32001D0264

L 101/1 *EUROOPA ÜHENDUSTE TEATAJA* 11.4.2001

# NÕUKOGU OTSUS, 19. märts 2001, millega võetakse vastu nõukogu julgeolekueeskirjad

(2001/264/EÜ)

EUROOPA LIIDU NÕUKOGU,

võttes arvesse Euroopa Ühenduse asutamislepingut, eriti selle artikli 207 lõiget 3,

võttes arvesse nõukogu 5. juuni 2000. aasta otsust 2000/396/EÜ/ESTÜ/Euratom, millega on vastu võetud nõukogu töökord, [1] eriti selle artiklit 24,

ning arvestades järgmist:

(1) Nõukogu töö arendamiseks valdkondades, mis eeldavat teatavat konfidentsiaalsust, on otstarbekas luua ulatuslik julgeolekusüsteem, mis hõlmaks nõukogu, selle peasekretariaati ja liikmesriike.

(2) Selline süsteem peaks koondama ühte teksti kõigi varasemate otsuste ja sama valdkonda käsitlevate sätete sisu.

(3) Tegelikkuses käsitleb suurem osa salastatuse kategooriasse CONFIDENTIEL UE või kõrgema salastatuse kategooriasse kuuluvat Euroopa Liidu teavet ühist julgeoleku- ja kaitsepoliitikat.

(4) Niiviisi kehtestatud julgeolekusüsteemi tõhususe tagamiseks peaksid liikmesriigid sellega ühinema, võttes käesoleva direktiivi sätete järgimiseks vajalikud siseriiklikud meetmed, kui nende pädevad asutused või ametnikud käitlevad Euroopa Liidu salajast teavet.

(5) Nõukogu avaldab rahulolu komisjoni kavatsuse üle võtta käesoleva otsuse kohaldamiskuupäevaks kasutusele ulatuslik süsteem, mis on kooskõlas käesoleva otsuse lisadega ja mille eesmärk on tagada otsustusprotsessi tõrgeteta toimimine Euroopa Liidus.

(6) Nõukogu rõhutab, et vajaduse korral tuleb ka Euroopa Parlament ja komisjon kaasata Euroopa Liidu ja tema liikmesriikide huvide kaitsmiseks vajalike konfidentsiaalsusreeglite ja -standardite kohaldamisse.

(7) Käesolev otsus ei piira asutamislepingu artikli 255 ega selle rakendamiseks antud õigusaktide kohaldamist.

(8) Käesolev otsus ei piira liikmesriikide seniste tavade kohaldamist seoses riikide parlamentide teavitamisega Euroopa Liidu toimingutest,

ON VASTU VÕTNUD JÄRGMISE OTSUSE:

*Artikkel 1*

Käesolevaga kiidetakse heaks lisas sätestatud nõukogu julgeolekueeskirjad.

*Artikkel 2*

1. Peasekretär/kõrge esindaja võtab asjakohased meetmed tagamaks, et Euroopa Liidu salastatud teabe käitlemisel nõukogu peasekretariaadis (edaspidi "peasekretariaat") peavad peasekretariaadi ametnikud ja muud teenistujad, peasekretariaadiga lepingu sõlminud tööettevõtjad ja peasekretariaati lähetatud isikud kinni artiklis 1 osutatud reeglitest ning et neist peetakse kinni ka nõukogu tööruumides ja Euroopa Liidu detsentraliseeritud asutustes. [2]

[1] EÜT L 149, 23.6.2000, lk 21.

[2] Vt nõukogu 10. novembri 2000. aasta järeldused.

2. Liikmesriigid võtavad kooskõlas siseriikliku korraga asjakohased meetmed tagamaks, et Euroopa Liidu salastatud teabe käitlemisel peavad järgmised isikud kinni artiklis 1 osutatud reeglitest:

a) Euroopa Liidu juures olevate liikmesriikide alaliste esinduste liikmed ja nõukogu või selle organite koosolekutel või muus nõukogu tegevuses osalevate riiklike delegatsioonide liikmed;

b) liikmesriikide valitsuste muud liikmed, kes käitlevad Euroopa Liidu salastatud teavet olenemata sellest, kas nad tegutsevad liikmesriikide territooriumil või välismaal, ja

c) liikmesriikide välislepingupartnerid ja lähetuses olevad töötajad, kes käitlevad Euroopa Liidu salastatud teavet.

Liikmesriigid teatavad võetud meetmetest viivitamata peasekretariaadile.

3. Lõigetes 1 ja 2 nimetatud meetmed võetakse enne 30. novembrit 2001.

*Artikkel 3*

Kooskõlas lisa I osas sätestatud julgeoleku üldpõhimõtete ja miinimumstandarditega võib peasekretär/kõrge esindaja võtta meetmeid lisa II osa I jao punktide 1 ja 2 kohaselt.

*Artikkel 4*

Käesoleva direktiiviga asendatakse alates kohaldamiskuupäevast järgmised õigusaktid:

a) nõukogu 27. aprilli 1998. aasta otsus 98/319/EÜ, mis käsitleb korda, mille kohaselt nõukogu peasekretariaadi ametnikele ja töötajatele võimaldatakse juurdepääs nõukogu käsutuses olevale salastatud teabele; [1]

b) kõrge esindajana tegutseva peasekretäri 27. juuli 2000. aasta otsus nõukogu peasekretariaadi suhtes kohaldatavate salastatud teabe kaitse meetmete kohta; [2]

c) nõukogu peasekretäri 22. mai 1997. aasta otsus 433/97 Cortesy võrgu töö eest vastutavate ametnike julgeolekukontrolli korra kohta.

*Artikkel 5*

1. Käesolev otsus jõustub selle avaldamise päeval.

2. Käesolevat otsust kohaldatakse alates 1. detsembrist 2001.

Brüssel, 19. märts 2001

*Nõukogu nimel*

*eesistuja*

A. LINDH

---

[1] EÜT L 140, 12.5.1998, lk 12.

[2] EÜT C 239, 23.8.2000, lk 1.

*LISA*

# EUROOPA LIIDU NÕUKOGU JULGEOLEKUEESKIRJAD

**SISUKORD**

*LK*

**Liited**

I OSA

## JULGEOLEKU ÜLDPÕHIMÕTTED JA MIINIMUMSTANDARDID

SISSEJUHATUS

1. Käesolevate sätetega nähakse ette julgeoleku üldpõhimõtted ja miinimumstandardid, mida nõukogu, nõukogu peasekretariaat (edaspidi "peasekretariaat"), liikmesriigid ja Euroopa Liidu detsentraliseeritud asutused (edaspidi "detsentraliseeritud asutused") peavad silmas pidama, et tagada julgeolek ja kindlustada kõigile ühise kaitsestandardi kehtestamine.

2. Mõiste "Euroopa Liidu salastatud teave" tähendab igasugust teavet ja materjali, mille ilma loata avaldamine võib eri määral kahjustada Euroopa Liidu huve või ühte või mitut Euroopa Liidu liikmesriiki, kui selline teave on pärit Euroopa Liidust või saadud tema liikmesriikidelt, kolmandatelt riikidelt või rahvusvahelistelt organisatsioonidelt.

3. Käesolevates eeskirjades kasutatakse järgmisi mõisteid:

   a) *dokument* — igasugune kiri, märkus, protokoll, aruanne, memorandum, signaal/sõnum, visand, foto, slaid, film, kaart, skeem, plaan, kaust, šabloon, koopiapaber, kirjutusmasina- ja printerilint, magnetlint, kassett, arvutiketas, CD-ROM või muu füüsiliselt eksisteeriv andmekandja;

   b) *materjal* — eespool punktis a määratletud dokumendid ja kõik valmistatud või valmistamisel olevad seadmed või relvad.

4. Julgeoleku peamised eesmärgid on järgmised:

   a) kaitsta Euroopa Liidu salastatud teavet spionaaži, kahjustamise ja loata avaldamise eest;

   b) kaitsta side- ja teabesüsteemides ning -võrkudes käideldavat Euroopa Liidu informatsiooni terviklikkuse ja kättesaadavuse ohtu seadmise eest;

   c) kaitsta Euroopa Liidu teavet sisaldavaid rajatisi sabotaaži ja kuritahtliku kahjustamise eest;

   d) kaitse ebaõnnestumise korral hinnata tekitatud kahju, piirata selle tagajärgi ja võtta vajalikke heastamismeetmeid.

5. Kindla julgeoleku aluseks on järgmised seigad:

   a) igas liikmesriigis on siseriiklik julgeolekuorganisatsioon, kes vastutab järgmiste asjaolude eest:

      i) spionaaži, sabotaaži, terrorismi ja muu õõnestava tegevuse kohta kogutakse luureandmeid ning need andmed talletatakse;

      ii) liikmesriigi valitsusele ja tema kaudu nõukogule antakse teavet julgeolekuohtude olemuse kohta ja nõu, milliste vahenditega nende ohtude eest kaitsta;

   b) igas liikmesriigis ja peasekretariaadis on tehniline teabeturbeasutus, kes vastutab koostöö eest asjaomase julgeolekuasutusega seoses teabega julgeolekuohtude tehniliste külgede kohta ja nõuannetega, milliste vahenditega nende ohtude eest kaitsta;

   c) valitsusasutused, ametkonnad ja peasekretariaadi asjaomased ametid teevad regulaarselt koostööd, et vastavalt vajadusele määrata kindlaks ja soovitada:

      i) millist teavet, milliseid vahendeid ja rajatisi on vaja kaitsta, ja

      ii) ühised kaitsestandardid.

6. Salastatuse puhul eeldab kaitstava teabe ja kaitstavate materjalide valik ning vajaliku kaitsetaseme hindamine hoolikust ja kogemusi. On äärmiselt oluline, et kaitse tase vastaks konkreetse kaitstava teabe või kaitstava materjali julgeoleku olulisusele. Teabe sujuva liikumise tagamiseks tuleb võtta meetmeid, mis välistaksid ülesalastamise. Salastamissüsteem on see vahend, mille abil saab kõnealused põhimõtted ellu viia; samalaadset salastamissüsteemi tuleks järgida spionaaži, sabotaaži, terrorismi ja muude ohtude kohta vastulöökide kavandamise ja korraldamise puhul, nii et kõige rohkem kaitstaks kõige olulisemaid salastatud teavet sisaldavaid rajatisi ja kõige tundlikumad kohti neis rajatistes.

ÜLDPÕHIMÕTTED

7. **Julgeolekumeetmed:**

a) laienevad kõigile isikutele, kellel on juurdepääs salastatud teabele, salastatud teabe kandjatele, kõigile sellist teavet sisaldavatele ruumidele ja olulistele rajatistele;

b) peavad olema kavandatud nii, et oleks võimalik avastada isikuid, kelle positsioon võib seada ohtu salastatud teabe ja sellist teavet sisaldavate oluliste rajatiste julgeoleku, ning tagada nende kõrvaldamine või viimine teisele tööle;

c) takistavad loata isikute juurdepääsu salastatud teabele ja rajatistele, mis sisaldavad sellist teavet;

d) tagavad salastatud teabe levitamise ainult lähtudes teadmisvajaduse põhimõttest, mis on esmatähtis julgeoleku kõigi aspektide seisukohast;

e) tagavad igasuguse teabe terviklikkuse (st välditakse rikkumist, loata muutmist ja loata kustutamist) ja kättesaadavuse (st ei takistata nende isikute juurdepääsu, kellel on seda vaja ja kellel on selleks luba) olenemata sellest, kas teave on salastatud või salastamata, ja eriti kui selline teave on salvestatud või seda töödeldakse või edastatakse elektromagnetilisel kujul.

JULGEOLEKUKORRALDUS

**Ühised miinimumstandardid**

8. Nõukogu ja kõik liikmesriigid tagavad, et kõik haldus- ja/või valitsusasutused, muud Euroopa Liidu institutsioonid, ametkonnad ja tööettevõtjad järgivad ühiseid julgeoleku miinimumstandardeid ja seetõttu võib Euroopa Liidu salastatud teavet edastada kindla teadmisega, et sellega käiakse kõikjal ringi võrdse hoolega. Sellised miinimumstandardid hõlmavad töötajate julgeolekukontrolli kriteeriume ja Euroopa Liidu salastatud teabe kaitsmise korda.

TÖÖTAJATEGA SEOTUD JULGEOLEK

**Töötajate julgeolekukontroll**

9. Kui keegi taotleb juurdepääsu kategooriasse CONFIDENTIEL UE või rangemasse kategooriasse kuuluvale salastatud teabele, peab ta enne sellise juurdepääsu saamist läbima julgeolekukontrolli. Samasuguse julgeolekukontrolli peavad läbima ka need isikud, kelle tööülesannete hulka kuulub salastatud teavet sisaldavate side- ja teabesüsteemide tehniline käitamine või hooldamine. Kõnealuse julgeolekukontrolliga tuleb kindlaks teha, kas asjaomane isik:

a) on vaieldamatult lojaalne;

b) on sellise iseloomu ja otsustusvõimega, et see ei sea kahtluse alla tema ausust salastatud teabe käitlemisel, või

c) võib olla aldis välisriikidest või muudest allikatest pärinevale survele näiteks varasema elukoha või varasemate suhete tõttu, mille puhul võib tegemist olla ohuga julgeolekule.

Julgeolekukontrolli käigus pööratakse eriti üksikasjalikku tähelepanu isikutele:

d) kellele antakse juurdepääs teabele, mis kuulub kategooriasse TRÈS SECRET UE/EU TOP SECRET;

e) kes töötavad ametikohal, kus on pidev juurdepääs märkimisväärsele hulgale teabele, mis kuulub kategooriasse SECRET UE;

f) kelle tööülesannetega kaasneb erijuurdepääs missioonikriitilistele side- või infosüsteemidele ja sellega ka võimalus pääseda ilma loata juurde suurele hulgale Euroopa Liidu salastatud teabele või tekitada tehnilise sabotaažiga tõsist kahju kõnealusele ülesandele.

Punktides d, e ja f kirjeldatud juhtudel kasutatakse võimalikult suures ulatuses taustauuringute tehnikat.

10. Kui tööle võetakse inimesed, kellel ei ole teadmisvajadust, kuid kellel võib asjaolude tõttu olla juurdepääs Euroopa Liidu salastatud teabele (nt käskjalad, turvatöötajad, hooldustöötajad ja koristajad jmt), peavad nad enne läbima nõuetekohase julgeolekukontrolli.

**Julgeolekukontrolli register**

11. Kõik teenistused, organid ja üksused, kes käitlevad Euroopa Liidu salastatud teavet või kelle ruumides on missioonikriitilised side- või infosüsteemid, peavad nendega tegelevate isikute julgeolekusertifikaatide kohta registrit. Vajaduse korral kontrollitakse iga julgeolekusertifikaati tagamaks, et see on vastavuses asjaomase isiku käsilolevate ülesannetega; seda kontrollitakse eelisjärjekorras uuesti alati, kui saadakse uut teavet, mis näitab, et asjaomase isiku töö salastatud teabega ei ole enam kooskõlas julgeolekuhuvidega. Julgeolekusertifikaatide registrit peab asjaomase teenistuse, organi või asutuse julgeolekujuht.

**Töötajatele antavad julgeolekujuhendid**

12. Kõigile töötajatele, kellel on oma ametikoha tõttu juurdepääs salastatud teabele, antakse tööleasumisel ja regulaarsete vaheaegade järel põhjalikud juhtnöörid julgeoleku vajalikkuse ja selle saavutamise korra kohta. Kasulik on juurutada kord, mille kohaselt kõik sellised töötajad peaksid kirjalikult kinnitama, et nad saavad täielikult aru nende tööga seotud olulistest julgeolekueeskirjadest.

**Juhtkonna vastutus**

13. Juhtkond on kohustatud teadma, kes nende töötajatest tegelevad oma töö käigus salastatud teabega või kellel on juurdepääs missioonikriitilistele side- ja teabesüsteemidele, ning registreerima kõik vahejuhtumid ja tõenäolised nõrgad kohad, mis võivad mõjutada julgeolekut, ja neist teatama.

**Töötajate julgeolekustaatus**

14. Tuleb kehtestada kord tagamaks, et juhul, kui mõne isiku kohta saadakse teada teda kahjustavat infot, tehakse kindlaks, kas see isik töötab salastatud teabega või kas tal on juurdepääs missioonikriitilistele side- või teabesüsteemidele, ja teatatakse sellest asjaomasele asutusele. Kui tehakse kindlaks, et sellise isiku näol on tegemist ohuga julgeolekule, tagandatakse või kõrvaldatakse ta nende tööülesannete täitmiselt, millega seoses ta võib julgeoleku ohtu seada.

FÜÜSILINE JULGEOLEK

**Kaitsevajadus**

15. Euroopa Liidu salastatud teabe kaitsmise tagamiseks rakendatavate füüsiliste julgeolekumeetmete tase on proportsionaalne teabe ja materjali salastatuse taseme, hulga ja neile suunatud ohuga. Seepärast tuleb vältida nii liiga kõrge kui ka liiga madala salastatuse taseme määramist ning salastatuse tasemed tuleb regulaarselt läbi vaadata. Kõik Euroopa Liidu salastatud teabe valdajad järgivad kõnealuse teabe salastatuse taseme määramisel ühtseid tavasid ja peavad kaitset vajava teabe ja materjali säilitamisel, edastamisel ja hävitamisel kinni ühistest kaitsestandarditest.

**Kontrollimine**

16. Enne kui Euroopa Liidu salastatud teavet sisaldav koht jäetakse järelevalveta, peab sellise teabe eest vastutav isik tagama, et teavet säilitatakse turvaliselt ja kõik turvaseadmed (lukud, häireseadmed jms) on aktiveeritud. Pärast tööpäeva lõppu toimub täiendav sõltumatu kontroll.

**Hoonete julgeolek**

17. Hooned, kus on Euroopa Liidu salastatud teavet või missioonikriitilisi side- ja teabesüsteeme, peavad olema kaitstud loata juurdepääsu eest. Euroopa Liidu salastatud teabe kaitsmise viis (nt trellitatud aknad, ukselukud, uksevalve, juurdepääsu kontrollimise automaatsüsteemid, turvakontrollid ja valvepatrullid, häiresüsteemid, sissetungimise avastamise süsteemid ja valvekoerad) sõltub järgmisest:

a) kaitstava teabe ja materjali salastatuse tase, maht ja asukoht hoones;

b) sellise teabe ja materjali turvakonteinerite kvaliteet;

c) hoone füüsilised omadused ja asukoht;

18. Side- ja teabesüsteemide kaitsmise viis sõltub samuti sellest, kui väärtuslikuks asjaomast teavet peetakse ja kui suurt kahju võib tekitada julgeoleku ohtu sattumine, sellest, millised on hoone füüsilised omadused ja hoone asukoht, ning sellest, milline on süsteemi asukoht hoones.

