. iedaļas 1. punkts). | Par deklasifikāciju vai slepenības pakāpes pazemināšanu atbild autors, kas informē par izmaiņām jebkuru tālāku adresātu, kuram tas ir nosūtījis vai kopējis dokumentu (17. iedaļas 3. punkts).<br>►M1 SECRET UE ◄ dokumentus iznīcina reģistrs, kas par tiem atbild, tādas personas klātbūtnē, kurai ir drošības pielaide. ►M1 SECRET UE ◄ dokumentus, kuri ir iznīcināti, uzskaita parakstītās apliecībās par iznīcināšanu, ko uzglabā reģistrs kopā ar iznīcināšanas veidlapām vismaz trīs gadus (22. iedaļas 5. punkts). | Iznīcina pāri palikušās kopijas un dokumentus, kas vairs nav vajadzīgi (22. iedaļas 5. punkts).<br>►M1 SECRET UE ◄ dokumentus, tostarp klasificētas informācijas atkritumus, kas rodas no ►M1 TRES SECRET UE/EU TOP SECRET ◄ dokumentu sagatavošanas, piemēram, bojātām kopijām, darba melnrakstiem, drukātām piezīmēm un kopapīra, iznīcina vai nu sadedzinot, saplēšot, sasmalcinot vai citā veidā samazinot līdz neatpazīstamai un neatjaunojamai formai (22. iedaļas 5. punkts). |
| ►M1 CONFIDENTIEL UE ◄:<br>Šo klasifikāciju piemēro tikai tai informācijai un materiāliem, kuru neatļauta atklāšana var apdraudēt Eiropas Savienības vai vienas vai vairāku tās dalībvalstu interešu ierobežojumus (16. iedaļas 1. punkts). | ►M1 CONFIDENTIEL UE ◄ lietu kompromitēšana:<br>— nodara materiālus zaudējumus diplomātiskām attiecībām, proti, izraisa oficiālus protestus vai citas sankcijas<br>— ierobežo personisko brīvību vai drošību<br>— nodara zaudējumus drošības efektivitātei | Personas ar atbilstošām atļaujām (autori), ģenerāldirektori, dienestu vadītāji (17. iedaļas 1. punkts).<br>Autori norāda datumu vai laika posmu, kad satura slepenības pakāpi var pazemināt vai to var deklasificēt. Citādi tie pārskata | ►M1 CONFIDENTIEL UE ◄ klasifikāciju piešķir ►M1 CONFIDENTIEL UE ◄ dokumentiem, un, vajadzības gadījumā, drošības marķējumu un/vai aizsardzības marķējumu — EDAP, vai nu mehāniski vai ar roku (16. iedaļas 4., 5. un 3. punkts). | Par deklasifikāciju vai slepenības pakāpes pazemināšanu atbild autors, kas informē par izmaiņām jebkuru tālāku adresātu, kuram tas ir nosūtījis vai kopējis dokumentu (17. iedaļas 3. punkts).<br>►M1 CONFIDENTIEL UE ◄ dokumentus iznīcina reģistrs, kas par tiem | Iznīcina pāri palikušās kopijas un dokumentus, kas vairs nav vajadzīgi (22. iedaļas 5. punkts).<br>►M1 CONFIDENTIEL UE ◄ dokumentus, tostarp klasificētas informācijas atkritumus, kas rodas no ►M1 CONFIDENTIEL UE ◄ dokumentu sagatavošanas, piemēram, bojātām |