**Situatsioonkavad**

19. Tuleb ette valmistada üksikasjalikud kavad salastatud teabe kaitsmiseks kohaliku või riikliku hädaolukorra puhul.

TEABETURVE (INFOSEC)

20. INFOSEC on seotud selliste julgeolekumeetmete kindlaksmääramise ja rakendamisega, millega kaitstakse side-, teabe- või muudes elektroonilistes süsteemides töödeldavat, salvestatavat või edastatavat teavet juhuslike või tahtlike toimingute eest, mis võiksid kahjustada teabe salastatust, terviklikkust või kättesaadavust. Võetakse piisavad vastumeetmed selleks, et välistada volitamata kasutajate juurdepääs Euroopa Liidu teabele, volitatud kasutajate juurdepääsu tõkestamine Euroopa Liidu teabele ja Euroopa Liidu teabe rikkumine, loata muutmine ja loata kustutamine.

KAITSE SABOTAAŽI JA KURITAHTLIKU KAHJUSTAMISE MUUDE VORMIDE VASTU

21. Salastatud teavet sisaldavate oluliste rajatiste kaitseks võetud füüsilised ettevaatusabinõud on parim julgeolekugarantii sabotaaži ja kuritahtliku kahjustamise muude vormide vastu ning seda ei saa asendada ainult töötajate julgeolekukontrolli läbiviimisega. Pädev siseriiklik organ kogub luureandmeid spionaaži, sabotaaži, terrorismi ja muu õõnestava tegevuse kohta.

SALASTATUD TEABE AVALDAMINE KOLMANDATELE RIIKIDELE JA RAHVUSVAHELISTELE ORGANISATSIOONIDELE

22. Nõukogust pärit Euroopa Liidu salastatud teabe avaldamise kolmandale riigile või rahvusvahelisele organisatsioonile otsustab nõukogu. Kui teave, mida soovitakse avaldada, ei ole pärit nõukogust, küsib nõukogu avaldamiseks kõigepealt teabe koostajate nõusolekut. Kui teabe koostajaid ei ole võimalik kindlaks teha, võtab nõukogu vastutuse teabe eest endale.

23. Kui nõukogu saab kolmandatelt riikidelt, rahvusvahelistelt organisatsioonidelt või muudelt kolmandatelt isikutelt salastatud teavet, kaitstakse kõnealust teavet selle salastatuse taseme kohaselt ja pidades kinni standarditest, mis on samaväärsed käesolevate eeskirjadega Euroopa Liidu salastatud teabe jaoks kehtestatutega, või rangematest standarditest, kui seda eeldab teabe avaldanud kolmas isik. Võib korraldada vastastikusi kontrollimisi.

24. Eespool kirjeldatud põhimõtteid rakendatakse kooskõlas II osas esitatud üksikasjalike sätetega.

II OSA

I JAGU

## JULGEOLEKUKORRALDUS EUROOPA LIIDU NÕUKOGUS

### Peasekretär/kõrge esindaja

1. Peasekretär/kõrge esindaja:

   a) viib ellu nõukogu julgeolekupoliitikat;

   b) uurib julgeolekuprobleeme, mille nõukogu või tema pädevad organid talle on edastanud;

   c) uurib tihedas koostöös liikmesriikide julgeolekuasutustega (või muude asjakohaste asutustega) küsimusi, mis toovad kaasa muutusi nõukogu julgeolekupoliitikas. Kõnealuste asutuste loetelu on esitatud liites 1.

2. Peasekretäri/kõrge esindaja ülesandeks on eelkõige:

   a) koordineerida kõiki nõukogu toimingutega seotud julgeolekuküsimusi;

   b) nõuda, et iga liikmesriik looks kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluva teabe keskregistri, ja nõuda, et selline register loodaks vajaduse korral ka Euroopa Liidu detsentraliseeritud asutustes;

   c) adresseerida liikmesriikide määratud asutustele liikmesriikide julgeolekuasutustele esitatud taotlused peasekretariaadis töötavate isikute julgeolekukontrolli läbimise kohta VI jao kohaselt;

   d) uurida või lasta uurida iga Euroopa Liidu salastatud teabe lekkimist, mis esmapilgul usutavate tõendite kohaselt on toimunud peasekretariaadis või mõnes Euroopa Liidu detsentraliseeritud asutuses;

   e) nõuda, et asjaomased julgeolekuasutused algataksid uurimise, kui ilmneb, et Euroopa Liidu salastatud teabe leke on toimunud väljaspool peasekretariaati ja Euroopa Liidu detsentraliseeritud asutusi, ning koordineerida uurimist, kui uurimisega on seotud mitu julgeolekuasutust;

   f) koostöös ja kokkuleppel asjaomase siseriikliku julgeolekuasutusega kontrollida regulaarselt Euroopa Liidu salastatud teabe kaitsmise julgeolekukorraldust liikmesriikides;

   g) säilitada tihedaid sidemeid kõigi asjaomaste julgeolekuasutustega, et tagada julgeoleku üldine koordineerimine;

   h) jälgida pidevalt nõukogu julgeolekupõhimõtteid ja -korda ning koostada vajaduse korral asjakohaseid ettepanekuid. Seoses sellega esitab peasekretär/kõrge esindaja nõukogule peasekretariaadi julgeolekubüroo koostatud iga-aastase kontrollimiskava.

### Nõukogu julgeolekukomitee

3. Luuakse julgeolekukomitee. Kõnealune komitee koosneb kõigi liikmesriikide julgeolekuasutuste esindajatest. Komitee eesistuja on peasekretär/kõrge esindaja või tema esindaja. Kui arutatakse Euroopa Liidu detsentraliseeritud asutustega seotud küsimusi, võib komitee istungitele kutsuda ka nimetatud asutuste esindajad.

4. Julgeolekukomitee tuleb kokku nõukogu korraldusel peasekretäri/kõrge esindaja või liikmesriigi julgeolekuasutuse taotlusel. Komitee on volitatud kontrollima ja hindama kõiki nõukogu tegevusega seotud julgeolekuküsimusi ja tegema nõukogule vajaduse korral ettepanekuid. Seoses peasekretariaadi tegevusega on komitee volitatud tegema julgeolekuküsimustes soovitusi peasekretärile/kõrgele esindajale.

### Nõukogu peasekretariaadi julgeolekubüroo

5. Selleks et täita punktides 1 ja 2 nimetatud kohustusi, on peasekretäri/kõrge esindaja käsutuses julgeolekumeetmete koordineerimiseks, järelevalveks ja rakendamiseks peasekretariaadi julgeolekubüroo.

6. Peasekretariaadi julgeolekubüroo juhataja on peasekretäri/kõrge esindaja peamine nõustaja julgeolekuküsimustes ning ta tegutseb julgeolekukomitee sekretärina. Seoses sellega juhib ta julgeolekueeskirjade ajakohastamist ning koordineerib julgeolekumeetmeid liikmesriikide pädevate asutustega ja vajaduse korral ka rahvusvaheliste organisatsioonidega, mis on nõukoguga seotud julgeolekukokkulepete alusel. Sellisel juhul tegutseb ta kontaktametnikuna.

7. Peasekretariaadi julgeolekubüroo juhataja vastutab infotehnoloogiasüsteemide ja -võrkude akrediteerimise eest peasekretariaadis. Kui infotehnoloogiasüsteemid ja -võrgud hõlmavad peasekretariaati, liikmesriike, Euroopa Liidu detsentraliseeritud asutusi ja/või kolmandaid isikuid (riike või rahvusvahelisi organisatsioone), otsustavad peasekretariaadi julgeolekubüroo juhataja ja asjaomane liikmesriigi julgeolekuasutus vajaduse korral koos selliste süsteemide ja võrkude akrediteerimise.

**Euroopa Liidu detsentraliseeritud asutused**

8. Iga Euroopa Liidu detsentraliseeritud asutuse juht vastutab julgeolekueeskirjade rakendamise eest oma asutuses. Sellise asutuse juht nimetab tavaliselt ühe oma asutuse töötaja kõnealuses valdkonnas vastutavaks isikuks. See töötaja nimetatakse julgeolekuametnikuks.

**Liikmesriigid**

9. Iga liikmesriik peaks määrama siseriikliku julgeolekuasutuse, kes vastutab Euroopa Liidu salastatud teabe eest. [1]

10. Iga liikmesriigi valitsuse raames vastutab vastav siseriiklik julgeolekuasutus:

a) igasuguse avalik-õigusliku või eraomandis oleva siseriikliku talituse, organi ja asutuse valduses oleva Euroopa Liidu salastatud teabe julgeoleku tagamise eest nii kodu- kui ka välismaal;

b) kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluva teabe registrite loomise volituse eest (selle volituse võib anda edasi kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluva teabe keskregistri kontrolliametnikule);

c) Euroopa Liidu salastatud teabe kaitsmiseks võetud julgeolekukorra regulaarse läbivaatamise eest;

d) selle tagamise eest, et kõik siseriiklikes talitustes, organites ja asutustes töötavad kodanikud ja välismaalased läbivad julgeolekukontrolli, kui neil isikutel võib olla juurdepääs Euroopa Liidu salastatud teabele, mis kuulub kategooriasse TRÈS SECRET UE/EU TOP SECRET või CONFIDENTIEL UE;

e) selliste julgeolekukavade väljatöötamise eest, mida peetakse vajalikuks, et vältida Euroopa Liidu salastatud teabe sattumist selleks volitamata isikute kätte.

**Julgeoleku vastastikune kontrollimine**

11. Peasekretariaadi julgeolekubüroo ja asjaomane liikmesriigi julgeolekuasutus koos ja vastastikusel kokkuleppel kontrollivad perioodiliselt Euroopa Liidu salastatud teabe kaitseks võetud julgeolekumeetmeid peasekretariaadis ja liikmesriikide alalistes esindustes Euroopa Liidu juures ja nõukogu hoonetes asuvates liikmesriikide ruumides. [2]

12. Peasekretariaadi julgeolekubüroo või peasekretäri taotlusel vastuvõtva liikmesriigi siseriiklik julgeolekuasutus kontrollib perioodiliselt Euroopa Liidu detsentraliseeritud asutustes Euroopa Liidu salastatud teabe kaitseks võetud julgeolekumeetmeid.

---

[1] Euroopa Liidu salastatud teabe julgeoleku eest vastutavate liikmesriikide julgeolekuasutuste nimekiri on sätestatud liites 1.

[2] Ilma et see piiraks 1961. aasta diplomaatiliste suhete Viini konventsiooni sätteid.

II JAGU

## SALASTATUSE KATEGOORIAD JA TÄHISTUSED

SALASTATUSE KATEGOORIAD ([1])

Teave liigitatakse järgmistesse salastatuse kategooriatesse.

1. TRÈS SECRET UE/EU TOP SECRET: seda kategooriat kasutatakse ainult sellise teabe ja materjali puhul, mille loata avaldamine võib väga tõsiselt kahjustada Euroopa Liidu või ühe või mitme Euroopa Liidu liikmesriigi olulisi huve.

2. SECRET UE: seda kategooriat kasutatakse ainult sellise teabe ja materjali puhul, mille loata avaldamine võib tõsiselt kahjustada Euroopa Liidu või ühe või mitme Euroopa Liidu liikmesriigi olulisi huve.

3. CONFIDENTIEL UE: seda kategooriat kasutatakse sellise teabe ja materjali puhul, mille loata avaldamine võib kahjustada Euroopa Liidu või ühe või mitme Euroopa Liidu liikmesriigi olulisi huve.

4. RESTREINT UE: seda kategooriat kasutatakse sellise teabe ja materjali puhul, mille loata avaldamine võib negatiivselt mõjutada Euroopa Liidu või ühe või mitme Euroopa Liidu liikmesriigi huve.

TÄHISTUS

5. Dokumendis käsitletud valdkonna määratlemiseks või dokumendi levitamiseks ainult teadmisvajaduse põhjal võib kasutada hoiatustähist.

6. Tähistust ESDP/PESD kasutatakse dokumentidel ja nende koopiatel, kui neis käsitletakse Euroopa Liidu või ühe või mitme Euroopa Liidu liikmesriigi julgeolekut ja kaitset või sõjalise või mittesõjalise kriisi ohjamist.

7. Teatavad dokumendid, näiteks dokumendid, mis on seotud infotehnoloogiasüsteemidega, võib tähistada lisatähisega, mis viitab asjaomastes eeskirjades määratletud lisajulgeolekumeetmetele.

SALASTATUSE KATEGOORIATE JA TÄHISTUSTE KINNITAMINE

8. Salastatuse kategooriad ja tähistused kantakse dokumentidele järgmiselt:

   a) kategooriasse RESTREINT UE kuuluvatele dokumentidele mehaaniliste või elektrooniliste vahenditega;

   b) kategooriasse CONFIDENTIEL UE kuuluvatele dokumentidele mehaaniliste vahenditega ja käsitsi või trükkides eelnevalt templiga varustatud ja registreeritud paberile;

   c) kategooriatesse SECRET UE ja TRÈS SECRET UE/EU TOP SECRET kuuluvatele dokumentidele mehaaniliste vahenditega ja käsitsi.

([1]) Euroopa Liidu, NATO, Lääne-Euroopa Liidu ja liikmesriikide salastatuse tasemete võrdlev tabel on esitatud liites 2.

III JAGU

## SALASTATUSE KATEGOORIATE HALDAMINE

1. Teave salastatakse ainult siis, kui see on vajalik. Salastatuse kategooria peab olema selgelt ja täpselt märgitud ning see säilib seni, kuni teavet on vaja kaitsta.

2. Teabe salastatuse kategooria ja selle hilisema alandamise või kaotamise ([1]) eest vastutab ainult teabe looja.

   Peasekretariaadi ametnikud ja muud teenistujad määravad salastatuse kategooria, alandavad seda või kaotavad selle kas oma peadirektori juhtnööride kohaselt või kokkuleppel temaga.

3. Salastatud dokumentide käitlemise üksikasjalik kord on koostatud nii, et oleks tagatud selliste dokumentide kaitse neis sisalduva teabe kohaselt.

4. Nende inimeste arv, kellel on lubatud anda välja kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluvaid dokumente, peab olema nii väike kui võimalik ning nende kohta tuleb koostada nimekiri peasekretariaadis, igas liikmesriigis ja vajaduse korral ka igas Euroopa Liidu detsentraliseeritud asutuses.

### SALASTATUSE KATEGOORIATE RAKENDAMINE

5. Dokumendi salastatuse kategooria määratakse dokumendi sisu delikaatsuse põhjal, võttes arvesse II jao punktides 1–4 esitatud määratlust. Salastatuse kategooriaid tuleb kasutada korrektselt ja mõõdukalt. Eelkõige kehtib see salastatuse kategooria TRÈS SECRET UE/EU TOP SECRET puhul.

6. Salastatava dokumendi looja peab kinni eespool sätestatud eeskirjadest ega lase dokumendile anda liiga kõrget või liiga madalat salastatuse kategooriat.

   Kuigi esmapilgul võib tunduda, et kõrgem salastatuse kategooria tagab dokumendile ulatuslikuma kaitse, võib pidev liiga kõrgete salastatuse kategooriate määramine kaotada usalduse salastatuse kategoriseerimissüsteemi vastu.

   Teisest küljest ei tohiks dokumentide salastatuse kategooriad olla ka liiga madalad, et vältida kaitsmisega seotud piiranguid.

   Salastatuse kategooriate määramise praktiline juhend on esitatud liites 3.

7. Ühe dokumendi eri leheküljed, lõiked, jaotised, lisad, liited, manused ja täiendused võivad vajada eri salastatuse kategooriat ning need ka tähistatakse vastavalt. Kogu dokumendi salastatuse kategooria määratakse selle osa järgi, mille salastatuse kategooria on kõige kõrgem.

8. Kui dokumentidele on lisatud kiri või teade, määratakse selle salastatuse kategooria kindlaks selle dokumendi järgi, mille salastatuse kategooria on kõige rangem. Koostaja peab selgelt tähistama sellise kirja või teate salastatuse kategooria juhul, kui see lahutatakse lisatud dokumentidest.

### SALASTATUSE KATEGOORIA ALANDAMINE JA KAOTAMINE

9. Euroopa Liidu salastatud dokumentide salastatuse kategooriat võib alandada või sellise kategooria kaotada ainult dokumendi koostaja loal ja vajaduse korral pärast arutelu muude huvitatud pooltega. Salastatuse kategooria alandamist või kaotamist tuleb kinnitada kirjalikult. Dokumendi koostanud institutsioon, liikmesriik, büroo, õigusjärglane või kõrgem asutus vastutab selle eest, et dokumendi adressaate teavitatakse muudatustest, ning need adressaadid omakorda vastutavad selle eest, et muudatustest teavitatakse järgmisi adressaate, kellele nemad on saatnud kõnealuse dokumendi või selle koopia.

10. Võimaluse korral määravad dokumentide koostajad salastatud dokumentidele kuupäeva või ajavahemiku, mille jooksul võib salastatuse kategooriat alandada või selle kaotada. Kui see ei ole võimalik, vaatavad nad dokumendid hiljemalt iga viie aasta järel läbi, et teha kindlaks, kas esialgne salastatuse kategooria on endiselt vajalik.

---

([1]) Salastatuse kategooria alandamine *(déclassement)* tähendab salastatuse taseme alandamist; salastatuse kategooria kaotamine *(déclassification)* tähendab igasuguse salastatuse kõrvaldamist.

IV JAGU

**FÜÜSILINE JULGEOLEK**

ÜLDOSA

1. Füüsiliste julgeolekumeetmete peamine eesmärk on välistada vastava loata isikute juurdepääs Euroopa Liidu salastatud teabele ja/või materjalile.

JULGEOLEKUNÕUDED

2. Kõiki kohti, piirkondi, hooneid, büroosid, ruume, side- ja teabesüsteeme jms, kus säilitatakse ja käideldakse Euroopa Liidu salastatud teavet, kaitstakse asjakohaste füüsiliste julgeolekumeetmetega.

3. Vajaliku füüsilise julgeoleku ulatuse kindlaksmääramisel võetakse arvesse asjaomased tegurid, näiteks:

   a) teabe ja/või materjali salastatuse kategooria;

   b) olemasoleva teabe hulk ja vorm (näiteks trükitud või elektrooniliselt salvestatud);

   c) kohapeal antud hinnang ohule, mida näiteks sabotaaži, terrorismi ja muude õõnestavate ja/või kriminaalsete toimingute tõttu kujutavad endast luureteenistused, kelle töö on suunatud Euroopa Liidule, liikmesriikidele ja/või muudele institutsioonidele või kolmandatele isikutele, kelle valduses on Euroopa Liidu salastatud teavet.

4. Kohaldatavate füüsiliste julgeolekumeetmete eesmärk on:

   a) välistada salajane või jõuga sissetung;

   b) hoida ära, takistada ja avastada ebalojaalsete töötajate (sisespioonide) toimingud;

   c) välistada peasekretariaadi, liikmesriikide valitsusasutuse ja/või muude institutsioonide ja kolmandate isikute teadmisvajaduseta ametnike ja muude teenistujate juurdepääs Euroopa Liidu salastatud teabele.