| Klasifikācija | Kad | Kas | Piešķir | Slepenības pakāpes pazemināšana/deklasifikācija/iznīcināšana | |
|---|---|---|---|---|---|
| | | | | Kas | Kad |
| | dalībvalstīs vai citos ieguldītāju spēkos, vai vērtīgām drošības vai ziņu ievākšanas darbībām<br>— būtiski iedragā lielu organizāciju finansiālo dzīvotspēju<br>— kavē izmeklēšanu vai veicina nopietnu noziegumu izdarīšanu<br>— nopietni darbojas pretrunā ES vai dalībvalstu finanšu, monetārām, ekonomiskām un komerciālām interesēm<br>— nopietni kavē svarīgas ES politikas attīstību vai darbību<br>— izbeidz vai citādi būtiski kaitē nopietnām ES darbībām. | dokumentus vismaz ik pēc pieciem gadiem, lai nodrošinātu sākotnējās klasifikācijas nepieciešamību (17. iedaļas 3. punkts). | ES klasifikāciju un drošības apzīmējumus norāda katras lappuses augšā, lejā un centrā, un katru lappusi numurē. Uz katra dokumenta norāda reģistrācijas numuru un datumu.<br>Visus papildinājumus un pielikumus uzskaita pirmajā lapā (21. iedaļas 1. punkts). | atbild, tādas personas klātbūtnē, kurai ir drošības pielaide. To iznīcināšanu reģistrē atbilstoši valsts tiesību aktiem un attiecībā uz Komisijas vai ES decentralizētām aģentūrām atbilstoši ►M2 Komisijas loceklis, kas atbild par drošības jautājumiem ◄ norādījumiem (22. iedaļas 5. punkts). | kopijām, darba melnrakstiem, drukātām piezīmēm un koppapīra, iznīcina vai nu sadedzinot, saplēšot, sasmalcinot vai citā veidā samazinot līdz neatpazīstamai un neatjaunojamai formai (22. iedaļas 5. punkts). |
| ►M1 RESTREINT UE ◄: Šo klasifikāciju piemēro tikai tai informācijai un materiāliem, kuru neatļauta atklāšana var kaitēt Eiropas Savienības vai vienas vai vairāku tās dalībvalstu interesēm (16. iedaļas 1. punkts). | ►M1 RESTREINT UE ◄ lietu kompromitēšana:<br>— negatīvi ietekmē diplomātiskas attiecības<br>— sagādā nopietnas ciešanas cilvēkiem<br>— sarežģī darbības efektivitātes vai drošības uzturēšanu dalībvalstīs vai ieguldītāju spēkos<br>— izraisa finansiālus zaudējumus vai veicina netaisnu personu vai uzņēmumu iedzīvošanos<br>— neievēro pasākumus, kas ir vērsti uz tādas informācijas uzticamības uzturēšanu, ko sniegušas trešās valstis<br>— pārkāpj tiesību aktus par | Personas ar atbilstošām atļaujām (autori), ģenerāldirektori, dienestu vadītāji (17. iedaļas 1. punkts).<br>Autori norāda datumu, laika posmu vai gadījumu, kad satura slepenības pakāpi var pazemināt vai to var deklasificēt (16. iedaļas 2. punkts).<br>Citādi tie pārskata dokumentus vismaz ik pēc pieciem gadiem, lai nodrošinātu sākotnējās klasifikācijas nepieciešamību (17. iedaļas 3. punkts). | ►M1 RESTREINT UE ◄ klasifikāciju piešķir<br>►M1 RESTREINT UE ◄dokumentiem, un, vajadzības gadījumā, drošības marķējumu un/vai aizsardzības marķējumu — *EDAP*, vai nu mehāniski vai ar roku (16. iedaļas 4., 5. un 3. punkts).<br>ES klasifikāciju un drošības apzīmējumus norāda pirmās lappuses augšā un katru lappusi numurē. Uz katra dokumenta norāda reģistrācijas numuru un datumu (21. iedaļas 1. punkts). | Par deklasifikāciju vai slepenības pakāpes pazemināšanu atbild autors, kas informē par izmaiņām jebkuru tālāku adresātu, kuram tas ir nosūtījis vai kopējis dokumentu (17. iedaļas 3. punkts).<br>►M1 RESTREINT UE ◄ dokumentus iznīcina reģistrs, kas par tiem atbild, vai lietotājs atbilstoši ►M2 Komisijas loceklis, kas atbild par drošības jautājumiem ◄ norādījumiem (22. iedaļas 5. punkts). | Iznīcina pāri palikušās kopijas un dokumentus, kas vairs nav vajadzīgi (22. iedaļas 5. punkts). |

| Klasifikācija | Kad | Kas | Piešķir | Slepenības pakāpes pazemināšana/deklasifikācija/iznīcināšana | |
|---|---|---|---|---|---|
| | | | | Kas | Kad |
| | informācijas atklāšanu<br>— kavē izmeklēšanu vai veicina noziegumu izdarīšanu<br>— dara neizdevīgu ES vai dalībvalstu stāvokli komerciālās vai politiskās pārrunās<br>— kavē svarīgas ES politikas attīstību vai darbību<br>— iedragā pareizu ES un tās darbību pārvaldību. | | | | |

▼B

*3. papildinājums*

**Pamatnostādnes par ES klasificētas informācijas nodošanu trešām valstīm vai starptautiskām organizācijām: 1. līmeņa sadarbība**

PROCEDŪRAS

1. Komisija lemj koleģiāli par ES klasificētas informācijas nodošanu valstīm, kas nav Eiropas Savienības dalībvalstis vai citām starptautiskām organizācijām, kuru drošības politika un noteikumi ir līdzvērtīgi ES.

2. Kamēr drošības vienošanās nav noslēgta, Komisijas loceklis, kas atbild par drošības jautājumiem, izskata lūgumus nodot ES klasificētu informāciju.

3. To darot, viņš/viņa:

   — lūdz to autoru viedokli, kuru *EUCI* grasās nodot;

   — nodibina nepieciešamos sakarus ar saņēmēju valstu vai starptautisko organizāciju drošības dienestiem, lai pārliecinātos, vai drošības politika un noteikumi garantē nodotās klasificētās informācijas aizsardzību saskaņā ar šiem drošības noteikumiem;

   — lūdz Komisijas drošības politikas konsultatīvās grupas atzinumu par uzticību, ko var sniegt saņēmējām valstīm vai starptautiskām organizācijām.