FÜÜSILISED JULGEOLEKUMEETMED

**Turvaalad**

5. Alad, kus käideldakse ja hoitakse salastatuse kategooriasse CONFIDENTIEL UE või kõrgemasse kategooriasse kuuluvat teavet, tuleb korraldada ja üles ehitada nii, et need vastaksid ühele järgmistest:

   a) I klassi turvaala: ala, kus käideldakse või hoitakse salastatuse kategooriasse CONFIDENTIEL UE või kõrgemasse kategooriasse kuuluvat teavet ja kus alale sisenemine tähendab põhimõtteliselt juurdepääsu salastatud teabele. Sellise ala puhul on nõutavad:

      i) selgelt määratletud ja kaitstud piirid, millesse sisenemist ja millest väljumist alati kontrollitakse;

      ii) sisenemise kontrollsüsteem, mis võimaldab alale siseneda ainult neil isikutel, kes on läbinud julgeolekukontrolli ja kellel on selleks eriluba;

      iii) kõnealusel alal tavaliselt hoitava teabe salastatuse kategooria täpsustamine, st täpsustatakse teave, millele saadakse juurdepääs alale sisenemisega.

   b) II klassi turvaala: ala, kus käideldakse või hoitakse kategooriasse CONFIDENTIEL UE või kõrgemasse kategooriasse kuuluvat teavet nii, et seda on volitamata isikute juurdepääsu eest võimalik kaitsta sisekontrollivahendite abil, näiteks hoone, kus asuvad ruumid, kus pidevalt käideldakse kategooriasse CONFIDENTIEL UE või kõrgemasse kategooriasse kuuluvat teavet. Sellisel ala puhul on nõutavad:

      i) selgelt määratletud ja kaitstud piirid, millesse sisenemist ja millest väljumist alati kontrollitakse;

      ii) sisenemise kontrollsüsteem, mis võimaldab alale ilma saatjata siseneda ainult neil isikutel, kes on läbinud julgeolekukontrolli ja kellel on selleks eriluba. Kõigi teiste isikute puhul nähakse ette saatja või samaväärse kontrolli läbimine, et välistada loata juurdepääs Euroopa Liidu salastatud teabele ja kontrollimatu sissepääs aladele, kus kasutatakse tehnilist julgeolekukontrolli.

Alasid, kus töötajad ei viibi ööpäev läbi, kontrollitakse kohe pärast tavalise tööaja lõppu, et tagada Euroopa Liidu salastatud teabe nõuetekohane kaitstus.

**Haldustegevuse ala**

6. I ja II klassi turvaalade ümber või ees võib luua madalama julgeolekuga haldustegevuse ala. Sellise ala piir peab olema visuaalselt selgelt tähistatud, et oleks võimalik töötajaid ja sõidukeid kontrollida. Haldustegevuse aladel võib käidelda ja hoida ainult salastatuse kategooriasse RESTREINT UE kuuluvat teavet.

**Sisse- ja väljapääsu kontrollimine**

7. I ja II klassi turvaaladele sisenemist kontrollitakse läbipääsulubade abil või alaliste töötajate puhul isikutuvastussüsteemide abil. Loata juurdepääsu välistamiseks Euroopa Liidu salastatud teabele tuleb luua ka külastajate kontrollimise süsteem. Läbipääsulubade süsteemi võib täiendada automaattuvastusega, mida käsitatakse valvureid täiendava, kuid mitte neid asendava vahendina. Kui ohtude hinnangus toimub muudatusi, võib sellega kaasneda sisse- ja väljapääsu kontrollimise meetmete karmistamine näiteks silmapaistvate isikute külaskäigu ajal.

**Valvepatrullid**

8. Väljaspool tavapärast tööaega patrullitakse I ja II klassi turvaaladel, et kaitsta Euroopa Liidu varasid rikkumise, kahjustamise ja hävimise eest. Patrullimissagedus määratakse kindlaks kohalike asjaolude põhjal, kuid see võiks olla vähemalt kord kahe tunni jooksul.

**Turvakonteinerid ja turvakambrid**

9. Euroopa Liidu salastatud teabe säilitamiseks kasutatakse kolme liiki konteinereid:

— A klass: konteinerid, mis on salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluva teabe säilitamiseks I või II klassi turvaalal siseriiklikult heaks kiidetud,

— B klass: konteinerid, mis on salastatuse kategooriatesse SECRET UE ja CONFIDENTIEL UE kuuluva teabe säilitamiseks I või II klassi turvaalal siseriiklikult heaks kiidetud,

— C klass: kontorimööbel, mis sobib vaid salastatuse kategooriasse RESTREINT UE kuuluva teabe säilitamiseks.

10. Liikmesriigi julgeolekuasutus peab sertifitseerima I või II klassi turvaalale ehitatud turvakambrite ja kõigi selliste I klassi turvaalade, kus salastatuse kategooriasse CONFIDENTIEL UE või kõrgemasse salastatuse kategooriasse kuuluvat teavet säilitatakse lahtistel riiulitel või kus see on skeemidel, kaartidel vms välja pandud, seinad, põrandad ja laed ning lukkudega uksed ja kinnitama, et need pakuvad samaväärset kaitset kui samasse salastatuse kategooriasse kuuluva teabe säilitamiseks heaks kiidetud klassi turvakonteinerid.

**Lukud**

11. Euroopa Liidu salastatud teabe säilitamiseks kasutatavate turvakonteinerite ja turvakambrite lukud peavad vastama järgmistele standarditele:

— A rühm: siseriiklikult heaks kiidetud A klassi konteinerite jaoks,

— B rühm: siseriiklikult heaks kiidetud B klassi konteinerite jaoks,

— C rühm: sobib ainult C klassi kuuluva mööbli jaoks.

**Võtmete ja koodide järelevalve**

12. Turvakonteinerite võtmeid ei tohi büroohoonest välja viia. Isikud, kellel on vaja teada turvakonteinerite koode, peavad need pähe õppima. Hädaolukordadeks on asjaomase asutuse julgeolekuametniku vastutusel varuvõtmed ja kõigi koodide kirjalik register; koode hoitakse eraldi pitseeritud läbipaistmatutes ümbrikes. Võtmeid, varuvõtmeid ja koode hoitakse eraldi turvakonteinerites. Kõnealuste võtmete ja koodide kaitse peaks olema sama range kui materjali kaitse, millele nendega on võimalik juurde pääseda.

13. Turvakonteinerite koode teadvate inimeste arv peab olema võimalikult väike. Koode muudetakse:

a) uue konteineri saabumisel;

b) iga personalimuutuse korral;

c) iga kord, kui on toimunud julgeoleku rikkumine või kui seda kahtlustatakse;

d) soovitatavalt iga kuue kuu järel ja vähemalt iga 12 kuu järel.

**Sissetungimise avastamise seadmed**

14. Kui Euroopa Liidu salastatud teabe kaitsmiseks kasutatakse alarmsüsteeme, valvekaameraid ja muid elektrilisi seadmeid, tuleb kasutada tagavaravooluallikat, mis tagaks süsteemi töötamise ka siis, kui voolu saamine peavooluallikast katkeb. Peale selle on oluline, et selliste süsteemide riketest või nende töö segamisest antaks valvetöötajatele teada häire või muu usaldusväärse hoiatusega.

**Heakskiidetud seadmed**

15. Liikmesriikide julgeolekuasutused haldavad kas omal jõul või kahepoolselt ajakohastatud nimekirju turvavarustuse tüüpide ja mudelite kohta, mille nad on heaks kiitnud salastatud teabe otseseks või kaudseks kaitsmiseks mitmesuguste kindlaksmääratud asjaolude ja tingimuste korral. Peasekretariaadi julgeolekubüroo haldab samalaadset nimekirja, mis põhineb muu hulgas liikmesriikide julgeolekuasutustelt saadud teabel. Euroopa Liidu detsentraliseeritud asutused konsulteerivad enne sellise varustuse ostmist peasekretariaadi julgeolekubürooga ja vajaduse korral vastuvõtva liikmesriigi julgeolekuasutusega.

**Koopiamasinate ja faksiseadmete füüsiline kaitse**

16. Koopiamasinaid ja faksiseadmeid kaitstakse füüsiliselt sellises ulatuses, nagu on vaja tagamaks, et neid võivad kasutada ainult selleks volitatud isikud ja et kõiki salastatud tooteid kontrollitakse nõuetekohaselt.

KAITSE SALAJASE JÄLGIMISE JA PEALTKUULAMISE EEST

**Salajane jälgimine**

17. Nii päeval kui ka öösel võetakse kõik vajalikud meetmed tagamaks, et selleks volitamata isikud ei näe Euroopa Liidu salastatud teavet ka mitte juhuslikult.

**Pealtkuulamine**

18. Kui esineb selline oht, tuleb ametiruume ja alasid, kus regulaarselt arutletakse salastatuse kategooriasse SECRET UE või kõrgemasse kategooriasse kuuluva teabe üle, kaitsta nii tahtliku kui ka tahtmatu pealtkuulamise eest. Sellise pealtkuulamise ohu hindamise eest vastutab pädev julgeolekuasutus, kes võib vajaduse korral enne konsulteerida liikmesriikide julgeolekuasutustega.

19. Tahtmatu pealtkuulamise vastu võetavate kaitsemeetmete (näiteks seinte, uste, põrandate ja lagede heliisolatsioon, paljastava kiirguse mõõtmine) ja tahtliku pealtkuulamise vastu võetavate kaitsemeetmete (näiteks mikrofonide otsimine) kindlaksmääramiseks võib peasekretariaadi julgeolekubüroo nõuda liikmesriikide julgeolekuasutuste abi. Euroopa Liidu detsentraliseeritud asutuste julgeolekuametnikud võivad paluda peasekretariaadi julgeolekubüroolt tehnilist kontrollimist ja/või liikmesriigi julgeolekuasutuste ekspertide abi.

20. Samuti võivad liikmesriigi julgeolekuasutuse tehnilise julgeoleku spetsialistid pädeva julgeolekuametniku taotluse põhjal vajaduse korral kontrollida kõiki sideseadmeid ja elektrilisi või elektroonilisi bürooseadmeid, mida kasutatakse salastatuse kategooriasse SECRET UE või kõrgemasse salastatuse kategooriasse kuuluvatel koosolekutel.

TEHNILISELT KAITSTUD ALAD

21. Teatavad alad võib määrata tehniliselt kaitstud aladeks. Neile aladele sisenemisel läbitakse erikontroll. Kui sellistel aladel ei ole inimesi, on need alad heakskiidetud viisil lukustatud ning kõiki võtmeid käsitatakse turvavõtmetena. Sellistel aladel toimub regulaarselt füüsiline kontroll, mis võetakse ette ka iga loata sisenemise või sellise sisenemise kahtluse järel.

22. Seadmete ja mööbli üle peetakse üksikasjalikku arvestust, et jälgida nende asukoha muutust. Sellisele alale ei tohi tuua ühtegi mööblieset ega seadet enne, kui erikoolitusega julgeolekutöötaja on selle hoolikalt üle kontrollinud, et tuvastada võimalike pealtkuulamisvahendite olemasolu. Üldjuhul tuleks vältida sideliinide paigaldamist tehniliselt kaitstud aladele.

V JAGU

## TEADMISVAJADUSE PÕHIMÕTTE JA JULGEOLEKUKONTROLLI KOHALDAMISE ÜLDEESKIRJAD

1. Luba pääseda juurde Euroopa Liidu salastatud teabele antakse ainult neile isikutele, kellel on teadmisvajadus seoses oma ülesannete ja kohustuste täitmisega. Luba pääseda juurde salastatuse kategooriatesse TRÈS SECRET UE/EU TOP SECRET, SECRET UE ja CONFIDENTIEL UE kuuluvale teabele antakse ainult isikutele, kes on läbinud nõuetekohase julgeolekukontrolli.

2. Teadmisvajaduse teeb kindlaks peasekretariaat, Euroopa Liidu detsentraliseeritud asutus või liikmesriigi üksus või talitus, kus asjaomane isik töötab, võttes arvesse ülesannetega seotud nõudeid.

3. Töötajate julgeolekukontrolli eest asjaomase korra kohaselt vastutab ametniku tööandja. Peasekretariaadi ametnike ja muude teenistujate julgeolekukontrolli kord on sätestatud VI jaos.

   Pärast julgeolekukontrolli läbimist antakse välja "julgeolekusertifikaat", millel on kirjas, millisesse salastatuse kategooriasse kuuluvale teabele on asjaomasel isikul juurdepääs, ja sertifikaadi kehtivusaeg.

   Kui julgeolekusertifikaat annab loa juurdepääsuks teatavasse salastatuse kategooriasse kuuluvale teabele, on sertifikaadi valdajal õigus juurdepääsuks ka madalamasse salastatuse kategooriasse kuuluvale teabele.

4. Kui isikud, kellega tuleb Euroopa Liidu salastatud teabe üle aru pidada või kellele tuleb sellist teavet näidata, ei ole peasekretariaadi ega liikmesriikide ametnikud ega muud teenistujad (vaid näiteks Euroopa Liidu institutsioonide liikmed, ametnikud või teenistujad), peavad nad läbima julgeolekukontrolli seoses Euroopa Liidu salastatud teabega ning neile tuleb tutvustada nende julgeolekuga seotud vastutust. Samasuguste tingimuste korral kohaldatakse seda reeglit ka väljastpoolt pärit tööettevõtjate, ekspertide ja konsultantide suhtes.

### ERIEESKIRJAD JUURDEPÄÄSUKS SALASTATUSE KATEGOORIASSE TRÈS SECRET UE/EU TOP SECRET KUULUVALE TEABELE

5. Kõik isikud, kes soovivad juurdepääsu salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluvale teabele, peavad juurdepääsu saamiseks sellisele teabele kõigepealt läbima julgeolekukontrolli.

6. Kõik isikud, kellel on vaja juurdepääsu salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluvale teabele, määrab nende osakonna juhataja ning nende nimed kantakse asjaomasesse salastatuse kategooria TRÈS SECRET UE/EU TOP SECRET registrisse.

7. Enne juurdepääsu saamist salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluvale teabele kirjutavad kõik isikud alla tunnistusele selle kohta, et neile on tutvustatud nõukogu julgeolekukorda ning nad mõistavad täielikult oma kohustust kaitsta salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluvat teavet ja tagajärgi, mis on Euroopa Liidu eeskirjade ja siseriiklike õigusaktidega ette nähtud juhuks, kui salastatud teave satub kas tahtlikult või hooletuse tõttu volitamata isikute kätte.

8. Kui isikutel on juurdepääs salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluvale teabele koosolekutel või muudel sellistel üritustel, teavitab selle üksuse või organi pädev kontrolliametnik, kus kõnealused isikud töötavad, koosoleku korraldajat sellest, et asjaomastel isikutel on luba juurdepääsuks sellisele teabele.

9. Kui isiku töökohustused ei eelda enam juurdepääsu salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluvale teabele, kustutatakse kõnealuse isiku nimi salastatuse kategooria TRÈS SECRET UE/EU TOP SECRET nimekirjast. Lisaks juhitakse selliste isikute tähelepanu veel kord nende erikohustustele seoses salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluva teabe kaitsmisega. Sellised isikud kirjutavad alla deklaratsioonile selle kohta, et nad ei kasuta ega edasta nende käsutuses olnud teavet, mis kuulub salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET.

ERIEESKIRJAD JUURDEPÄÄSUKS SALASTATUSE KATEGOORIATESSE SECRET UE JA CONFIDENTIEL UE KUULUVALE TEABELE

10. Kõik isikud, kes soovivad juurdepääsu salastatuse kategooriasse SECRET UE või CONFIDENTIEL UE kuuluvale teabele, peavad kõigepealt läbima vastava taseme julgeolekukontrolli.

11. Kõigile isikutele, kellele antakse juurdepääs salastatuse kategooriasse SECRET UE või CONFIDENTIEL UE kuuluvale teabele, tutvustatakse asjakohaseid julgeolekueeskirju ja nad peavad olema kursis nende rikkumise tagajärgedega.

12. Kui isikutel on juurdepääs salastatuse kategooriasse SECRET UE või CONFIDENTIEL UE kuuluvale teabele koosolekutel või muudel sellistel üritustel, teavitab selle organi julgeolekuametnik, kus kõnealune isik töötab, koosoleku korraldajat sellest, et asjaomastel isikutel on luba juurdepääsuks sellisele teabele.

ERIEESKIRJAD JUURDEPÄÄSUKS SALASTATUSE KATEGOORIASSE RESTREINT UE KUULUVALE TEABELE

13. Kõigile isikutele, kellel on juurdepääs salastatuse kategooriasse RESTREINT UE kuuluvale teabele, tutvustatakse käesolevaid julgeolekueeskirju ja nende rikkumise tagajärgi.

ÜLEANDMINE

14. Kui töötaja lahkub töökohalt, kus tema tegevus hõlmas Euroopa Liidu salastatud teabe käitlemist, jälgib registripidaja kõnealuse materjali nõuetekohast üleandmist lahkuvalt ametnikult saabuvale ametnikule.

ERIJUHENDID

15. Isikuid, kes peavad käitlema Euroopa Liidu salastatud teavet, tuleks kõigepealt tööülesannete täitmisele asumisel ja pärast seda regulaarselt teavitada järgmisest:

    a) ebadiskreetsetest vestlustest tulenev oht julgeolekule;

    b) ettevaatusabinõud, mida tuleb järgida suheldes ajakirjandusega;

    c) oht, mida kujutavad endast luureteenistuste Euroopa Liidule ja selle liikmesriikidele suunatud toimingud seoses Euroopa Liidu salastatud teabe ja toimingutega;

    d) kohustus teatada viivitamata asjaomasele julgeolekuasutusele kõigist lähenemistest või teguviisidest, mis võivad anda alust kahtlustada spionaaži, ja muudest ebatavalistest julgeolekuga seotud asjaoludest.

16. Kui isikud puutuvad sageli kokku selliste riikide esindajatega, mille luureteenistuste tegevus võib olla suunatud Euroopa Liidu ja liikmesriikide vastu seoses Euroopa Liidu salastatud teabe ja toimingutega, tutvustatakse neile lühidalt eri luureteenistustes teadaolevalt kasutatavat tehnikat.

17. Nõukogul ei ole julgeolekueeskirju Euroopa Liidu salastatud teabele juurdepääsu omavate isikute erareiside kohta olenemata sellise reisi sihtkohast. Pädevad julgeolekuasutused tutvustavad oma vastutusalasse kuuluvatele ametnikele ja muudele teenistujatele siiski neid eeskirju, mida nende suhtes võidakse reisimisel kohaldada. Julgeolekuametnikud korraldavad töötajatele koosolekuid selliste erijuhendite meeldetuletamiseks.

VI JAGU

**PEASEKRETARIAADI AMETNIKE JA MUUDE TEENISTUJATE JULGEOLEKUKONTROLLI KORD**

1. Juurdepääs nõukogu valduses olevale salastatud teabele antakse ainult sellistele peasekretariaadi ametnikele ja muudele teenistujatele või muudele peasekretariaadis töötavatele isikutele, kes oma ülesannete või oma teenistusnõuete tõttu peavad sellist teavet teadma või kasutama.

2. Juurdepääsuks salastatuse kategooriatesse TRÈS SECRET UE/EU TOP SECRET, SECRET UE ja CONFIDENTIEL UE kuuluvale teabele peavad lõikes 1 osutatud isikud saama loa punktides 4 ja 5 osutatud korra kohaselt.

3. Luba antakse ainult isikutele, kes on läbinud liikmesriigi pädeva julgeolekuasutuse julgeolekukontrolli punktides 6-10 osutatud korra kohaselt.