4. Komisijas loceklis, kas atbild par drošības jautājumiem, nodod pieprasījumu un Komisijas drošības politikas konsultatīvās grupas atzinumu Komisijai lēmuma pieņemšanai.

DROŠĪBAS NOTEIKUMI, KO PIEMĒRO SAŅĒMĒJIEM

5. Komisijas loceklis, kas atbild par drošības jautājumiem, paziņo saņēmējām valstīm vai starptautiskām organizācijām Komisijas lēmumu par atļauju ES klasificētas informācijas nodošanai.

6. Lēmums par informācijas nodošanu stājas spēkā tikai pēc tam, kad saņēmēji ir rakstiski apliecinājuši:

   — izmantot informāciju tikai tiem mērķiem, par kuriem ir panākta vienošanās;

   — aizsargāt informāciju atbilstoši šiem drošības noteikumiem un jo īpaši turpmāk izklāstītiem īpašiem noteikumiem.

7. Personāls

   a) Ierēdņu skaits, kuriem ir piekļuve ES klasificētai informācijai, ir stingri ierobežots un pamatots ar nepieciešamību zināt principu; piekļuve ir tikai tām personām, kam pienākumu veikšanai tā ir nepieciešama.

   b) Visiem ierēdņiem vai pilsoņiem, kam ir atļauja piekļūt informācijai ar klasifikācijas pakāpi ►M1 CONFIDENTIEL UE ◄ vai augstāku, ir vai nu atbilstoša līmeņa drošības sertifikāts, vai līdzvērtīga drošības pielaide, katru no kurām ir izsniegusi to valsts valdība.

8. Dokumentu nosūtīšana

   a) Praktisku procedūru dokumentu pārsūtīšanai nosaka vienojoties. Kamēr šāda vienošanās nav noslēgta, piemēro 21. iedaļas noteikumus. Vienošanās jo īpaši norāda reģistrus, kuriem tiks pārsūtīta informācija.

   b) Ja klasificēta informācija, kuras nodošanu ir atļāvusi Komisija, iekļauj ►M1 TRES SECRET UE/EU TOP SECRET ◄ informāciju, saņēmēja valsts vai starptautiska organizācija izveido ES centrālo reģistru un, ja nepieciešams, ES apakšreģistrus. Šādi reģistri piemēro noteikumus, kas stingri atbilst šo drošības noteikumu 22. iedaļai.

▼B

9. Reģistrācija

Tiklīdz reģistrs saņem ES dokumentu ar klasifikācijas pakāpi ►M1 CONFIDENTIEL UE ◄ vai augstāku, tas norāda datus par dokumentu īpašā reģistrā, kas ir organizācijas rīcībā, ailēs par saņemšanas datumu, dokumenta īpašībām (datums, reģistrācijas un kopijas numurs), tā klasifikāciju, nosaukumu, saņēmēja nosaukumu vai vārdu, datumu, kurā nosūtīts paziņojums par saņemšanu, un datumu, kurā dokuments ir atdots ES autoram vai iznīcināts.

10. Iznīcināšana

a) ES klasificētu informāciju iznīcina atbilstoši norādījumiem, kas ir izklāstīti šo drošības noteikumu 22. iedaļā. Apliecību par iznīcināšanu kopijas ►M1 SECRET UE ◄ un ►M1 TRES SECRET UE/EU TOP SECRET ◄ informācijai nosūta ES reģistram, kas ir sūtījis dokumentus.

b) ES klasificētu informāciju iekļauj ārkārtas iznīcināšanas plānos, kas ir izstrādāti saņēmēja iestādes klasificētiem dokumentiem.

11. Dokumentu aizsardzība

Veic visus pasākumus, lai novērstu neatļautu personu piekļūšanu ES klasificētai informācijai.

12. Kopijas, tulkojumi un izvilkumi

Informāciju ar klasifikācijas pakāpi ►M1 CONFIDENTIEL UE ◄ vai ►M1 SECRET UE ◄ nedrīkst kopēt, tulkot vai izdarīt izvilkumus bez attiecīgās organizācijas drošības dienesta vadītāja atļaujas, kas reģistrē un pārbauda kopijas, tulkojumus vai izvilkumus un nepieciešamības gadījumā tos apzīmogo.

►M1 TRES SECRET UE/EU TOP SECRET ◄ dokumenta atveidošanu vai tulkošanu var atļaut tikai tā autors, kas norāda atļauto kopiju skaitu; ja autoru nevar noteikt, prasību nosūta ►M2 Komisijas Drošības direktorātam ◄.

13. Drošības pārkāpumi

Ja ir noticis drošības pārkāpums, kurā ir iesaistīta ES klasificēta informācija, vai ir aizdomas par šādu pārkāpumu, pēc drošības vienošanās noslēgšanas nekavējoties veic šādas darbības:

a) veic izmeklēšanu, lai noskaidrotu apstākļus, kuros noticis drošības pārkāpums;

b) paziņo ►M2 Komisijas Drošības direktorātam ◄, atbilstošām nacionālām drošības iestādēm un autoram, vai skaidri norāda, ka pēdējam nav paziņots, ja tas nav izdarīts;

c) veic pasākumus drošības pārkāpuma seku mazināšanai;

d) pārskata un īsteno pasākumus, lai novērstu atkārtošanos;

e) īsteno jebkurus pasākumus, ko ir ieteicis ►M2 Komisijas Drošības direktorāts ◄ atkārtošanās novēršanai.

14. Pārbaudes

►M2 Komisijas Drošības direktorātam ◄ ir atļauts, vienojoties par to ar attiecīgajām valstīm vai starptautiskām organizācijām, izvērtēt to pasākumu efektivitāti, kas ir vērsti uz nodotās ES klasificētās informācijas aizsardzību.

15. Ziņojumu sagatavošana

Ja ir parakstīta vienošanās par drošību, kamēr valsts vai starptautiskās organizācijas rīcībā ir ES klasificēta informācija, tā iesniedz gadskārtēju ziņojumu līdz datumam, kas ir norādīts atļaujā nodot klasificētu informāciju, apstiprinot to, ka šie drošības noteikumi ir ievēroti.

▼B

*4. papildinājums*

**Pamatnostādnes par ES klasificētas informācijas nodošanu trešām valstīm vai starptautiskām organizācijām: 2. līmeņa sadarbība**

PROCEDŪRAS

1. Autors atbild par ES klasificētas informācijas nodošanu trešām valstīm vai starptautiskām organizācijām, kuru drošības politika un noteikumi būtiski atšķiras no ES. Komisija atbild koleģiāli par Komisijā izstrādātas *EUCI* nodošanu.

2. Parasti tā iekļauj informāciju, kas ir klasificēta līdz un tostarp ►M1 SECRET UE ◄; tā neiekļauj klasificētu informāciju, kas ir aizsargāta ar īpašām drošības norādēm vai marķējumu.

3. Kamēr drošības vienošanās nav noslēgta, Komisijas loceklis, kas atbild par drošības jautājumiem, izskata lūgumus nodot ES klasificētu informāciju.

4. To darot, viņš/viņa:

   — lūdz to autoru viedokli, kuru *EUCI* grasās nodot,

   — nodibina nepieciešamos sakarus ar saņēmējas valsts vai starptautiskās organizācijas drošības dienestiem, lai saņemtu informāciju par to drošības politiku un noteikumiem un jo īpaši izstrādātu tabulu, kurā ir salīdzinātas klasifikācijas, ko piemēro ES un attiecīgajai valstij vai organizācijai,

   — organizē tikšanos ar Komisijas drošības politikas konsultatīvo grupu vai, nepieciešamības gadījumā, izmantojot klusējošo procedūru, lūdz informāciju dalībvalstu nacionālajām drošības iestādēm, lai iegūtu Komisijas drošības politikas konsultatīvās grupas atzinumu.

5. Komisijas drošības politikas konsultatīvā grupa sniedz atzinumu par:

   — uzticību, ko var izrādīt saņēmējai valstij vai starptautiskai organizācijai, lai izvērtētu drošības riskus ES vai tās dalībvalstīm,

   — izvērtējumu par saņēmēja spēju aizsargāt ES nodoto klasificēto informāciju,

   — ieteikumiem par ES klasificētas informācijas praktisko procedūru (kas, piemēram, norāda tekstu, kurā ir izsvītrotas nevēlamās vietas) un pārsūtītajiem dokumentiem (saglabājot vai izdzēšot ES klasificētus virsrakstus, īpašu marķējumu u.c.),

   — slepenības pakāpes pazemināšanu vai deklasifikāciju pirms informācija ir nodota saņēmējām valstīm vai starptautiskām organizācijām.

6. Komisijas loceklis, kas atbild par drošības jautājumiem, nodod pieprasījumu un Komisijas drošības politikas konsultatīvās grupas atzinumu Komisijai lēmuma pieņemšanai.

DROŠĪBAS NOTEIKUMI, KO PIEMĒRO SAŅĒMĒJIEM

7. Komisijas loceklis, kas atbild par drošības jautājumiem, paziņo saņēmējām valstīm vai starptautiskām organizācijām Komisijas lēmumu par atļauju ES klasificētas informācijas nodošanai un tajā minētajiem ierobežojumiem.

8. Lēmums par informācijas nodošanu stājas spēkā tikai pēc tam, kad saņēmēji ir rakstiski apliecinājuši:

   — izmantot informāciju tikai tiem mērķiem, par kuriem ir panākta vienošanās,

   — aizsargāt informāciju atbilstoši noteikumiem, ko ir izklāstījusi Komisija.