4. Punktides 1, 2 ja 3 nimetatud lubade andmise eest vastutab ametisse nimetav asutus või ametiisik personalieeskirjade artikli 2 esimese lõigus määratletud tähenduses.

   Ametisse nimetav asutus või ametiisik annab loa pärast seda, kui on saanud punktides 6-10 osutatud korra kohaselt tehtud julgeolekukontrolli põhjal liikmesriigi pädeva julgeolekuasutuse koostatud seisukoha.

5. Luba, mille kehtivusaeg on viis aastat, ei tohi kehtida kauem kui tööülesanne, mille põhjal luba anti. Ametisse nimetav asutus või ametiisik võib kehtivusaega pikendada punktis 4 osutatud korra kohaselt.

   Ametisse nimetav asutus või ametiisik võib loa tühistada, kui ta leiab, et see on põhjendatud. Loa tühistamise otsusest teatatakse asjaomasele isikule, kes võib esitada oma selgitused ametisse nimetavale asutusele või ametiisikule ja pädevale siseriiklikule asutusele.

6. Julgeolekukontrolliga tuleks teha kindlaks, et ei ole vastuväiteid, mille tõttu ei tohiks anda asjaomasele isikule juurdepääsu nõukogu valduses olevale salastatud teabele.

7. Julgeolekukontroll toimub koostöös asjaomase isikuga ja ametisse nimetava asutuse või ametiisiku taotlusel ning selle teostab selle liikmesriigi pädev siseriiklik asutus, mille kodanik luba taotlev isik on. Kui asjaomane isik elab teise liikmesriigi territooriumil, võib kõnealune siseriiklik asutus teha koostööd isiku elukohajärgse riigi asutustega.

8. Julgeolekukontrolli raames peab asjaomane isik täitma isikliku infolehe.

9. Ametisse nimetav asutus või ametiisik täpsustab oma taotluses, millist liiki ja millise salastatuse tasemega teabe võib asjaomasele isikule kättesaadavaks teha, et pädev siseriiklik asutus saaks teostada julgeolekukontrolli ja esitada oma seisukoha seoses kõnealusele isikule antava loa tasemega.

10. Kogu julgeolekukontrolli protsessi suhtes, kaasa arvatud selle tulemused, kohaldatakse kõnealuses liikmesriigis kehtivaid asjaomaseid õigusnorme, sealhulgas kaebusi käsitlevaid õigusnorme.

11. Kui liikmesriigi pädevate asutuste seisukoht on positiivne, võib ametisse nimetav asutus või ametiisik anda kõnealusele isikule loa.

12. Pädeva siseriikliku asutuse negatiivsest seisukohast teatatakse asjaomasele isikule, kes võib paluda, et ametisse nimetav asutus või ametiisik kuulaks ära tema selgitused. Kui ametisse nimetav asutus või ametiisik peab seda vajalikuks, võib ta paluda, et pädevad siseriiklikud asutused annaksid oma võimete piires täiendavaid selgitusi. Kui kinnitatakse negatiivset seisukohta, siis luba ei anta.

13. Kõigile isikutele, kellele antakse punktides 4 ja 5 osutatud luba, antakse loa väljaandmisel ja pärast seda regulaarsete ajavahemike järel vajalikud juhtnöörid salastatud teabe kaitsmise ja sellise kaitse tagamise vahendite kohta. Sellised isikud kirjutavad alla deklaratsioonile, milles nad kinnitavad, et on saanud juhtnöörid ja kohustuvad neid järgima.

14. Ametisse nimetav asutus või ametiisik võtab käesoleva jao rakendamiseks kõik vajalikud meetmed, eelkõige seoses eeskirjadega, mis reguleerivad juurdepääsu loa saanud isikute nimekirjale.

15. Erandkorras, kui teenistus seda eeldab, võib ametisse nimetav asutus või ametiisik pärast pädevatele siseriiklikele asutustele teatamist ja tingimusel, et nimetatud asutused ei ole selle teatise kohta kuu aja jooksul märkusi teinud, anda enne punktis 7 osutatud julgeolekukontrolli tulemuste selgumist kuni kuueks kuuks ajutise loa.

16. Niiviisi antud ajutised load ei anna juurdepääsu salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluvale teabele; juurdepääs nimetatud kategooriasse kuuluvale teabele antakse ainult ametnikele, kes on positiivsete tulemustega läbinud julgeolekukontrolli punkti 7 kohaselt. Kuni julgeolekukontrolli tulemuste selgumiseni võib ametnikele, kes peavad julgeolekukontrolli läbima salastatuse kategooria TRÈS SECRET UE/EU TOP SECRET jaoks, anda ajutise loa juurdepääsuks teabele, mis kuulub salastatuse kategooriasse SECRET UE või madalamatesse kategooriatesse.

VII JAGU

# EUROOPA LIIDU SALASTATUD MATERJALI ETTEVALMISTAMINE, LEVITAMINE, EDASTAMINE, SÄILITAMINE JA HÄVITAMINE

## Sisukord

**Üldsätted**

Käesolevas jaos sätestatakse üksikasjalikud meetmed käesoleva lisa I osas sätestatud julgeoleku üldpõhimõtete ja miinimumnõuete punkti 3 alapunktis a määratletud Euroopa Liidu salastatud dokumentide ettevalmistamiseks, levitamiseks, edastamiseks, säilitamiseks ja hävitamiseks. Käesolevas jaos sätestatut kasutatakse baasina kõnealuste meetmete kohandamisel muude Euroopa Liidu salastatud materjalide jaoks vastavalt sellise materjali liigile ja igal üksikjuhul eraldi.

*I peatükk*

**Euroopa Liidu salastatud dokumentide ettevalmistamine ja levitamine**

ETTEVALMISTAMINE

1. Euroopa Liidu salastatuse kategooriaid ja nende tähistusi kasutatakse II jao sätete kohaselt ja need peavad olema iga lehe keskel ülemises ja alumises servas ning kõik lehed peavad olema nummerdatud. Igale Euroopa Liidu salastatud dokumendile peab olema märgitud viitenumber ja kuupäev. Kui tegemist on salastatuse kategooriatesse TRÈS SECRET UE/EU TOP SECRET ja SECRET UE kuuluvate dokumentidega, peab kõnealune viitenumber olema märgitud igale lehele. Kui dokumente levitatakse mitme koopiana, peab iga koopia esilehele olema märgitud koopia number ja dokumendi lehekülgede arv. Kui tegemist on salastatuse kategooriasse CONFIDENTIEL UE või rangemasse kategooriasse kuuluva dokumendiga, peab dokumendi esimesel lehel olema nimekiri kõigi lisade ja lisatud dokumentide kohta.

2. Kui tegemist ei ole käesoleva jao punktis 27 kirjeldatud erandjuhtumiga, võivad salastatuse kategooriasse CONFIDENTIEL UE või kõrgemasse kategooriasse kuuluvaid dokumente trükkida, tõlkida, säilitada, neist koopiaid teha, neid magnetkujul paljundada või neist mikrofilme teha ainult isikud, kes on läbinud julgeolekukontrolli seoses juurdepääsuga vähemalt sellesse salastatuse kategooriasse kuuluvatele dokumentidele, kuhu kuulub asjaomane dokument.

   Sätted, mis reguleerivad salastatud dokumentide koostamist arvutiga, on ette nähtud XI jaos.

LEVITAMINE

3. Euroopa Liidu salastatud teavet levitatakse ainult isikutele, kellel on vastav teadmisvajadus ja kes on läbinud asjakohase julgeolekukontrolli. Dokumendi esialgse levitamise täpsustab dokumendi koostaja.

4. Salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluvaid dokumente levitatakse salastatuse kategooria TRÈS SECRET UE/EU TOP SECRET registri kaudu (vt VIII jagu). Kui tegemist on salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluvate sõnumitega, võib pädev register volitada sidekeskuse juhatajat tegema adressaatide loetelus märgitud hulga koopiaid.

5. Esialgne adressaat võib salastatuse kategooriasse SECRET UE ja madalamatesse salastatuse kategooriatesse kuuluvaid dokumente edastada teistele adressaatidele teadmisvajaduse põhjal. Dokumendi koostanud asutus või ametiisik annab siiski selgelt teada kõigist piirangutest, mida ta soovib kohaldada. Selliste piirangute kehtestamise korral võivad adressaadid dokumente edasi levitada ainult dokumendi koostanud asutuse või ametiisiku loal.

6. Kõik dokumendid, mis kuuluvad salastatuse kategooriasse CONFIDENTIEL UE või kõrgemasse salastatuse kategooriasse, kantakse üksusesse saabumisel ja sealt lahkumisel asutuse registrisse. Registrisse kantavad andmed (viitenumber, kuupäev ja vajaduse korral koopia number) peavad võimaldama dokumente kindlaks teha ning need tuleb kanda logiraamatusse või spetsiaalsele kaitstud andmekandjale.

*II peatükk*

**Euroopa Liidu salastatud teabe edastamine**

PAKENDAMINE

7. Salastatuse kategooriasse CONFIDENTIEL UE või kõrgemasse salastatuse kategooriasse kuuluvaid dokumente edastatakse tugevates ja läbipaistmatutes kahekordsetes ümbrikes. Sisemisele ümbrikule märgitakse vajalik Euroopa Liidu salastatuse kategooria ning võimaluse korral saaja täielik ametinimetus ja aadress.

8. Kui ümbrik ei ole adresseeritud konkreetsele isikule, võib sisemise ümbriku avada ja selles olevate dokumentide vastuvõtmist kinnitada ainult registri kontrolliametnik. Kui ümbrik on adresseeritud konkreetsele isikule, märgitakse asjaomases registris ümbriku saabumine logiraamatusse ning sisemise ümbriku võib avada ja selles olevate dokumentide vastuvõtmist kinnitada vaid isik, kellele see on adresseeritud.

9. Sisemisse ümbrikusse tuleb panna kättesaamistõendi vorm. Kättesaamistõend ei ole salastatud ning sellele peaks olema märgitud dokumendi viitenumber, kuupäev ja koopia number, kuid sellele ei tohi kunagi kirjutada dokumendis käsitletavat teemat.

10. Sisemine ümbrik pannakse välimisse ümbrikusse, millel on kättesaamiskinnituse jaoks kirjas paki number. Mingil juhul ei tohi välimisele ümbrikule märkida salastatuse kategooriat.

11. Salastatuse kategooriasse CONFIDENTIEL UE ja kõrgematesse kategooriatesse kuuluvate dokumentide puhul antakse kullerile või virgatsile paki numbri vastu kättesaamistõend.

EDASTAMINE ÜHE HOONE VÕI HOONERÜHMA PIIRES

12. Ühe hoone või hoonerühma piires võib salastatud dokumente transportida pitseeritud ümbrikus, millel on kirjas ainult adressaadi nimi, kui sellist ümbrikut transpordib isik, kes on läbinud julgeolekukontrolli seoses vastava kategooria salastatud dokumentidega.

EUROOPA LIIDU DOKUMENTIDE EDASTAMINE ÜHE RIIGI PIIRES

13. Ühe riigi piires tuleks salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluvaid dokumente saata ainult ametliku kullerteenuse vahendusel või isikutega, kellel on luba juurdepääsuks salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluvatele dokumentidele.

14. Kui salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluvate dokumentide edastamiseks väljapoole ühe hoone või hoonerühma piire kasutatakse kullerteenust, tuleb täita käesolevas peatükis sisalduvaid sätteid pakendamise ja kättesaamistõendite kohta. Kättetoimetamisüksustel peab olema piisavalt töötajaid tagamaks, et salastatuse kategooriasse kuuluvaid dokumente sisaldavad pakid on kogu aeg vastutava ametniku otsese järelevalve all.

15. Erandkorras võivad ametnikud, kes ei ole kullerid, viia salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluvaid dokumente hoonest või hoonerühmast välja, et neid kasutada kohalikul koosolekul või arutelul, kui:

    a) dokumentide kandjal on luba juurdepääsuks kõnealustele salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluvatele dokumentidele;

    b) transpordiliik vastab siseriiklikele eeskirjadele, mis reguleerivad siseriiklike ülisalajaste dokumentide edastamist;

    c) ametnik ei jäta salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluvaid dokumente mingil juhul järelevalveta;

    d) nähakse ette kord sel viisil edastatavate dokumentide loetelu andmiseks salastatuse kategooria registrisse, kus nimetatud dokumente hoitakse, ja nende dokumentide kontrollimiseks nimetatud loetelu alusel pärast tagasitoomist.

16. Ühe riigi piires võib salastatuse kategooriatesse SECRET UE ja CONFIDENTIEL UE kuuluvaid dokumente saata kas postiga, kui selline edastamisviis on siseriiklike õigusnormidega lubatud ja vastab nende õigusnormide sätetele, või selliste kullerteenistuste või isikute kaudu, kes on läbinud julgeolekukontrolli seoses juurdepääsuga Euroopa Liidu salastatud teabele.

17. Iga liikmesriik või Euroopa Liidu detsentraliseeritud asutus peaks koostama juhtnöörid isikutele, kes transpordivad Euroopa Liidu salastatud teavet sisaldavaid dokumente kõnealuste õigusnormide põhjal. Dokumentide transportijad peaksid sellised juhtnöörid läbi lugema ja neile alla kirjutama. Eelkõige tuleks sellistes juhtnöörides sätestada, et mingil juhul ei või:

    a) dokumendid lahkuda nende vedaja valdusest, kui nad ei ole turvaliselt hoiule antud IV jao sätete kohaselt;

    b) jätta dokumente järelevalveta ühissõidukis või eraautos või sellistes kohtades nagu restoranid ja hotellid. Selliseid dokumente ei tohi hoida hotelli seifis ega jätta järelevalveta hotellituppa;

    c) lugeda avalikus kohas, näiteks õhusõidukis või rongis.

EDASTAMINE ÜHEST LIIKMESRIIGIST TEISE

18. Salastatuse kategooriasse CONFIDENTIEL UE ja kõrgemasse salastatuse kategooriasse kuuluvat materjali võib ühest liikmesriigist teise toimetada ainult diplomaatilise või sõjalise kullerteenistuse abil.

19. Salastatuse kategooriatesse SECRET UE ja CONFIDENTIEL UE kuuluva materjali isiklikku transportimist võib lubada, kui transporti käsitlevad sätted tagavad, et selline materjal ei või sattuda volitamata isikute kätte.

20. Liikmesriigi julgeolekuasutus võib lubada isikutel materjali transportida, kui diplomaatilise või sõjalise kullerteenistuse abi ei ole võimalik kasutada või kui selliste kullerteenistuste kasutamine tooks kaasa viivituse, mis kahjustaks Euroopa Liidu toiminguid, ning kui kavandatud adressaadil on kõnealust materjali kiiresti vaja. Iga liikmesriik peaks koostama juhtnöörid, mis käsitlevad salastatuse kategooriasse SECRET UE või madalamasse kategooriasse kuuluva materjali rahvusvahelist transportimist isikute poolt, kes ei tööta diplomaatilises ega sõjalises kullerteenistuses. Sellistes juhtnöörides tuleb sätestada järgmised nõuded:

a) materjali transportijal on liikmesriigi väljastatud asjakohane julgeolekusertifikaat;

b) kõigi sel viisil transporditavate materjalide kohta peetakse arvet asjaomases büroos või registris;

c) Euroopa Liidu materjale sisaldavad pakid või kotid peavad olema varustatud ametliku pitseriga, et välistada või piirata nende läbivaatamist tollis, ning tunnussiltide ja juhtnööridega paki või koti leidjale;

d) materjali transportijal on kõigis Euroopa Liidu liikmesriikides tunnustatud kulleritunnistus ja/või töökäsk, mis lubavad tal nõuetekohaselt tähistatud pakki transportida;

e) maismaal reisides ei tohi läbida kolmandaid riike ega ületada nende riikide piire, kui materjali saatev riik ei ole saanud asjaomaselt kolmandalt riigilt konkreetset garantiid;

f) materjali transportija reisimine peab sihtkoha, läbitava marsruudi ja kasutatavate transpordivahendite poolest vastama Euroopa Liidu õigusnormidele või kui siseriiklikud õigusnormid on sellises küsimuses rangemad, siis neile õigusnormidele;

g) materjal peab olema kogu aeg selle transportija valduses, kuni see antakse hoiule IV jao turvalist säilitamist käsitlevate sätete kohaselt;

h) materjali ei tohi jätta järelevalveta ühissõidukis või eraautos või sellistes kohtades nagu restoranid ja hotellid. Sellist materjali ei tohi hoida hotelli seifis ega jätta järelevalveta hotellituppa;

i) kui transporditava materjali hulka kuuluvad ka dokumendid, ei tohi neid lugeda avalikus kohas (näiteks lennukis, rongis jms sellises kohas).

Salastatud materjali transportiv isik peab läbi lugema ja allkirjastama julgeolekujuhendid, mis sisaldavad vähemalt eespool loetletud juhtnööre ja korda, mida tuleb järgida hädaolukorras või juhul, kui toll või lennujaama julgeolekuametnikud soovivad kontrollida salastatud materjali sisaldavat pakki.

SALASTATUSE KATEGOORIASSE RESTREINT UE KUULUVATE DOKUMENTIDE EDASTAMINE

21. Salastatuse kategooriasse RESTREINT UE kuuluvate dokumentide edasitoimetamiseks ei nähta ette erisätteid, kuid nende dokumentide edasitoimetamisel tuleks tagada, et nad ei satu volitamata isikute kätte.

KULLERTEENISTUSTE TÖÖTAJATE JULGEOLEK

22. Kui virgatsit või kullerit kavatsetakse kasutada salastatuse kategooriatesse SECRET UE ja CONFIDENTIEL UE kuuluvate dokumentide vedamiseks, peab ta läbima nõuetekohase julgeolekukontrolli.

*III peatükk*

**Elektrilised ja muud tehnilised edastusvahendid**

23. Sideturbe julgeolekumeetmete eesmärk on tagada Euroopa Liidu salastatud teabe turvaline edastamine. Sellise Euroopa Liidu salastatud teabe edastamise üksikasjalikke eeskirju käsitletakse XI jaos.

24. Salastatuse kategooriatesse CONFIDENTIEL UE ja SECRET UE kuuluvat teavet võib edastada ainult akrediteeritud sidekeskuste, -võrkude ja/või -terminalide ja -süsteemide kaudu.

*IV peatükk*

**Euroopa Liidu salastatud teabe täiendavad koopiad ja tõlked ning väljavõtted sellistest dokumentidest**

25. Salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluvatest dokumentidest võib teha koopiaid või selliseid dokumente tõlkida ainult dokumendi koostaja loal.

26. Kui isik, kes ei ole läbinud julgeolekukontrolli salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluva teabe jaoks, vajab teavet, mis sisaldub salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluvas dokumendis, kuid ei kuulu nimetatud salastatuse kategooriasse, võib salastatuse kategooria TRÈS SECRET UE/EU TOP SECRET registri juhataja anda loa teha kõnealusest dokumendist vajaliku hulga väljavõtteid. Samal ajal võtab asjaomase registri juhataja vajalikud meetmed tagamaks, et nimetatud väljavõtetele antakse asjakohane salastatuse tase.

27. Adressaat võib salastatuse kategooriasse SECRET UE või madalamasse kategooriasse kuuluvaid dokumente paljundada või tõlkida siseriiklike julgeolekueeskirjade kohaselt ja tingimusel, et selline tegevus on rangelt kooskõlas teadmisvajaduse põhimõttega. Esialgse dokumendi suhtes rakendatavaid julgeolekumeetmeid rakendatakse ka selle dokumendi paljunduste ja/või tõlgete suhtes. Euroopa Liidu detsentraliseeritud asutused järgivad käesolevaid julgeolekueeskirju.

*V peatükk*

**Euroopa Liidu salastatud teabe inventeerimine ja kontrollimine, säilitamine ja hävitamine**

INVENTEERIMINE JA KONTROLLIMINE

28. Igal aastal teeb VIII jaos nimetatud salastatuse kategooria TRÈS SECRET UE/EU TOP SECRET register salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluvate dokumentide üksikasjaliku inventuuri VIII jao punktides 9-11 sätestatud eeskirjade kohaselt. Kui Euroopa Liidu salastatud dokumentide salastatuse kategooria on madalam kui TRÈS SECRET UE/EU TOP SECRET, tehakse nende üle sisekontroll siseriiklike suuniste kohaselt ning peasekretariaadi ja Euroopa Liidu detsentraliseeritud asutuste puhul peasekretäri/kõrge esindaja juhtnööride kohaselt.

Selliste toimingute käigus võiva salastatud teabe valdajad võtta seisukoha:

a) teatavate dokumentide salastatuse kategooria alandamise või kaotamise kohta;

b) dokumentide hävitamise kohta.

EUROOPA LIIDU SALASTATUD TEABE SÄILITAMINE ARHIIVIDES

29. Säilitamisega seotud probleemide minimeerimiseks on kõigi registrite kontrolliametnikel luba kanda salastatuse kategooriatesse TRÈS SECRET UE/EU TOP SECRET, SECRET UE ja CONFIDENTIEL UE kuuluvad dokumendid mikrofilmile või säilitada neid arhiveerimiseks muul magnet- või optilisel andmekandjal, kui:

a) mikrofilmile kandmise/salvestamisega tegelevad töötajad, kes on läbinud julgeolekukontrolli, mis vastab asjaomasele salastatuse tasemele;

b) mikrofilmile/andmekandjale tagatakse samasugune julgeolek nagu esialgsetele dokumentidele;

c) salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluva dokumendi mikrofilmile kandmisest/salvestamisest teatatakse dokumendi koostajale;

d) filmirullid või muud salvestusvahendid sisaldavad ainult samasse salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET, SECRET UE või CONFIDENTIEL UE kuuluvaid dokumente;

e) salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET või SECRET UE kuuluva dokumendi kandmisest mikrofilmile/salvestamisest tehakse selge märkus iga-aastaseks inventuuriks kasutatavasse registrisse;

f) originaaldokumendid, mis on kantud mikrofilmile või muul viisil salvestatud, hävitatakse punktides 31–36 sätestatud eeskirjade kohaselt.

30. Neid eeskirju kohaldatakse ka muude liikmesriigi julgeolekuasutuste lubatud salvestusvahendite suhtes, näiteks elektromagnetiliste andmekandjate ja optiliste ketaste suhtes.

EUROOPA LIIDU SALASTATUD DOKUMENTIDE REGULAARNE HÄVITAMINE

31. Euroopa Liidu salastatud dokumentide asjatu kuhjumise vältimiseks hävitatakse need dokumendid, mis dokumente valdava asutuse juhataja arvates on aegunud või üleliigsed, nii ruttu kui võimalik järgmisel viisil:

a) salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluvaid dokumente võib hävitada ainult nende dokumentide eest vastutav keskregister. Iga hävitatud dokumendi kohta koostatakse hävitamisakt, millele kirjutavad alla salastatuse kategooria TRÈS SECRET UE/EU TOP SECRET kontrolliametnik ja hävitamist tunnistama kutsutud ametnik, kes peavad olema läbinud julgeolekukontrolli salastatuse kategooria TRÈS SECRET UE/EU TOP SECRET jaoks. Logiraamatusse tehakse vastav märkus;

b) register säilitab hävitamisakte koos ringkäigulehtedega kümme aastat. Koopiad edastatakse esialgse dokumendi koostajale või asjaomasele keskregistrile ainult selgesõnalise taotluse korral;

c) salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluvad dokumendid, kaasa arvatud salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluvate dokumentide koostamise käigus tekkinud salastatud jäätmed (näiteks vigased koopiad, mustandid, trükitud märkmed ja koopiapaber) hävitatakse salastatuse kategooria TRÈS SECRET UE/EU TOP SECRET ametniku järelevalve all kas põletamise, paberimassiks muutmise või narmastamise teel või muutes need muul viisil loetamatuks nii, et neid ei ole võimalik enam kokku panna.

32. Salastatuse kategooriasse SECRET UE kuuluvad dokumendid hävitab nende dokumentide eest vastutav register, kasutades üht punkti 31 alapunktis c osutatud meetoditest sellise isiku järelevalve all, kes on läbinud julgeolekukontrolli. Salastatuse kategooriasse SECRET UE kuulunud hävitatud dokumendid loetletakse allakirjutatud hävitamisaktis, mida register säilitab koos ringkäigulehtedega vähemalt kolm aastat.

33. Salastatuse kategooriasse CONFIDENTIEL UE kuuluvad dokumendid hävitab nende dokumentide eest vastutav register, kasutades üht punkti 31 alapunktis c osutatud meetoditest sellise isiku järelevalve all, kes on läbinud julgeolekukontrolli. Nende hävitamine dokumenteeritakse siseriiklike õigusnormide kohaselt ning peasekretariaadi ja Euroopa Liidu detsentraliseeritud asutuste puhul peasekretäri/kõrge esindaja juhtnööride kohaselt.

34. Salastatuse kategooriasse RESTREINT UE kuuluvad dokumendid hävitab kas nende eest vastutav register või nende kasutaja siseriiklike õigusnormide kohaselt ning peasekretariaadi ja Euroopa Liidu detsentraliseeritud asutuste puhul peasekretäri/kõrge esindaja juhtnööride kohaselt.

HÄVITAMINE HÄDAOLUKORRAS

35. Peasekretariaat, liikmesriigid ja Euroopa Liidu detsentraliseeritud asutused koostavad kohalike olude põhjal kava Euroopa Liidu salastatud teabe kaitsmiseks kriisiolukorras, sätestades sealhulgas vajaduse korral kava dokumentide hävitamiseks hädaolukorras ja evakuatsiooniplaani; nad teevad oma vastavas organisatsioonis teatavaks juhtnöörid, mida peetakse vajalikuks, et välistada Euroopa Liidu salastatud teabe langemine volitamata isikute kätte.

36. Salastatuse kategooriatesse SECRET UE ja CONFIDENTIEL UE kuuluva materjali kaitsmiseks ja/või hävitamiseks kriisiolukorras võetavad meetmed ei tohi mingil juhul kahjustada salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluva materjali, sealhulgas šifreerimisvahendite kaitsmist või hävitamist, mis on olulisemad kui kõik muud ülesanded. Hädaolukorras šifreerimisvahendite kaitsmiseks või hävitamiseks võetavate meetmete puhul kohaldatakse *ad hoc* juhtnööre.

*VI peatükk*

**Nõukogule suunatud dokumentide suhtes kohaldatavad erieeskirjad**

37. Peasekretariaadis jälgib nõukogule suunatud dokumentides sisalduvat salastatuse kategooriatesse SECRET UE ja CONFIDENTIEL UE kuuluvat teavet salastatud teabe büroo.

Personali- ja hallduskü simuste peadirektori juhtimisel nimetatud büroo:

a) juhib toiminguid, mis on seotud sellise teabe registreerimise, kopeerimise, tõlkimise, edastamise, lähetamise ja hävitamisega;

b) ajakohastab salastatud teabe andmete loetelu;

c) küsitleb korrapäraselt teabe väljaandjaid seoses teabe salastatuse säilitamise vajalikkusega;

d) sätestab koostöös julgeolekubürooga teabe salastamise ja salastatuse kaotamise praktilise korra.

38. Salastatud teabe büroo peab registrit järgmiste andmete kohta:

a) salastatud teabe koostamise kuupäev;

b) salastatuse tase;

c) salastatuse tähtaeg;

d) väljaandja nimi ja üksus;

e) vastuvõtja või vastuvõtjad, järjekorranumber;

f) teema;

g) number;

h) tehtud koopiate arv;

i) nõukogule esitatud salastatud teabe kohta koostatud inventuurid;

j) salastatud teabe salastatuse kaotamise ja alandamise register.

39. Käesoleva jao I–V peatükis sätestatud üldeeskirju kohaldatakse peasekretariaadi salastatud teabe büroo suhtes, kui käesolevas peatükis sätestatud erieeskirjad neid ei muuda.

VIII JAGU

## SALASTATUSE KATEGOORIA TRÈS SECRET UE/EU TOP SECRET REGISTRID

1. Salastatuse kategooria TRÈS SECRET UE/EU TOP SECRET registrite eesmärk on tagada, et salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluvate dokumentide registreerimine, käitlemine ja levitamine toimuks julgeolekueeskirjade kohaselt. Salastatuse kategooria TRÈS SECRET UE/EU TOP SECRET registri juhataja on igas liikmesriigis, peasekretariaadis ja vajaduse korral Euroopa Liidu detsentraliseeritud asutuses salastatuse kategooria TRÈS SECRET UE/EU TOP SECRET kontrolliametnik.

2. Keskregister on peamine vastuvõttev ja lähetav asutus liikmesriikides, peasekretariaadis ja Euroopa Liidu detsentraliseeritud asutustes, kus sellised registrid on loodud, ja vajaduse korral ka muudes Euroopa Liidu institutsioonides, rahvusvahelistes organisatsioonides ja kolmandates riikides, millega nõukogu on sõlminud kokkulepped salastatud teabe vahetamise julgeolekukorra kohta.

3. Vajaduse korral luuakse alamregistrid, mis vastutavad salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluvate dokumentide sisemise haldamise eest; sellistes alamregistrites peetakse ajakohastatud andmeid iga alamregistri vastutusel oleva dokumendi liikumise kohta.

4. Salastatuse kategooria TRÈS SECRET UE/EU TOP SECRET alamregistrid luuakse I jao kohaselt, et rahuldada pikaajaline vajadus, ning sellised alamregistrid on seotud salastatuse kategooria TRÈS SECRET UE/EU TOP SECRET keskregistriga. Kui salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluvaid dokumente on vaja kasutada üksnes ajutiselt ja juhuti, võib neid dokumente välja anda, ilma et selleks loodaks salastatuse kategooria TRÈS SECRET UE/EU TOP SECRET alamregister, kui ette on nähtud eeskirjad, millega tagatakse, et sellised dokumendid jäävad salastatuse kategooria TRÈS SECRET UE/EU TOP SECRET asjaomase registri kontrolli alla ning et järgitakse kõiki füüsilisi ja personaliga seotud julgeolekumeetmeid.

5. Alamregistrid ei või salastatuse kategooriasse SECRET UE/EU TOP SECRET kuuluvaid dokumente edastada otse teistele salastatuse kategooria SECRET UE/EU TOP SECRET sama keskregistri alamregistritele, kui selleks ei ole keskregistri selgesõnalist nõusolekut.

6. Eri keskregistrite juurde kuuluvad alamregistrid vahetavad salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluvaid dokumente salastatuse kategooria TRÈS SECRET UE/EU TOP SECRET keskregistri vahendusel.

### SALASTATUSE KATEGOORIA TRÈS SECRET UE/EU TOP SECRET KESKREGISTRID

7. Kontrolliametnikuna vastutab salastatuse kategooria TRÈS SECRET UE/EU TOP SECRET keskregistri juhataja järgmise eest:

   a) salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluvate dokumentide edastamine kooskõlas VII jaos määratletud eeskirjadega;

   b) kõigi keskregistriga seotud salastatuse kategooria TRÈS SECRET UE/EU TOP SECRET alamregistrite loetelu pidamine koos ametissenimetatud kontrolliametnike ja nende volitatud asetäitjate nimede ja allkirjadega;

   c) registrite kättesaamistõendite säilitamine kõigi salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluvate ja keskregistri kaudu levitatud dokumentide kohta;

   d) registri pidamine hallatavate ja levitatavate salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluvate dokumentide kohta;

   e) ajakohastatud loetelu pidamine kõigi salastatuse kategooria TRÈS SECRET UE/EU TOP SECRET keskregistrite kohta, millega ta tavapäraselt suhtleb, koos nende ametissenimetatud kontrolliametnike ja nende volitatud asetäitjate nimede ja allkirjadega;

   f) kõigi registris olevate salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluvate dokumentide füüsiline kaitsmine IV jaos sätestatud eeskirjade kohaselt.

### SALASTATUSE KATEGOORIA TRÈS SECRET UE/EU TOP SECRET ALAMREGISTRID

8. Kontrolliametnikuna vastutab salastatuse kategooria TRÈS SECRET UE/EU TOP SECRET alamregistri juhataja järgmise eest:

   a) salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluvate dokumentide edastamine kooskõlas VII jaos ja VIII jao punktides 5 ja 6 sätestatud eeskirjadega;

b) ajakohastatud loetelu pidamine kõigi isikute kohta, kellel on luba juurdepääsuks tema kontrolli all olevale salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluvale teabele;

c) salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluvate dokumentide levitamine kooskõlas nende koostaja juhtnööridega või teadmisvajaduse põhimõttel, olles kõigepealt kontrollinud, et adressaat on läbinud julgeolekukontrolli nõutaval tasemel;

d) ajakohastatud registri pidamine kõigi salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluvate dokumentide kohta, mida hoitakse või mis ringlevad tema kontrolli all või mis on antud edasi teistele salastatuse kategooria TRÈS SECRET UE/EU TOP SECRET registritele, ja kõigi asjaomaste kättesaamistõendite säilitamine;

e) ajakohastatud loetelu pidamine salastatuse kategooria TRÈS SECRET UE/EU TOP SECRET registrite kohta, millega tal on lubatud vahetada salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluvaid dokumente, koos nende kontrolliametnike ja nende volitatud asetäitjate nimede ja allkirjadega;

f) kõigi alamregistris olevate salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluvate dokumentide füüsiline kaitsmine IV jaos sätestatud eeskirjade kohaselt.

INVENTUUR

9. Iga salastatuse kategooria TRÈS SECRET UE/EU TOP SECRET register teeb iga kaheteistkümne kuu järel üksikasjaliku inventuuri kõigi salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluvate dokumentide kohta, mille eest ta vastutab. Dokument loetakse arvelevõetuks, kui ta on registris füüsiliselt inventeeritud või kui registris on kättesaamistõend salastatuse kategooria SECRET UE/EU TOP SECRET registrilt, kuhu dokument on edasi antud, dokumendi hävitamisakt või juhend asjaomase dokumendi salastatuse taseme vähendamiseks või kaotamiseks.

10. Alamregistrid edastavad oma iga-aastase inventuuri tulemused keskregistrisse, mille ees nad vastutavad, asjaomase keskregistri määratud kuupäevaks.

11. Liikmesriikide julgeolekuasutused ja need Euroopa Liidu institutsioonid, rahvusvahelised organisatsioonid ja Euroopa Liidu detsentraliseeritud asutused, milles on loodud salastatuse kategooria TRÈS SECRET UE/EU TOP SECRET keskregister, edastavad salastatuse kategooria TRÈS SECRET UE/EU TOP SECRET keskregistrite iga-aastaste inventuuride tulemused peasekretärile/kõrgele esindajale hiljemalt iga aasta 1. aprilliks.

IX JAGU

## VÄLJASPOOL NÕUKOGU RUUME TOIMUVATE JA DELIKAATSEID TEEMASID KÄSITLEVATE ERIKOOSOLEKUTE AJAL KOHALDATAVAD JULGEOLEKUMEETMED

ÜLDOSA

1. Kui Euroopa Ülemkogu või nõukogu istungeid, ministrite kokkusaamisi või muid olulisi koosolekuid peetakse väljaspool nõukogu ruume Brüsselis ja Luxembourgis ja kui see on põhjendatud konkreetsete julgeolekueeskirjadega, mis on seotud käsitletavate teemade või teabe delikaatsusega, tuleb võtta allpool kirjeldatud julgeolekumeetmed. Kõnealused meetmed on seotud ainult Euroopa Liidu salastatud teabe kaitsega; kavandada võib ka muid julgeolekmeetmeid.

VASTUTUS

**Vastuvõtvad liikmesriigid**

2. Liikmesriik, mille territooriumil koosolek toimub (vastuvõttev liikmesriik) peaks koostöös peasekretariaadi julgeolekuametnikuga vastutama Euroopa Ülemkogu või nõukogu istungi, ministrite kokkusaamise või muu olulise koosoleku julgeoleku eest ning peamiste osalejate ja nende kaastöötajate füüsilise julgeoleku eest.

Seoses julgeoleku kaitsmisega peaks kõnealune liikmesriik eelkõige tagama, et:

a) koostatakse kavad selle kohta, kuidas reageerida julgeolekut ähvardavatele ohtudele ja julgeolekuga seotud vahejuhtumitele; kõnealused meetmed peavad eelkõige hõlmama Euroopa Liidu salastatud dokumentide turvalist säilitamist büroodes;

b) võetakse meetmeid võimaldamaks juurdepääs nõukogu sidesüsteemidele, et nende kaudu võtta vastu ja edastada Euroopa Liidu salastatud sõnumeid. Vajaduse korral võimaldab vastuvõttev liikmesriik juurdepääsu ka turvalistele telefonisüsteemidele.

**Liikmesriigid**

3. Liikmesriikide asutused peaksid võtma vajalikud meetmed tagamaks, et:

a) nende riigi esindajate julgeolekusertifikaadid esitatakse vajaduse korral signaali või faksiga kas otse koosoleku julgeolekuametnikule või peasekretariaadi julgeolekuametniku kaudu;

b) kõigist konkreetsetest ohtudest teatatakse vastuvõtva liikmesriigi asutustele ja vajaduse korral peasekretariaadi julgeolekubüroole, et saaks võtta asjakohaseid meetmeid.

**Koosoleku julgeolekuametnik**

4. Ametisse tuleb määrata julgeolekuametnik, kes vastutab üldise ettevalmistamise ja üldiste sisemiste julgeolekumeetmete kontrollimise eest ning kooskõlastamise eest muude asjaomaste julgeolekuasutustega. Kõnealuse isiku võetavad meetmed peaksid üldiselt olema seotud järgmisega:

a) i) kaitsemeetmed koosoleku toimumiskohas tagamaks, et koosolek toimub vahejuhtumiteta, mis võiksid kahjustada koosolekul kasutatava Euroopa Liidu salastatud teabe julgeolekut;

ii) nende töötajate kontrollimine, kellele on lubatud juurdepääs koosoleku toimumiskohta, osalejate ruumidesse ja konverentsiruumidesse, ja seadmete kontrollimine;

iii) pidev koordineerimine vastuvõtva liikmesriigi pädevate asutustega ja peasekretariaadi julgeolekubürooga;

b) julgeolekujuhendite lisamine koosoleku kausta, võttes nõuetekohaselt arvesse käesolevates julgeolekueeskirjades sätestatud nõudeid ja muid vajalikuks peetavaid julgeolekujuhendeid.