▼B

9. Ja Komisija pēc Komisijas drošības politikas konsultatīvās grupas atzinuma saņemšanas ir pieņēmusi lēmumu par procedūru, kādā apstrādā ES klasificētus dokumentus (izdzēšot vietas, kurās ir pieminēta ES klasifikācija, īpašs marķējums u.c.), piemēro turpmāk izklāstītos noteikumus.

10. Personāls

a) Ierēdņu skaits, kuriem ir piekļuve ES klasificētai informācijai, ir stingri ierobežots un pamatots ar nepieciešamību zināt principu; piekļuve ir tikai tām personām, kuru pienākumu veikšanai tā ir nepieciešama;

b) visiem ierēdņiem vai pilsoņiem, kuriem ir atļauta piekļuve klasificētai informācijai, ko ir izsniegusi Komisija, ir valsts izsniegta drošības pielaide vai piekļuves atļauja atbilstošas klasifikācijas līmeņa informācijai, kura atbilst ES, atbilstoši tam, kas ir izklāstīts salīdzinošajā tabulā;

c) šādas drošības pielaides vai piekļuves atļaujas informācijas nolūkos pārsūta ►M2 Komisijas Drošības direktorāta direktors ◄.

11. Dokumentu nosūtīšana

Praktisku procedūru dokumentu pārsūtīšanai nosaka vienojoties. Kamēr šāda vienošanās nav noslēgta, piemēro 21. iedaļas noteikumus. Vienošanās jo īpaši norāda reģistrus, kuriem pārsūta ES klasificētu informāciju un precīzu adresi, uz kuru pārsūta dokumentus, kā arī kurjerdienestu vai pastu, ko izmanto ES klasificētas informācijas pārsūtīšanai.

12. Reģistrēšana pēc saņemšanas

Valsts saņēmēja nacionālā drošības iestāde vai tai līdzvērtīga valstī, kurā tās valdības vārdā saņem klasificētu informāciju, ko ir pārsūtījusi Komisija, vai saņēmējas starptautiskas organizācijas drošības dienests izveido īpašu reģistru ES klasificētas informācijas reģistrēšanai pēc tās saņemšanas. Reģistrā iekļauj ailes, kurās norāda saņemšanas datumu, ziņas par dokumentu (datumu, reģistrācijas un kopijas numuru), tā klasifikāciju, nosaukumu, adresāta vārdu vai nosaukumu, paziņojuma par saņemšanu nosūtīšanas datumu un datumu, kurā dokumenti ir nosūtīti ES vai iznīcināti.

13. Dokumentu nosūtīšana atpakaļ

Kad saņēmējs nosūta atpakaļ klasificētos dokumentus Komisijai, to veic atbilstoši iepriekšminētajā punktā "Dokumenta pārsūtīšana" izklāstītajam.

14. Aizsardzība

a) Ja dokumentus neizmanto, tos uzglabā drošās tvertnēs, kurās ir atļauts uzglabāt attiecīgās valsts klasificētus dokumentus ar tādu pašu klasifikācijas pakāpi. Uz tvertnes nenorāda neko, pēc kā varētu spriest par tās saturu, un tai ir piekļuve tikai tām personām, kurām ir atļauja apstrādāt ES klasificētu informāciju. Ja tiek izmantotas kodu kombinācijas, kombinācijas ir zināmas tikai tiem ierēdņiem attiecīgajā valstī vai organizācijā, kuriem ir atļauja piekļūt ES klasificētai informācijai, ko uzglabā tvertnēs, un kuras nomaina ik pēc sešiem mēnešiem vai ātrāk, ja ierēdnis tiek pārcelts citā amatā, ja vienam no ierēdņiem, kas zina kodu kombināciju, tiek anulēta drošības pielaide, vai pastāv kompromitēšanas risks.

b) ES klasificētus dokumentus izņem no drošības tvertnes tikai tie ierēdņi, kuriem ir piekļuve ES klasificētiem dokumentiem un kuriem ir nepieciešamība zināt. Tie atbild par šādu dokumentu uzglabāšanu seifos tik ilgi, kamēr tie ir viņu rīcībā, jo īpaši, lai nodrošinātu to, ka neatļautas personas nevar tiem piekļūt. Viņi

▼B

nodrošina arī to, ka dokumentus uzglabā seifā pēc to izmantošanas un pēc darba laika.

c) Nekopē dokumentu ar klasifikācijas pakāpi ►M1 CONFIDENTIEL UE ◄ vai augstāku, kamēr ►M2 Komisijas Drošības direktorāts ◄ to nav atļāvis.

d) ►M2 Komisijas Drošības direktorāts ◄ nosaka un apstiprina procedūru ātrai un pilnīgai dokumentu iznīcināšanai ārkārtas gadījumos.