**Peasekretariaadi julgeolekubüroo**

5. Peasekretariaadi julgeolekubüroo peaks koosoleku ettevalmistamisel tegutsema julgeolekunõuandjana; kõnealune büroo peaks olema koosolekul esindatud ja vajaduse korral nõustama koosoleku julgeolekuametnikku ja osalejaid.

6. Iga koosolekul osalev delegatsioon peaks määrama julgeolekuametniku, kes vastutab julgeolekuküsimuste eest oma delegatsioonis ja peab sidet koosoleku julgeolekuametnikuga ning vajaduse korral ka peasekretariaadi julgeolekubüroo esindajaga.

JULGEOLEKUMEETMED

**Turvaalad**

7. Järgmised turvaalad tuleks kindlaks määrata:

a) II klassi turvaala, mis hõlmab dokumentide ettevalmistamise ruumi, peasekretariaadi ametiruume ja paljundusseadmeid ning vajaduse korral delegatsioonide ametiruume;

b) I klassi turvaala, mis hõlmab konverentsiruumi, tõlkekabiine ja helitehnikute kabiine;

c) haldustegevuse alad, mis hõlmavad pressiruume ja koosolekukoha neid osi, mida kasutatakse haldustegevuseks, toitlustamiseks ja majutamiseks, ning vahetult pressikeskuse ja koosoleku toimumiskoha ümbruses paiknev ala.

**Läbipääsuload**

8. Koosoleku julgeolekuametnik peaks andma välja vajalikud nimesildid delegatsioonide teatatud vajaduste kohaselt. Vajaduse korral võib eristada juurdepääsu eri turvaaladele.

9. Koosoleku julgeolekujuhendid peaksid kohustama kõiki asjaomaseid isikuid kandma oma nimesilti koosolekukohas viibides alati nähtaval kohal, et julgeolekutöötajad saaksid neid vajaduse korral kontrollida.

10. Peale nimesilti kandvate osalejate tuleks koosoleku toimumiskohta lubada võimalikult vähe inimesi. Riikide delegatsioonid, kes soovivad koosoleku ajal külalisi vastu võtta, peaksid sellest teatama koosoleku julgeolekuametnikule. Külalistele tuleb anda külalise nimesilt. Tuleb täita külalise läbipääsuloa vorm, millele tuleb kirjutada nii külalise kui ka külalise vastuvõtja nimi. Külalist peab alati saatma kas turvamees või külalise vastuvõtja. Külalise läbipääsuloa vorm peaks olema külalise saatja käes, kes tagastab selle koos külalise nimesildiga julgeolekutöötajale, kui külaline lahkub koosoleku toimumiskohast.

**Foto- ja heliseadmete kontrollimine**

11. I klassi turvaalale ei tohi tuua fotoaparaate ega salvestusseadmeid, kui tegemist ei ole seadmetega, mille toovad sinna fotograafid või helitehnikud, kellel on selleks koosoleku julgeolekuametniku nõuetekohane luba.

**Portfellide, kaasaskantavate arvutite ja pakkide kontrollimine**

12. Läbipääsuloa omanikud, kellel on lubatud pääs turvaaladele, võivad tavaliselt võtta kaasa oma portfellid ja kaasaskantavad arvutid (ainult autonoomse vooluallikaga), ilma et neid kontrollitaks. Delegatsioonidele mõeldud pakkide puhul võivad delegatsioonid võtta vastu neile toodud pakid, mida kontrollib kas delegatsiooni julgeolekuametnik, mis vaadatakse läbi spetsiaalsete seadmetega või mille julgeolekutöötajad avavad kontrollimiseks. Kui koosoleku julgeolekuametnik peab seda vajalikuks, võib portfellide ja pakkide kontrollimiseks kehtestada rangemad meetmed.

**Tehniline julgeolek**

13. Tehnilise julgeoleku meeskond võib tagada tehniliselt koosolekuruumi julgeoleku ja jälgida seda ka elektrooniliselt koosoleku ajal.

**Delegatsioonide dokumendid**

14. Delegatsioonid peaksid vastutama Euroopa Liidu salastatud dokumentide viimise eest koosolekule ja sealt ära. Nad peaksid vastutama ka nende dokumentide kontrollimise ja julgeoleku eest dokumentide kasutamise ajal neile määratud ruumides. Vastuvõtvatelt liikmesriikidelt võib paluda, et nad aitaksid vedada salastatud dokumente koosolekukohta ja sealt tagasi.

**Dokumentide turvaline hoidmine**

15. Kui peasekretariaat, komisjon või delegatsioonid ei suuda oma salastatud dokumente säilitada kooskõlas vastuvõetud standarditega, võivad nad jätta sellised dokumendid pitseeritud ümbrikus kättesaamistõendi vastu koosoleku julgeolekuametniku kätte, kes säilitab dokumente kooskõlas vastuvõetud standarditega.

**Ametiruumide kontrollimine**

16. Koosoleku julgeolekuametnik peaks korraldama peasekretariaadi ja delegatsioonide ametiruumide kontrollimise iga tööpäeva lõpus, et tagada kõigi Euroopa Liidu salastatud dokumentide säilitamine turvalises kohas; teistsuguste asjaolude korral peab ta võtma vajalikke meetmeid.

**Euroopa Liidu salastatud jäätmete kõrvaldamine**

17. Kõiki jäätmeid tuleb pidada Euroopa Liidu seisukohast salastatuks ning prügikorvid ja -kotid tuleks anda peasekretariaadile või delegatsioonidele nende kõrvaldamiseks. Enne kui peasekretariaat ja delegatsioonid lahkuvad neile määratud ruumidest, peaksid nad viima oma jäätmed koosoleku julgeolekuametnikule, kes korraldab jäätmete hävitamise eeskirjade kohaselt.

18. Koosoleku lõpus tuleb kõiki peasekretariaadis või delegatsioonides olevaid dokumente, mida enam vaja ei ole, käsitleda jäätmetena. Enne koosoleku jaoks võetud julgeolekumeetmete lõpetamist tuleb peasekretariaadi ja delegatsioonide ruumides teha põhjalik läbiotsmine. Dokumendid, mille kohta on kättesaamistõendile alla kirjutatud, tuleb võimaluse korral hävitada nii, nagu on sätestatud VII jaos.

X JAGU

## JULGEOLEKU RIKKUMINE JA EUROOPA LIIDU SALASTATUD TEABE KAHJUSTAMINE

1. Julgeoleku rikkumine toimub sellise toimingu või toimimatajätmise tagajärjel, mis on vastuolus nõukogu või siseriiklike julgeolekueeskirjadega ja mis võib seada ohtu Euroopa Liidu salastatud teabe või kahjustada seda.

2. Euroopa Liidu salastatud teabe kahjustamine toimub siis, kui kõnealune teave on tervikuna või osaliselt sattunud volitamata isikute kätte, st isikute kätte, kes ei ole läbinud julgeolekukontrolli vastaval tasemel või kellel puudub asjaomaste dokumentide kohta teadmisvajadus, või kui on tõenäoline, et teave on sattunud selliste isikute kätte.

3. Euroopa Liidu salastatud teavet võidakse kahjustada hooletuse, ettevaatamatuse või mõtlematuse tagajärjel või seda võivad teha Euroopa Liidu või tema liikmesriikide vastu suunatud teenistused, kes huvituvad Euroopa Liidu salastatud teabest ja tema tegevusest, või õõnestusorganisatsioonid.

4. On oluline, et kõigile isikutele, kes peavad käitlema Euroopa Liidu salastatud teavet, tutvustatakse põhjalikult julgeolekukorda, ebadiskreetsete vestluste ohtlikkust ja seda, millised peaksid olema nende suhted ajakirjandusega. Sellised isikud peaksid teadma, kui oluline on teatada igast märgatud julgeoleku rikkumise juhust viivitamata asutusele või ametiisikule, kes vastutab julgeoleku eest liikmesriigis, institutsioonis või asutuses, kus asjaomane isik töötab.

5. Kui julgeolekuasutus avastab Euroopa Liidu salastatud teabega seotud julgeoleku rikkumise või Euroopa Liidu salastatud materjali kaotamise või kadumise või kui talle teatatakse sellest, võtab ta viivitamata meetmeid, et:

   a) teha kindlaks asjaolud;

   b) hinnata kahju ja minimeerida selle mõju;

   c) välistada sellise juhtumi kordumine;

   d) teavitada asjaomaseid asutusi julgeoleku rikkumise tagajärgedest.

   Seoses sellega esitatakse järgmine teave:

   i) asjaomase teabe kirjeldus, sealhulgas selle salastatuse tase, viitenumber, koopia number, kuupäev, koostaja, teema ja reguleerimisala;

   ii) lühike ülevaade julgeoleku rikkumise asjaoludest, sealhulgas kuupäev ja ajavahemik, mille jooksul teavet kahjustati;

   iii) teatis selle kohta, kas juhtunust on teatatud dokumendi koostajale.

6. Pärast seda, kui neile on teatatud sellise julgeoleku rikkumise võimalikkusest, on kõik julgeolekuasutused kohustatud sellest viivitamata aru andma järgmises korras: salastatuse kategooria EU TOP SECRET alamregister annab oma salastatuse kategooria EU TOP SECRET keskregistri kaudu asjast aru peasekretariaadi julgeolekubüroole; kui Euroopa Liidu salastatud teavet kahjustatakse liikmesriigi õigusruumis, teatab vastutav siseriiklik julgeolekuasutus sellest peasekretariaadi julgeolekubüroole punktis 5 sätestatu kohaselt.

7. Salastatuse kategooriasse RESTREINT UE kuuluva teabega seotud juhtumitest tuleb teatada ainult siis, kui tegemist on ebatavaliste asjaoludega.

8. Saanud teate julgeoleku rikkumise kohta, peasekretär/kõrge esindaja:

   a) teatab sellest asutusele või ametiisikule, kes koostas kõnealuse salastatud teabe;

   b) palub asjaomasel julgeolekuasutusel alustada uurimist;

   c) koordineerib uurimist, kui juhtum puudutab mitut julgeolekuasutust;

d) palub esitada aruande rikkumise asjaolude, toimumise tõenäolise kuupäeva ja ajavahemiku ning avastamise kuupäeva ja aja kohta koos asjaomase materjali sisu ja salastatuse taseme üksikasjaliku kirjeldusega. Aruanne tuleks esitada ka Euroopa Liidu või ühe või mitme tema liikmesriigi huvidele tekitatud kahju ja sellise juhtumi kordumise välistamiseks võetud meetmete kohta.

9. Dokumendi koostaja teatab juhtunust dokumendi adressaatidele ja annab neile vajalikud juhtnöörid.

10. Kõik isikud, kes vastutavad Euroopa Liidu salastatud teabe kahjustamise eest, kannavad distsiplinaarvastutust asjakohaste reeglite ja eeskirjade kohaselt. Distsiplinaarvastutus ei piira õiguslike meetmete võtmist.

XI JAGU

# INFOTEHNOLOOGIA JA SIDESÜSTEEMIDE ABIL KÄIDELDAVA TEABE KAITSMINE

## Sisukord

*I peatükk*

**Sissejuhatus**

ÜLDOSA

1. Käesolevas jaos sätestatud julgeolekupõhimõtteid ja -eeskirju kohaldatakse kõigi side- ja infosüsteemide ja -võrkude (edaspidi SÜSTEEMID) suhtes, mille abil käideldakse salastatuse kategooriasse CONFIDENTIEL UE ja kõrgemasse salastatuse kategooriasse kuuluvat teavet.

2. Ka SÜSTEEMIDE puhul, mille abil käideldakse salastatuse kategooriasse RESTREINT UE kuuluvat teavet, tuleb võtta julgeolekumeetmeid sellise teabe kaitsmiseks. Kõigi SÜSTEEMIDE puhul tuleb võtta julgeolekumeetmed, et kaitsta nende süsteemide ja neis sisalduva teabe terviklikkust ja kättesaadavust. Kõnealuste süsteemide suhtes kohaldatavad julgeolekumeetmed määrab kindlaks julgeoleku akrediteerimisasutus (*security accreditation authority* — saa) ning need on vastavuses hinnatava ohuga ja kooskõlas käesolevates julgeolekueeskirjades sätestatud põhimõtetega.

3. Kui sensorsüsteemid sisaldavad integreeritud infotehnoloogiasüsteeme, määratakse selliste süsteemide kaitse kindlaks ja täpsustatakse seoses nende süsteemidega, mille juurde nad kuuluvad, kasutades võimaluse korral käesoleva jao kohaldatavaid sätteid.

SÜSTEEME ÄHVARDAVAD OHUD JA NENDE NÕRGAD KOHAD

4. Üldiselt võib ohtu määratleda kui võimalust, et juhuslikult või tahtlikult kahjustatakse julgeolekut. SÜSTEEMIDE puhul kaasneb sellise kahjustamisega ühe või mitme salastatuse, terviklikkuse või kättesaadavuse atribuudi kaotus. Nõrka kohta võib määratleda kui nõrkust või kontrolli puudumist, mis soodustab konkreetse vahendi või sihtmärgi vastu suunatud ohu realiseerumist või võimaldab sellel realiseeruda. Nõrkus võib tuleneda millegi tegemata jätmisest või olla seotud puudustega kontrollimise intensiivsuses, täiemahulisuses või järjepidevuses; see võib olla tehnilist, korralduslikku või kasutuslikku laadi.

5. Kiirotsinguteks, edastamiseks ja kasutamiseks mõeldud SÜSTEEMIDES kontsentreeritud kujul käideldavat Euroopa Liidu salastatud ja salastamata teavet võivad ohustada mitmed riskid. Selliste riskide hulka kuuluvad volitamata kasutajate juurdepääs teabele ja juurdepääsu keelamine volitatud kasutajatele. Samuti on olemas teabe volitamata avaldamise, kahjustamise, muutmise või kustutamise risk. Lisaks sellele on keerukad ja vahel ka haprad seadmed sageli kallid ning neid on raske parandada või kiiresti asendada. Seega on kõnealused SÜSTEEMID luureandmete kogumise ja sabotaaži seisukohast atraktiivne sihtmärk eriti juhul, kui arvatakse, et julgeolekumeetmed ei ole tõhusad.

JULGEOLEKUMEETMED

6. Käesolevas jaos sätestatud julgeolekumeetmete põhieesmärk on kaitsta teavet volitamata avaldamise (salastatuse kadumise) ning teabe terviklikkuse ja kättesaadavuse kadumise vastu. Euroopa Liidu salastatud teabe käitlemiseks kasutatava SÜSTEEMI julgeoleku piisavaks kaitsmiseks määratletakse tavapärase julgeoleku asjakohased standardid koos iga SÜSTEEMI jaoks kavandatud spetsiaalsete julgeolekumenetluste ja -tehnikaga.

7. Selleks et luua SÜSTEEMI turvaline töökeskkond, määratakse kindlaks ja viiakse ellu tasakaalustatud julgeolekumeetmete kogum. Selliseid meetmeid rakendatakse seoses füüsiliste elementide, töötajate, mittetehniliste menetluste ning arvutite ja sideseadmete käitamise korraga.

8. Teadmisvajaduse põhimõtte rakendamiseks ning teabe volitamata avaldamise välistamiseks ja avastamiseks tuleb ette näha arvutiturbemeetmed (riistvara ja tarkvara turvaelemendid). Julgeolekunõuete kehtestamise käigus määratakse kindlaks, kuivõrd arvutiturbemeetmeid võib usaldada. Akrediteerimisel määratakse kindlaks, et olemas on arvutiturbemeetmete usaldusväärsust toetav kindluse tase.

SÜSTEEMISPETSIIFILISTE JULGEOLEKUNÕUETE LOETELU

9. Infotehnoloogiasüsteemi vastutav käitaja (*IT System Operational Authority* — ITSOA) peab koostöös projektiga töötavate isikute ja teabeturbeasutusega esitama kõigi SÜSTEEMIDE kohta, mille abil käideldakse salastatuse kategooriasse CONFIDENTIEL UE või kõrgemasse kategooriasse kuuluvat teavet, süsteemispetsiifiliste julgeolekunõuete loetelu (*SYSTEM-Specific Security Requirement Statement* — SSRS), mille peab olema heaks kiitnud julgeoleku akrediteerimisasutus. Süsteemispetsiifiliste julgeolekunõuete loetelu nõutakse ka siis, kui julgeoleku akrediteerimisasutus peab salastatuse kategooriasse RESTREINT UE kuuluva teabe või salastamata teabe kättesaadavust ja terviklikkust üliloluliseks.

10. Süsteemispetsiifiliste julgeolekunõuete loetelu koostatakse võimalikult varases projekti käivitamise järgus ning projekti jätkumise käigus arendatakse seda edasi ja täiustatakse; projekti eri etappidel ja SÜSTEEMI elutsükli jooksul täidab süsteemispetsiifiliste julgeolekunõuete loetelu eri funktsioone.

11. Süsteemispetsiifiliste julgeolekunõuete loetelu näol on tegemist siduva kokkuleppega infotehnoloogiasüsteemi vastutava käitaja ja julgeoleku akrediteerimisasutuse vahel, mille põhjal SÜSTEEM akrediteeritakse.

12. Süsteemispetsiifiliste julgeolekunõuete loetelus väljendatakse lõplikult ja selgelt, milliseid julgeolekupõhimõtteid tuleb järgida ja milliseid üksikasjalikke julgeolekunõudeid täita. See põhineb nõukogu julgeolekupoliitikal ja riski hindamisel või see määratakse kindlaks selliste parameetritega nagu töökeskkond, töötajate julgeolekukontrolli miinimumtase, käideldava teabe salastatuse kõrgeim tase, süsteemi turvarežiim või kasutajate nõudmised. Süsteemispetsiifiliste julgeolekunõuete loetelu on projekti dokumentatsiooni lahutamatu osa, mis esitatakse pädevatele asutustele tehniliseks, eelarveliseks ja julgeolekualaseks heakskiitmiseks. Lõplikul kujul moodustab süsteemispetsiifiliste julgeolekunõuete loetelu täieliku selgituse selle kohta, mida tähendab SÜSTEEMI turvalisus.

SÜSTEEMI TURVAREŽIIMID

13. Kõik SÜSTEEMID, mille abil käideldakse salastatuse kategooriasse CONFIDENTIEL UE või kõrgemasse kategooriasse kuuluvat teavet, akrediteeritakse tööks ühes või kui eri ajavahemike nõuded seda eeldavad, mitmes turvarežiimis või selle siseriiklikus ekvivalendis:

a) ühtlane ülaturve;

b) diferentsiaalne ülaturve ja

c) mitmetasemeline turve.

*II peatükk*

**Mõisted**

LISATÄHISTUSED

14. Lisatähistusi, näiteks tähistust CRYPTO ja muid Euroopa Liidus tunnustatud käitlemise eritähiseid kasutatakse siis, kui peale salastatuse kategooria on vaja veel tähistada piiratud levikut ja erikäitlemist.

15. ÜHTLASE ÜLATURBE REŽIIM tähendab süsteemi turvarežiimi, mille puhul KÕIK isikud, kellel on SÜSTEEMILE juurdepääs, peavad läbima SÜSTEEMIS käideldava teabe kõrgeimale salastatuse tasemele vastava julgeolekukontrolli ja neil on ühine teadmisvajadus KOGU SÜSTEEMIS käideldava teabe järele.

*Märkused:*

1) Ühine teadmisvajadus tähendab seda, et arvutiturvaelementidega ei pea kohustuslikus korras eristama teavet SÜSTEEMI sees.

2) Muud turvaelemendid (näiteks füüsilised, personaliga seotud ja menetluslikud) vastavad SÜSTEEMIS käideldava teabe kõrgeima salastatuse taseme nõuetele ja kõigi kategooriate tähistele.

16. DIFERENTSIAALSE ÜLATURBE REŽIIM tähendab süsteemi turvarežiimi, mille puhul KÕIK isikud, kellel on juurdepääs SÜSTEEMILE, peavad läbima SÜSTEEMIS käideldava teabe kõrgeimale salastatuse tasemele vastava julgeolekukontrolli, kuid KÕIGIL isikutel EI ole ühist teadmisvajadust KOGU SÜSTEEMIS käideldava teabe järele.

*Märkused:*

1) Ühise teadmisvajaduse puudumine tähendab seda, et arvutiturvaelementidega tuleb tagada valikuline juurdepääs SÜSTEEMIs sisalduvale teabele ja selle teabe eristamine SÜSTEEMI sees.

2) Muud turvaelemendid (näiteks füüsilised, personaliga seotud ja menetluslikud) vastavad SÜSTEEMIS käideldava teabe kõrgeima salastatuse taseme nõudmistele ja kõigi kategooriate tähistele.

3) Kõnealuses turvarežiimis SÜSTEEMIS käideldavat või olemasolevat teavet koos genereeritava väljundiga kaitstakse nii, nagu kuuluks see vastavasse teabekategooriasse ja nõuaks kõrgeimat salastatuse taset, kuni vastupidise otsuse tegemiseni, kui puudub piisavalt usaldusväärne kasutatav märgistamissüsteem.

17. MITMETASEMELISE TURBE REŽIIM tähendab süsteemi turvarežiimi, mille puhul KÕIK isikud, kellel on juurdepääs SÜSTEEMILE, EI pea läbima SÜSTEEMIS käideldava teabe kõrgeimale salastatuse tasemele vastavat julgeolekukontrolli ning KÕIGIL isikutel EI ole ühist teadmisvajadust KOGU SÜSTEEMIS käideldava teabe järele.

*Märkused:*

1) Kõnealune süsteemi turvarežiim võimaldab praegu käidelda eri salastatuse tasemetele ja eri teabekategooriatesse kuuluvat teavet.

2) Asjaolu, et kõiki isikud ei pea läbima kõige kõrgemale salastatuse tasemele vastavat julgeolekukontrolli koos ühise teadmisvajaduse puudumisega tähendab seda, et arvutiturvaelementidega tuleb tagada valikuline juurdepääs SÜSTEEMIS sisalduvale teabele ja selle teabe eristamine SÜSTEEMI sees.

18. TEABETURVE (INFOSEC) tähendab turvameetmete rakendamist selleks, et kaitsta side-, teabe- ja muudes elektroonilistes süsteemides töödeldavat, säilitatavat ja edastatavat teavet salastatuse, terviklikkuse või kättesaadavuse juhusliku ja tahtliku rikkumise eest ning välistada süsteemide terviklikkuse ja kättesaadavuse rikkumine. Teabeturbe meetmete hulka kuuluvad arvutite, edastuse, lähetuste ja krüptograafia turvalisus ning teabe ja SÜSTEEMIDE vastu suunatud ohtude avastamine, dokumenteerimine ja nende suhtes vastumeetmete võtmine.

19. ARVUTITURVE (COMPUSEC) tähendab riistvara, püsivara ja tarkvara turvaelementide rakendamist arvutisüsteemis, et kaitsta teabe volitamata avaldamise, manipuleerimise, muutmise/kustutamise ja teenuste keelamise eest või neid takistada.

20. ARVUTITURBETOODE tähendab üldist arvutiturbeeset, mis sisestatakse infotehnoloogiasüsteemi, et see tõhustaks või tagaks käideldava teabe salastatuse, terviklikkuse ja kättesaadavuse.

21. SIDETURVE (COMSEC) tähendab turvameetmete rakendamist sides, et keelata volitamata isikutele juurdepääs väärtuslikule teabele, mida nad võiksid saada sellise side valdamise ja uurimise käigus, ning tagada sellise side autentsus.

*Märkus:*

Sellised meetmed hõlmavad ühest küljest krüptograafia, edastuse ja lähetuste turvalisust ning teisest küljest korralduslikku, füüsilist, personali, dokumentide ja arvutite julgeolekut.

22. HINDAMINE tähendab seda, et asjaomane asutus teeb üksikasjaliku tehnilise uuringu SÜSTEEMI julgeolekuaspektide või krüpteerimis- või arvutiturbetoote kohta.

*Märkused:*

1) Hindamise käigus uuritakse nõutavate turbefunktsioonide olemasolu ja selliste funktsioonide kahjulike kõrvalmõjude puudumist ning antakse hinnang sellele, kas kõnealuseid funktsioone on võimalik rikkuda.

2) Hindamise käigus tehakse kindlaks, kui suures ulatuses on täidetud SÜSTEEMI või arvutiturbetoote turvanõuded, ja kehtestatakse SÜSTEEMI või krüpteerimisseadme või arvutiturbetootele usaldatud funktsiooni kindluse tase.

23. SERTIFITSEERIMINE tähendab sellise ametliku teatise väljaandmist, mida toetab sõltumatu ülevaade hindamise käigu ja tulemuste kohta ning selle kohta, kuivõrd SÜSTEEM vastab julgeolekunõuetele või arvutiturbetoode eelnevalt kindlaksmääratud turvanõuetele.

24. AKREDITEERIMINE tähendab SÜSTEEMILE loa andmist ja heakskiitu töödelda Euroopa Liidu salastatud teavet süsteemi töökeskkonnas.

*Märkus:*

Selline akrediteerimine peaks toimuma pärast kõigi asjakohaste julgeolekumenetluste rakendamist ja süsteemi vahendite piisava julgeolekutaseme saavutamist. Akrediteerimine peaks tavaliselt toimuma süsteemispetsiifiliste julgeolekunõuete loetelu põhjal ja sisaldama järgmist:

a) süsteemi akrediteerimise eesmärk; eelkõige see, millisesse salastatuse kategooriasse kuuluvat teavet kavatsetakse käitlema hakata ja milliseid süsteemi või võrgu turvarežiime kavatsetakse kasutada;

b) riskijuhtimise ülevaade, et teha kindlaks ohud ja nõrgad kohad ning nende vastu võetavad meetmed;

c) julgeolekuga seotud töökord koos kavandatud toimingute üksikasjalise kirjeldusega (näiteks pakutavad režiimid, teenused), kaasa arvatud SÜSTEEMI turvaelementide kirjeldus, mis on akrediteerimise aluseks;

d) turvaelementide rakendamise ja ülalpidamise kava;

e) süsteemi turvalisuse või võrgu turvalisuse esialgse ja edaspidise katsetamise, hindamise ja sertifitseerimise kava ja

f) vajaduse korral tõend koos muude akrediteerimisdokumentidega.

25. INFOTEHNOLOOGIASÜSTEEM tähendab seadmete, meetodite ja menetluste ja vajaduse korral töötajate kogumit, mis täidab teabe töötlemisega seotud funktsioone.

*Märkused:*

1) Seda käsitatakse kui vahendite kogumit, mis on konfigureeritud teabe käitlemiseks süsteemis.

2) Sellised süsteemid võivad toetada konsulteerimist, juhtimist, sidet, teadus- ja haldusrakendusi, kaasa arvatud tekstitöötlus.

3) Süsteemi piirid määratakse üldiselt kindlaks kui elemendid, mis on ühe infotehnoloogiasüsteemi vastutava käitaja kontrolli all.

4) Infotehnoloogiasüsteem võib hõlmata alamsüsteeme, millest mõned on ise infotehnoloogiasüsteemid.

26. INFOTEHNOLOOGIASÜSTEEMI TURVAELEMENTIDE hulka kuuluvad kõik riistvara/püsivara/tarkvara funktsioonid, omadused ja elemendid; operatsioonisüsteemid, arvestussüsteemid ja juurdepääsu kontroll, infotehnoloogia ala, terminali- või tööjaamaala ja juhtimispiirangud, füüsiline struktuur ja seadmed, töötajad ja sidekontroll, mis on vajalikud, et pakkuda infotehnoloogiasüsteemis käideldavale salastatud teabele vastuvõetaval tasemel kaitse.

27. INFOTEHNOLOOGIAVÕRK tähendab teabe vahetamiseks omavahel seotud infotehnoloogiasüsteemide geograafiliselt jaotatud organisatsiooni, mis hõlmab omavahel seotud infotehnoloogiasüsteemide komponente ja nende liideseid koos toetava teabe ja sidevõrkudega.

*Märkused:*

1) Infotehnoloogiavõrk võib teabe vahetamiseks kasutada üht või mitut omavahel seotud sidevõrku; mitu infotehnoloogiavõrku võivad kasutada ühise sidevõrgu teenuseid.

2) Infotehnoloogiavõrku nimetatakse "kohalikuks", kui see ühendab mitu samas kohas asuvat arvutit.

28. INFOTEHNOLOOGIAVÕRGU TURVAELEMENDID hõlmavad üksikute infotehnoloogiasüsteemide turvaelemente, koosnedes võrgust koos võrgu kui sellisega seotud lisakomponentide ja -omadustega (näiteks võrguside, turvatunnus, märgistusmehhanismid ja -menetlused, juurdepääsu kontroll, programmid ja kontrolljäljed), mis on vajalikud salastatud teabe vastuvõetava kaitsetaseme pakkumiseks.

29. INFOTEHNOLOOGIAALA tähendab ala, millel on üks või mitu arvutit, nende kohalikud välis- ja salvestusseadmed, juhtimisseadmed ning erivõrgu- ja -sideseadmed.

*Märkus:*

Kõnealune ala ei hõlma eraldi ala, millel asuvad kaugvälisseadmed või -terminalid/tööjaamad, isegi siis, kui need seadmed on ühendatud infotehnoloogiaalal asuvate seadmetega.

30. TERMINALI- või TÖÖJAAMAALA tähendab ala, kus on mõned arvutiseadmed, nende kohalikud välisseadmed või terminalid/tööjaamad ja nendega seotud sideseadmed, mis paiknevad väljaspool infotehnoloogiaala.

31. TEMPEST-vastumeetmed on julgeolekumeetmed, mille eesmärk on kaitsta seadmeid ja side infrastruktuure salastatud teabe kahjustamise eest tahtmatu elektromagnetkiirgusega.

*III peatükk*

**Vastutus julgeolekuküsimustes**

ÜLDOSA

32. I jao punktis 4 määratletud julgeolekukomitee vastutab ka teabeturbeküsimuste eest. Julgeolekukomitee korraldab oma töö nii, et ta suudab anda eksperdiabi eespool kirjeldatud küsimustes.

33. Julgeolekuga seotud probleemide puhul (vahejuhtumid, rikkumised jms) võtab vastutav siseriiklik asutus ja/või peasekretariaadi julgeolekubüroo viivitamata meetmeid. Kõigist probleemidest teatatakse peasekretariaadi julgeolekubüroole.

34. Peasekretär/kõrge esindaja või vajaduse korral Euroopa Liidu detsentraliseeritud asutuse juhataja loob teabeturbebüroo, et anda julgeolekuasutusele suuniseid SÜSTEEMIDE osaks kavandatud eriliste turvaelementide rakendamise ja kontrollimise kohta.

JULGEOLEKU AKREDITEERIMISASUTUS (*SECURITY ACCREDITATION AUTHORITY* — SAA)

35. Julgeoleku akrediteerimisasutus on kas:

— liikmesriigi julgeolekuasutus,

— peasekretäri/kõrge esindaja määratud asutus,

— Euroopa Liidu detsentraliseeritud asutuse julgeolekuasutus või

— nende delegeeritud/nimetatud esindajad olenevalt akrediteeritavast SÜSTEEMIST.

36. Julgeoleku akrediteerimisasutus vastutab selle eest, et SÜSTEEMID oleksid kooskõlas nõukogu julgeolekupõhimõtetega. Üks sellise asutuse ülesannetest on SÜSTEEMIDE tunnustamine seoses Euroopa Liidu salastatud teabe käitlemisega määratud salastatuse tasemel tema töökeskkonnas. Peasekretariaadi ja vajaduse korral Euroopa Liidu detsentraliseeritud asutuste puhul vastutab julgeoleku akrediteerimisasutus julgeoleku eest peasekretäri/kõrge esindaja või detsentraliseeritud asutuste juhtide nimel.

Peasekretariaadi julgeoleku akrediteerimisasutuse jurisdiktsioon hõlmab kõiki süsteeme, mis töötavad peasekretariaadi territooriumil. Liikmesriikides kasutatavad SÜSTEEMID ja SÜSTEEMIDE komponendid kuuluvad selle liikmesriigi jurisdiktsiooni alla. Kui SÜSTEEMI eri komponendid kuuluvad peasekretariaadi julgeoleku akrediteerimisasutuse ja muude julgeoleku akrediteerimisasutuste jurisdiktsiooni alla, määravad kõik osapooled peasekretariaadi julgeoleku akrediteerimisasutuse koordineerimisel ühise akrediteerimisameti.

TEABETURBEASUTUS (*INFOSEC AUTHORITY* — IA)

37. Teabeturbeasutus vastutab teabeturbebüroo tegevuse eest. Seoses peasekretariaadi ja vajaduse korral Euroopa Liidu detsentraliseeritud asutustega vastutab teabeturbeasutus järgmise eest:

— tehniliste nõuannete ja abi andmine julgeoleku akrediteerimisasutusele,

— süsteemispetsiifiliste julgeolekunõuete loetelu väljatöötamisele kaasaaitamine,

— süsteemispetsiifiliste julgeolekunõuete loetelu läbivaatamine, et tagada nende vastavus käesolevatele julgeolekueeskirjadele, teabeturbe põhimõtetele ja arhitektuuri käsitlevatele dokumentidele,

— osalemine akrediteerimisrühmades/-kogudes vastavalt vajadusele ja akrediteerimisega seotud teabeturbesoovituste andmine julgeoleku akrediteerimisasutusele,

— teabeturbealase koolitus- ja haridustegevuse toetamine,

— tehniliste nõuannete jagamine teabeturbega seotud vahejuhtumite uurimiseks,

— tehniliste suuniste koostamine selleks, et tagada ainult lubatud tarkvara kasutamine.

INFOTEHNOLOOGIASÜSTEEMI VASTUTAV KÄITAJA (*IT SYSTEM OPERATIONAL AUTHORITY* — ITSOA)

38. Teabeturbeasutus delegeerib vastutuse SÜSTEEMI juhtimise ja eriliste turvaelementide rakendamise ja käitamise eest võimalikult varajases etapis infotehnoloogiasüsteemi vastutavale käitajale. Kõnealune vastutus laieneb kogu SÜSTEEMI elutsüklile alates projekti idee väljatöötamise etapist kuni selle lõpetamiseni.

39. Infotehnoloogiasüsteemi vastutav käitaja vastutab kõigi üldise SÜSTEEMI osaks kavandatud julgeolekumeetmete eest. Selline vastutus hõlmab julgeolekuga seotud töökorra ettevalmistamist. Infotehnoloogiasüsteemi vastutav käitaja täpsustab julgeolekustandardid ja -tavad, mida SÜSTEEMI tarnijad peavad järgima.

40. Infotehnoloogiasüsteemi vastutav käitaja võib vajaduse korral delegeerida osa oma vastutusest näiteks teabeturbe julgeolekuametnikule ja teabeturbe kohalikule julgeolekuametnikule. Teabeturbe eri funktsioone võib täita üks isik.

KASUTAJAD

41. Kõik kasutajad vastutavad selle eest, et nende toimingud ei kahjustaks nende kasutatava SÜSTEEMI julgeolekut.

TEABETURBEALANE KOOLITUS

42. Teabeturbealast haridust ja koolitust pakutakse eri tasemetel ja mitmesuguste töötajate jaoks vastavalt vajadusele peasekretariaadis, Euroopa Liidu detsentraliseeritud asutustes või liikmesriikide valitsusasutustes.

*IV peatükk*

**Mittetehnilised julgeolekumeetmed**

TÖÖTAJATEGA SEOTUD JULGEOLEK

43. Süsteemi kasutajad peavad läbima julgeolekukontrolli ning neil peab olema teadmisvajadus, mis vastab nende konkreetses SÜSTEEMIS käideldava teabe salastatuse tasemele ja sisule. Juurdepääs teatavatele seadmetele või teabele, mis iseloomustavad SÜSTEEMIDE julgeolekut, eeldab seda, et asjaomane isik on nõukogu korra kohaselt läbinud julgeolekukontrolli.

44. Julgeoleku akrediteerimisasutus määrab kindlaks kõik tundlikud ametikohad ja täpsustab neile ametikohtadele asuvate isikute julgeolekukontrolli ja järelevalve taseme.

45. SÜSTEEMID täpsustatakse ja määratakse kindlaks viisil, mis soodustab ülesannete ja vastutuse jagamist töötajate vahel, et välistada olukord, kus kõiki süsteemi julgeoleku võtmeaspekte teaks või kontrolliks täielikult üks isik. Eesmärk peaks olema, et süsteemi või võrgu muutmine või tahtlik rikkumine eeldab vähemalt kahe inimese koostööd.

FÜÜSILINE JULGEOLEK

46. Infotehnoloogiaalad ja terminali-või tööjaamaalad (mis on määratletud punktides 29 ja 30), kus infotehnoloogiavahendite abil käideldakse salastatuse kategooriasse CONFIDENTIEL UE või kõrgemasse kategooriasse kuuluvat teavet või kus on võimalik sellisele teabele juurde pääseda, kinnitatakse vastavalt vajadusele Euroopa Liidu I või II klassi turvaaladeks või siseriikliku süsteemi kohaselt samaväärseteks aladeks.

47. Infotehnoloogiaaladel ning terminali- või tööjaamaaladel, kus on võimalik SÜSTEEMI turvalisust muuta, ei tohi viibida ainult üks volitatud ametnik/muu teenistuja.

SÜSTEEMILE JUURDEPÄÄSU KONTROLLIMINE

48. Kogu teavet ja materjali, mis võimaldavad kontrollida SÜSTEEMILE juurdepääsu, kaitstakse abinõudega, mis vastavad kõrgeimale salastatuse tasemele ja salastatuse teabe kategooriale, millele süsteem juurdepääsu võimaldab.

49. Kui juurdepääsu kontrollimise teavet ja materjali sel otstarbel enam ei kasutata, hävitatakse need punktide 61–63 kohaselt.