15. Fiziskā drošība

a) Kad tos neizmanto, seifi, ko izmanto ES klasificētas informācijas uzglabāšanai, visu laiku ir slēgti.

b) Kad apkalpojošam personālam vai apkopējiem nepieciešams ienākt vai strādāt telpā, kurā atrodas seifi, tos visu laiku pavada valsts vai organizācijas drošības dienesta pārstāvis vai ierēdnis, kas īpaši atbild par drošības telpas pārraudzīšanu.

c) Ārpus parastā darba laika (naktīs, brīvdienās un valsts svētku dienās) seifus, kuros atrodas ES klasificēti dokumenti, sargā vai nu sargs, vai automātiskā signalizācija.

16. Drošības pārkāpumi

Ja ir noticis drošības pārkāpums, kurā ir iesaistīta ES klasificēta informācija vai ir aizdomas par šādu pārkāpumu, nekavējoties veic šādus pasākumus:

a) nekavējoties pārsūta ziņojumu ►M2 Komisijas Drošības direktorātam ◄ vai tās dalībvalsts nacionālajam drošības dienestam, kas ir uzņēmusies pārsūtīt dokumentus (ar kopiju ►M2 Komisijas Drošības direktorātam ◄);

b) veic izmeklēšanu, pabeidzot iesniedz pilnīgu ziņojumu drošības dienestam (skatīt iepriekšminēto a) apakšpunktu). Pēc tam veic nepieciešamos pasākumus situācijas uzlabošanai.

17. Pārbaudes

►M2 Komisijas Drošības direktorātam ◄ ir atļauts, vienojoties par to ar attiecīgajām valstīm vai starptautiskām organizācijām, izvērtēt to pasākumu efektivitāti, kas ir vērsti uz nodotās ES klasificētās informācijas aizsardzību.

18. Ziņojumu sagatavošana

Ja ir parakstīta vienošanās par drošību, kamēr valsts vai starptautiskās organizācijas rīcībā ir ES klasificēta informācija, tā iesniedz gadskārtēju ziņojumu līdz datumam, kas ir norādīts atļaujā nodot klasificētu informāciju, apstiprinot to, ka šie drošības noteikumi ir ievēroti.

▼B

*5. papildinājums*

**Pamatnostādnes par ES klasificētas informācijas nodošanu trešām valstīm vai starptautiskām organizācijām: 3. līmeņa sadarbība**

PROCEDŪRAS

1. Laiku pa laikam Komisija var vēlēties sadarboties konkrētos apstākļos ar valstīm vai organizācijām, kas nevar sniegt garantijas, kuras pieprasa šie drošības noteikumi, tomēr šādas sadarbības rezultātā var tikt nodota ES klasificēta informācija.

2. Autors atbild par ES klasificētas informācijas nodošanu trešām valstīm vai starptautiskām organizācijām, kuru drošības politika un noteikumi būtiski atšķiras no ES. Komisija atbild koleģiāli par Komisijā izstrādātas *EUCI* nodošanu.

   Parasti tā iekļauj informāciju, kas ir klasificēta līdz un tostarp ►M1 SECRET UE ◄; tā neiekļauj klasificētu informāciju, kas ir aizsargāta ar īpašām drošības norādēm vai marķējumu.

3. Komisija apspriež iespēju atklāt klasificētu informāciju, izvērtē saņēmēja nepieciešamību zināt un lemj par tādu klasificētās informācijas saturu, ko var atklāt.

4. Ja Komisija to atbalsta, Komisijas loceklis, kas atbild par drošības jautājumiem:

   — lūdz to autoru viedokli, kuru *EUCI* grasās nodot,

   — organizē tikšanos ar Komisijas drošības politikas konsultatīvo grupu vai, nepieciešamības gadījumā, izmantojot klusējošo procedūru, lūdz informāciju dalībvalstu nacionālajām drošības iestādēm, lai iegūtu Komisijas drošības politikas konsultatīvās grupas atzinumu.

5. Komisijas drošības politikas konsultatīvā grupa sniedz atzinumu par:

   a) ES un tās dalībvalstu drošības risku izvērtējumu;

   b) tādas informācijas klasifikācijas līmeni, ko var atklāt;

   c) slepenības pakāpes pazemināšanu vai deklasificēšanu pirms informācijas atklāšanas;

   d) procedūru atklāto dokumentu apstrādāšanai (skatīt turpmāk minēto);

   e) iespējamām pārsūtīšanas metodēm (pasta pakalpojumu izmantošanu, publisko vai drošo telekomunikāciju sistēmu izmantošanu, diplomātisko pastu, kurjerdienestu pakalpojumu izmantošanu u.c.).

6. Dokumentus, kas ir nodoti valstu vai starptautisko organizāciju rīcībā, kas ir uzskaitītas šajā papildinājumā, parasti sagatavo, neatsaucoties uz informācijas avotu vai ES klasifikāciju. Komisijas drošības politikas konsultatīvā grupa var ieteikt:

   — īpaša marķējuma vai koda vārda lietošanu,

   — īpašas klasifikācijas sistēmas izmantošanu, kas saista informācijas jutīgumu ar kontroles pasākumiem, ko jāizmanto saņēmējam pārsūtot dokumentu.

7. ►M2 Komisijas loceklis, kas atbild par drošības jautājumiem ◄ pārsūta Komisijas drošības politikas konsultatīvās grupas atzinumu Komisijai lēmuma pieņemšanai.

8. Kad Komisija ir apstiprinājusi ES klasificētas informācijas atklāšanu un praktisku īstenošanas procedūru, ►M2 Komisijas Drošības direktorāts ◄ nodibina nepieciešamos sakarus ar tās valsts vai organizācijas drošības dienestu, lai veicinātu norādīto drošības pasākumu piemērošanu.

▼B

9. Komisijas loceklis, kas atbild par drošības jautājumiem, informē dalībvalstis par informācijas būtību un klasifikāciju, uzskaitot organizācijas un valstis, kurām to var nodot saskaņā ar Komisijas lēmumu.

10. ►M2 Komisijas Drošības direktorāts ◄ veic visus nepieciešamos pasākumus, lai veicinātu jebkuru sekojošu zaudējumu izvērtēšanu un procedūru pārskatīšanu.

    Katru reizi, kad mainās sadarbības nosacījumi, Komisija pārskata jautājumu.

DROŠĪBAS NOTEIKUMI, KO PIEMĒRO SAŅĒMĒJIEM

11. Komisijas loceklis, kas atbild par drošības jautājumiem, paziņo saņēmējām valstīm vai organizācijām par Komisijas lēmumu atļaut ES klasificētas informācijas nodošanu, kā arī par sīki izstrādātiem noteikumiem, ko ir ieteikusi Komisijas drošības politikas konsultatīvā grupa un apstiprinājusi Komisija.

12. Lēmums par informācijas nodošanu stājas spēkā tikai pēc tam, kad saņēmēji ir rakstiski apliecinājuši:

    — izmantot informāciju tikai tai sadarbībai, ko ir apstiprinājusi Komisija,

    — sniegt informācijai aizsardzību, ko ir pieprasījusi Komisija.

13. Dokumentu nosūtīšana

    a) Par praktisku procedūru dokumentu pārsūtīšanai vienojas ►M2 Komisijas Drošības direktorāts ◄ un saņēmējas valsts vai starptautiskas organizācijas drošības dienesti. Jo īpaši tie norāda adreses, uz kurām jāpārsūta informācija.

    b) Dokumentus ar klasifikācijas pakāpi ►M1 CONFIDENTIEL UE ◄ un augstāku pārsūta dubultā aploksnē. Iekšējā aploksne ir īpaši apzīmogota vai arī uz tās ir norādīts koda vārds, kā arī īpašā klasifikācija, kas ir piemērota dokumentam. Katram klasificētam dokumentam pievieno saņemšanas veidlapu. Saņemšanas veidlapa, kas pati par sevi nav klasificēta, norāda tikai ziņas par dokumentu (tā reģistrācijas numuru, datumu, kopijas numuru) un tā valodu, taču ne nosaukumu.

    c) Iekšējo aploksni ievieto ārējā aploksnē, uz kuras ir norādīts iepakojuma numurs, lai varētu sniegt paziņojumu par saņemšanu. Uz ārējās aploksnes drošības klasifikāciju nenorāda.

    d) Paziņojumu par saņemšanu, uz kura ir norādīts iepakojuma numurs, vienmēr iedod kurjeriem.

14. Reģistrēšana pēc saņemšanas

    Saņēmējas valsts nacionālā drošības iestāde vai tai līdzvērtīga iestāde valstī, kas tās valdības vārdā saņem klasificētu informāciju, ko ir pārsūtījusi Komisija, vai saņēmējas starptautiskas organizācijas drošības dienests izveido īpašu reģistru ES klasificētas informācijas reģistrēšanai pēc tās saņemšanas. Reģistrā iekļauj ailes, kurās norāda saņemšanas datumu, ziņas par dokumentu (datumu, reģistrācijas un kopijas numuru), tā klasifikāciju, nosaukumu, adresāta vārdu vai nosaukumu, paziņojuma par saņemšanu nosūtīšanas datumu un datumu, kurā dokumenti ir nosūtīti ES vai iznīcināti.

15. Apmainītās klasificētās informācijas izmantošana un aizsardzība

    a) Informāciju ar klasifikācijas pakāpi ►M1 SECRET UE ◄ apstrādā tam īpaši iecelti ierēdņi, kam ir atļauja piekļūt informācijai ar šādu klasifikāciju. To uzglabā kvalitatīvos drošos kabinetos, kurus drīkst atvērt tikai tās personas, kam ir atļauja piekļūt informācijai, kura tajos atrodas. Visu laiku apsargā zonas, kurās atrodas šādi kabineti, turklāt ir izveidota pārbaudes sistēma, lai nodrošinātu tikai tādu personu ienākšanu, kam ir atbilstošas

▼B

atļaujas. ►M1 SECRET UE ◄ līmeņa informāciju pārsūta ar diplomātisko pastu, drošo pastu vai drošo telekomunikāciju. ►M1 SECRET UE ◄ dokumentu kopē tikai ar rakstisku autora atļauju. Visas kopijas reģistrē un uzrauga. Izziņas izsniedz par visām darbībām, kas attiecas uz ►M1 SECRET UE ◄ dokumentiem.

b) ►M1 CONFIDENTIEL UE ◄ informāciju apstrādā ierēdņi, kuriem ir atļauja būt informētiem par attiecīgajiem jautājumiem. Dokumentus uzglabā slēgtos drošos kabinetos kontrolētās zonās.

►M1 CONFIDENTIEL UE ◄ informāciju nosūta ar diplomātisko pastu, militāro pastu un drošo telekomunikāciju. Saņēmēja struktūra var kopēt dokumentus, reģistrējot to numuru un izplatīšanu īpašos reģistros.

c) ►M1 RESTREINT UE ◄ informāciju apstrādā telpās, kurām nevar piekļūt neatļautas personās, un uzglabā slēgtās tvertnēs. Dokumentus var pārsūtīt ar valsts pastu kā ierakstītas vēstules dubultā aploksnē un, ārkārtas gadījumos darbību laikā, ar neaizsargāto sabiedrisko telekomunikāciju sistēmu. Saņēmēji var kopēt.

d) Neklasificētai informācijai īpaši aizsardzības pasākumi nav nepieciešami un to var pārsūtīt ar pastu un valsts telekomunikāciju sistēmu. Adresāti informāciju var kopēt.

16. Iznīcināšana

Iznīcina dokumentus, kas vairs nav vajadzīgi. Attiecībā uz ►M1 RESTREINT UE ◄ un ►M1 CONFIDENTIEL UE ◄ dokumentiem īpašos reģistros ieraksta atbilstošas piezīmes. Attiecībā uz ►M1 SECRET UE ◄ dokumentiem apliecības par iznīcināšanu izsniedz un paraksta divas personas, kas piedalās to iznīcināšanā.

17. Drošības pārkāpumi

Ja ►M1 CONFIDENTIEL UE ◄ vai ►M1 SECRET UE ◄ informācija ir kompromitēta vai ir aizdomas par kompromitēšanu, valsts nacionālais drošības dienests vai drošības dienesta vadītājs organizācijā izmeklē apstākļus, kuros notikusi kompromitēšana. Par rezultātiem paziņo ►M2 Komisijas Drošības direktorātam ◄. Veic nepieciešamos pasākumus, lai novērstu nepareizas procedūras vai uzglabāšanas metodes tad, ja tās ir izraisījušas kompromitēšanu.

▼B

*6. papildinājums*

**SAĪSINĀJUMU SARAKSTS**

| | |
|---|---|
| ACPC | Pasūtījumu un līgumu padomdevēja komiteja |
| CrA | Kripto iestāde |
| CISO | Galvenais IT drošības speciālists |
| COMPUSEC | Datoru drošība |
| COMSEC | Komunikāciju drošība |
| CSO | ►M2 Komisijas Drošības direktorāts ◄ |
| EDAP | Eiropas drošības un aizsardzības politika |
| EUCI | ES klasificēta informācija |
| IA | *INFOSEC* iestāde |
| INFOSEC | Informācijas drošība |
| IO | Informācijas īpašnieks |
| ISO | Starptautiskā standartizācijas organizācija |
| IT | Informācijas tehnoloģija |
| LISO | Vietējais IT drošības speciālists |
| LSO | Vietējais drošības speciālists |
| MSO | Sanāksmes drošības speciālists |
| NSA | Nacionālā drošības iestāde |
| PC | Personālais dators |
| RCO | Reģistra kontrolieris |
| SAA | Drošības akreditācijas iestāde |
| SecOPS | Drošības ekspluatācijas procedūras |
| SSRS | Sistēmas drošības prasību izklāsts |
| TA | Tempest iestāde |
| TSO | Tehniskās sistēmas īpašnieks |

▼M3

| | |
|---|---|
| DSA | atbildīgā drošības iestāde, |
| FSC | objekta drošības pielaide, |
| FSO | objekta drošības speciālists, |
| PSC | personāla drošības pielaide, |
| SAL | dokuments, kurā izklāstīti drošības aspekti, |
| SCG | drošības klasifikācijas rokasgrāmata. |