*V peatükk*

**Tehnilised julgeolekumeetmed**

TEABETURVE

50. Teabe koostaja on kohustatud kindlaks tegema ja salastama kõik teavet sisaldavad dokumendid olenemata sellest, kas need on paberkoopiad või elektrooniliselt salvestatud. Paberkoopiate kõigi lehekülgede ülemisse ja alumisse serva märgitakse salastatuse kategooria. Olenemata sellest, kas väljund on paberkoopia või elektrooniliselt salvestatud, on selle salastatuse kategooria sama nagu kõrgeima salastatuse kategooriaga teabel, mida dokumendi koostamisel kasutati. Ka SÜSTEEMI kasutamisviis võib mõjutada kõnealuse süsteemi väljundite salastatuse kategooriat.

51. Organisatsioon ja selle teabe valdajad on kohustatud arvesse võtma üksikute teabeelementide koondumisega seotud probleeme ja järeldusi, mida võib teha omavahel seotud elementide põhjal, ning otsustama, kas kogu teabekogumi salastatuse kategooriat tuleks tõsta või ei.

52. Asjaolu, et teave võib olla lühikood, edastuskood või esitatud kahendkujul, ei taga julgeoleku kaitstust ja seega ei tohiks see mõjutada teabe salastatuse kategooriat.

53. Kui teave edastatakse ühest SÜSTEEMIST teise, tuleb teavet edastamise ajal ja vastuvõtvas süsteemis kaitsta viisil, mis oleks vastavuses esialgse salastatuse taseme ja teabe salastatuse kategooriaga.

54. Kõiki elektroonilisi salvestusvahendeid tuleb käsitleda viisil, mis on vastavuses salvestatud teabe kõrgeima salastatuse kategooria või vahendi liigiga, ja alati vastavalt kaitsta.

55. Korduvkasutusega elektroonilistel salvestusvahenditel, mida on kasutatud Euroopa Liidu salastatud teabe salvestamiseks, säilib kõrgeim salastatuse tase, mille jaoks neid on kasutatud, kuni asjaomase teabe salastatuse kategooriat on vajalikul määral alandatud või see on kaotatud ja elektroonilise salvestusvahendi salastatuse taset on vastavalt muudetud, selle salastatuse tase kaotatud või vahend hävitatud korras, mille on heaks kiitnud peasekretariaat või liikmesriik (vt punktid 61–63).

TEABE KONTROLLIMINE JA ARVESTUS

56. Salastatuse kategooriasse SECRET UE ja kõrgemasse kategooriasse kuuluva teabe kasutamise üle peetakse registrit automaatsete (kontrolljälg) või manuaalsete logiraamatute abil. Kõnealuseid registreid säilitatakse käesolevate julgeolekueeskirjade kohaselt.

57. Infotehnoloogiaaladel asuvaid Euroopa Liidu salastatud teabe väljundeid võib käidelda ühe salastatud ühikuna ning neid ei pea registreerima, kui materjal on identifitseeritud, salastatuse kategooriaga tähistatud ja nõuetekohaselt kontrollitud.

58. Kui väljund luuakse Euroopa Liidu salastatud teavet käitlevas SÜSTEEMIS ja edastatakse infotehnoloogiaalalt terminali- või tööjaamaalale, kehtestatakse julgeoleku akrediteerimisasutuse nõusolekul kaugväljundi kontrollimise kord. Salastatuse kategooriasse SECRET UE ja kõrgemasse salastatuse kategooriasse kuuluva teabe korral hõlmab selline kord konkreetseid juhtnööre arvestuse pidamiseks teabe üle.

TEISALDATAVATE ELEKTROONILISTE SALVESTUSVAHENDITE KÄITLEMINE JA KONTROLLIMINE

59. Kõiki teisaldatavaid elektroonilisi salvestusvahendeid, mis kuuluvad salastatuse kategooriasse CONFIDENTIEL UE või rangemasse kategooriasse, käsitatakse materjalina ja nende suhtes kohaldatakse üldisi eeskirju. Vajalikke tunnuseid ja salastatuse kategooriate tähiseid tuleb kohandada konkreetsete salvestusvahendite välimusega, et neid oleks võimalik selgelt ära tunda.

60. Kasutajad vastutavad selle eest, et Euroopa Liidu salastatud teavet säilitatakse vahendite abil, millel on nõuetekohane salastatuse kategooria ja kaitstus. Kehtestatakse kord tagamaks, et kõigisse salastatuse kategooriatesse kuuluvat Euroopa Liidu salastatud teavet säilitatakse elektroonilistel salvestusvahenditel käesolevate julgeolekueeskirjade kohaselt.

ELEKTROONILISTE SALVESTUSVAHENDITE SALASTATUSE KATEGOORIA KAOTAMINE JA HÄVITAMINE

61. Euroopa Liidu salastatud teabe salvestamiseks kasutatud elektrooniliste salvestusvahendite salastatuse kategooriat võib alandada või selle kaotada, kui kohaldatakse korda, mille on heaks kiitnud peasekretariaat või liikmesriik.

62. Kui salvestusvahendeid on kasutatud salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET või erikategooriasse kuuluva teabe säilitamiseks, ei tohi sellise vahendi salastatuse kategooriat kaotada ega vahendit uuesti kasutada.

63. Kui elektroonilise salvestusvahendi salastatuse kategooriat ei saa kaotada või vahendit uuesti kasutada, tuleb vahend hävitada korra kohaselt, mille on heaks kiitnud peasekretariaat või liikmesriik.

SIDETURVE

64. Kui Euroopa Liidu teavet edastatakse elektromagnetiliselt, tuleb sellise edastuse salastatuse, terviklikkuse ja kättesaadavuse kaitsmiseks rakendada erimeetmeid. Julgeoleku akrediteerimisasutus määrab kindlaks nõuded, mille kohaselt kaitstakse edastust avastamise ja pealtkuulamise eest. Sidesüsteemi abil edastatavat teavet kaitstakse salastatuse, terviklikkuse ja kättesaadavuse nõuete kohaselt.

65. Kui salastatuse, terviklikkuse ja kättesaadavuse kaitsmine eeldab krüptograafiameetodite kasutamist, peab julgeoleku akrediteerimisasutus sellised meetodid ja seotud tooted selleks otstarbeks eraldi heaks kiitma.

66. Edastuse ajal kaitstakse salastatuse kategooriasse SECRET UE ja kõrgemasse kategooriasse kuuluvat teavet krüptograafiameetoditega või toodetega, mille nõukogu on nõukogu julgeolekukomitee soovitusel heaks kiitnud. Edastuse ajal kaitstakse salastatuse kategooriatesse CONFIDENTIEL UE ja RESTREINT UE kuuluvat teavet krüptograafiameetoditega või toodetega, mille on heaks kiitnud kas peasekretär/kõrge esindaja nõukogu julgeolekukomitee soovitusel või liikmesriik.

67. Euroopa Liidu salastatud teabe edastamise suhtes kohaldatavad üksikasjalikud eeskirjad sätestatakse julgeoleku erijuhendites, mille nõukogu kiidab heaks julgeolekukomitee soovitusel.

68. Erandolukorras võib salastatuse kategooriatesse RESTREINT UE, CONFIDENTIEL UE ja SECRET UE kuuluvat teavet edastada tavalise tekstina, kuid iga selline juhtum eeldab selgesõnalise loa andmist. Sellised erandolukorrad on järgmised:

a) ähvardav või reaalne kriisi-, konflikti- või sõjaolukord ja

b) kui kohaletoimetamise kiirus on esmatähtis ja krüpteerimisvahendid ei ole kättesaadavad ning leitakse, et edastatavat teavet ei saa kasutada nii ruttu, et see kahjustaks toiminguid.

69. SÜSTEEM peab olema suuteline keelama vajaduse korral juurdepääsu Euroopa Liidu salastatud teabele kõigis tööjaamades ja terminalides kas ühenduse füüsilise katkestamise teel või spetsiaalsete tarkvaravõimaluste abil, mille julgeoleku akrediteerimisasutus on heaks kiitnud.

INSTALLEERIMISE JA KIIRGUSEGA SEOTUD JULGEOLEK

70. SÜSTEEMI esialgse installeerimise ja edaspidise olulise muutmise sätetes peab olema ette nähtud, et süsteemi installeerivad julgeolekukontrolli läbinud isikud tehniliselt pädevate töötajate pideva järelevalve all, kes on läbinud julgeolekukontrolli juurdepääsuks sellisele Euroopa Liidu salastatud teabele, mille salastatuse kategooria on samaväärne kõrgeima salastatuse kategooriaga, millesse kuuluvat teavet kavatsetakse SÜSTEEMIS säilitada ja käidelda.

71. Kõigi seadmed tuleb installeerida nõukogu kehtivate julgeolekueeskirjade kohaselt.

72. Salastatuse kategooriasse CONFIDENTIEL UE või kõrgemasse kategooriasse kuuluva teabe käitlemiseks kasutatavaid SÜSTEEME tuleb kaitsta nii, et nende julgeolekut ei seaks ohtu paljastav kiirgus, mille uurimise ja kontrollimise kohta kasutatakse tähistust "TEMPEST".

73. Peasekretariaadi julgeolekuasutuse määratud TEMPESTi asutus vaatab läbi TEMPESTi vastumeetmed peasekretariaadi ja Euroopa Liidu detsentraliseeritud seadmete jaoks. Euroopa Liidu salastatud teavet käitlevate siseriiklike seadmete puhul on heakskiitvaks asutuseks tunnustatud siseriiklik TEMPESTi heakskiitev asutus.

*VI peatükk*

**Julgeolek käitlemise ajal**

JULGEOLEKUGA SEOTUD TÖÖKORD

74. Julgeolekuga seotud töökord määrab kindlaks julgeolekuküsimustes vastuvõetavad põhimõtted, järgitava töökorra ja töötajate vastutuse. Julgeolekuga seotud töökorra ettevalmistamise eest vastutab infotehnoloogiasüsteemi vastutav käitaja.

TARKVARA KAITSMINE/KONFIGUREERIMISE JUHTIMINE

75. Rakendusprogrammide julgeoleku kaitset ei määrata kindlaks mitte programmi abil töödeldava teabe, vaid programmi enda salastatuse kategooria hindamise põhjal. Kasutatavaid tarkvaraversioone tuleks regulaarselt kontrollida, et tagada nende terviklikkus ja korrektne funktsioneerimine.

76. Tarkvara uusi või muudetud versioone ei tohiks hakata Euroopa Liidu salastatud teabe käitlemiseks kasutama enne, kui infotehnoloogiasüsteemi vastutav käitaja on need üle kontrollinud.

KAHJULIKU TARKVARA/ARVUTIVIIRUSTE KONTROLLIMINE

77. Kahjuliku tarkvara/arvutiviiruste kontrollitakse regulaarselt julgeoleku akrediteerimisasutuse nõuete kohaselt.

78. Kõiki elektroonilisi salvestusvahendeid, mis tuuakse peasekretariaati või Euroopa Liidu detsentraliseeritud asutustesse liikmesriikides, tuleb kontrollida kahjuliku tarkvara ja arvutiviiruste suhtes enne, nende kasutamist SÜSTEEMIS.

HOOLDUS

79. Selliste SÜSTEEMIDE korralise ja erakorralise hoolduse lepingutes ja korras, mille kohta on koostatud süsteemispetsiifiliste julgeolekunõuete loetelu, täpsustatakse infotehnoloogiaalale sisenevatele hooldetöötajatele ja nende seadmetele kehtestatud nõuded ja kord.

80. Nõuded sätestatakse selgelt süsteemispetsiifiliste julgeolekunõuete loetelus ja kord julgeolekuga seotud töökorras. Kaugjuurdepääsu diagnostikameetodeid eeldav lepinguline hooldus on lubatud ainult erandolukorras range julgeolekukontrolli all ja julgeoleku akrediteerimisasutuse nõusolekul.

*VII peatükk*

**Hanked**

81. Kõik SÜSTEEMIS kasutatavad turbetooted, mida kavatsetakse hankida, peavad olema kas hinnatud ja sertifitseeritud või nende hindamine ja sertifitseerimine hindamis- ja sertifitseerimisasutuses rahvusvaheliselt tunnustatud kriteeriumide kohaselt (näiteks infotehnoloogia turvalisuse hindamise ühised kriteeriumid, vt ISO 15 408) peab olema pooleli.

82. Otsustades, kas seadmeid, eriti elektroonilisi salvestusvahendeid, võiks ostmise asemel pigem üürida, tuleks meeles pidada, et pärast seda, kui selliseid seadmeid on kasutatud Euroopa Liidu salastatud teabe käitlemiseks, ei tohi neid lubada nõuetekohase julgeolekuga alast välja, ilma et nende salastatuse kategooria kaotataks julgeoleku akrediteerimisasutuse nõusolekul, ning et sellise nõusoleku saamine ei pruugi alati võimalik olla.

AKREDITEERIMINE

83. Julgeoleku akrediteerimisasutus akrediteerib süsteemispetsiifiliste julgeolekunõuete loetelus, julgeolekuga seotud töökorras ja muudes asjaomastes dokumentides esitatud teabe põhjal kõik SÜSTEEMID, mille jaoks tuleb enne Euroopa Liidu salastatud teabe käitlemist koostada süsteemispetsiifiliste julgeolekunõuete loetelu. Alamsüsteemid ja terminalid/tööjaamad akrediteeritakse selle SÜSTEEMI osana, millega nad on ühendatud. Kui SÜSTEEMI kasutavad peale nõukogu ka muud organisatsioonid, siis lepivad peasekretariaat ja asjaomased julgeolekuasutused akrediteerimises vastastikku kokku.

84. Akrediteerimise protsess võib toimuda akrediteerimisstrateegia kohaselt, mis iseloomustab konkreetset SÜSTEEMI ja mille on määratlenud julgeoleku akrediteerimisasutus.

HINDAMINE JA SERTIFITSEERIMINE

85. Teatavatel juhtudel hinnatakse enne akrediteerimist SÜSTEEMI riistvara, püsivara ja tarkvara turvaelemente ning need sertifitseeritakse, kui nad on suutelised tagama teabe julgeoleku kavandatud salastatuse tasemel.

86. Hindamis- ja sertifitseerimisnõuded peavad sisalduma süsteemi planeerimises ning need peavad olema täpselt sätestatud süsteemispetsiifiliste julgeolekunõuete loetelus.

87. Hindamine ja sertifitseerimine toimub heakskiidetud suuniste kohaselt ning seda teostavad tehnilise kvalifikatsiooniga ja vajalikul tasemel julgeolekukontrolli läbinud töötajad, kes tegutsevad infotehnoloogiasüsteemi vastutava käitaja nimel.

88. Töörühmad võib moodustada nimetatud liikmesriigi hindamis- ja sertifitseerimisasutusest või selle nimetatud esindajatest, näiteks pädevast tööettevõtjast, kes on läbinud julgeolekukontrolli.

89. Asjaomase hindamise ja sertifitseerimise ulatust võib vähendada (näiteks nii, et hõlmatakse ainult integreerimisega seotud aspektid), kui SÜSTEEMID põhinevad olemasolevatel siseriiklikult hinnatud ja sertifitseeritud arvutiturbetoodetel.

TURVAELEMENTIDE KORRALINE KONTROLLIMINE PIDEVAKS AKREDITEERIMISEKS

90. Infotehnoloogiasüsteemi vastutav käitaja kehtestab korralise kontrollimise korra, mis tagab, et kõik SÜSTEEMI turvaelemendid on endiselt kehtivad.

91. Süsteemispetsiifiliste julgeolekunõuete loetelus tuleb selgelt kindlaks teha ja sätestada sellised muudatused, mis eeldavad uut akrediteerimist või julgeoleku akrediteerimisasutuse eelnevat nõusolekut. Pärast igasugust muutmist, parandamist või riket, mis võis mõjutada SÜSTEEMI turvaelemente, tagab infotehnoloogiasüsteemi vastutav käitaja turvaelementide nõuetekohase toimimise kontrollimise. SÜSTEEMI akrediteeringu pikendamine sõltub tavaliselt sellest, kas kontrolli tulemused on rahuldavad.

92. Julgeoleku akrediteerimisasutus kontrollib või vaatab regulaarselt üle kõik SÜSTEEMID, mille puhul on rakendatud turvaelemente. Kui SÜSTEEMI kasutatakse salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluva teabe või lisatähistustega teabe käitlemiseks, kontrollitakse seda vähemalt kord aastas.

*VIII peatükk*

## Ajutine või juhuslik kasutamine

MIKROARVUTITE/PERSONAALARVUTITE TURVALISUS

93. Püsikettaga (või muude alaliste salvestusseadmetega) mikroarvuteid/personaalarvuteid, mis töötavad kas autonoomselt või võrku ühendatuna, ja kaasaskantavaid, püsikõvakettaga arvutiseadmeid (näiteks kaasaskantavad personaalarvutid ja sülearvutid) peetakse samasugusteks teabesalvestusvahenditeks nagu diskette ja muid teisaldatavaid elektroonilisi salvestusvahendeid.

94. Sellistele seadmetele tagatakse seoses nende kasutamise, käitlemise, säilitamise ja transportimisega kaitse, mis vastab nende abil aegade jooksul salvestatud või töödeldud teabe kõrgeimale salastatuse tasemele (kuni salastatuse kategooria vähendamise või kaotamiseni asjaomase korra kohaselt).

ISIKLIKE INFOTEHNOLOOGIASEADMETE KASUTAMINE NÕUKOGU AMETLIKUS TÖÖS

95. Salvestusvõimeliste isiklike teisaldatavate elektrooniliste salvestusvahendite, tarkvara ja infotehnoloogilise riistvara (näiteks personaalarvutite ja kaasaskantavate arvutite) kasutamine Euroopa Liidu salastatud teabe käitlemiseks on keelatud.

96. Isiklikku riistvara, tarkvara ja vahendeid ei või tuua I ja II klassi turvaaladele, kus käideldakse Euroopa Liidu salastatud teavet, kui selleks ei ole peasekretariaadi julgeolekubüroo juhataja või liikmesriigi talituse või vastava Euroopa Liidu detsentraliseeritud asutuse luba.

TÖÖETTEVÕTJATELE KUULUVATE VÕI RIIGI PAKUTUD INFOTEHNOLOOGIASEADMETE KASUTAMINE NÕUKOGU AMETLIKUS TÖÖS

97. Tööettevõtjatele kuuluvate infotehnoloogiaseadmete ja tarkvara kasutamiseks nõukogu ametlikku tööd toetavates organisatsioonides võib anda loa peasekretariaadi julgeolekubüroo, liikmesriigi talituse või vastava Euroopa Liidu detsentraliseeritud asutuse juhataja. Nõukogu peasekretariaadi või Euroopa Liidu detsentraliseeritud asutuse töötajad võivad saada loa kasutada ka riikide pakutud infotehnoloogiaseadmeid ja tarkvara; sellisel juhul kuuluvad infotehnoloogiaseadmed peasekretariaadi kontrolli alla. Kui infotehnoloogiaseadmeid kasutatakse Euroopa Liidu salastatud teabe käitlemiseks, konsulteeritakse asjaomase julgeoleku akrediteerimisasutusega, et kõnealuste seadmete kasutamisel kohaldatavaid teabeturbeelemente võetaks arvesse ja rakendataks nõuetekohaselt.

XII JAGU

## EUROOPA LIIDU SALASTATUD TEABE AVALDAMINE KOLMANDATELE RIIKIDELE JA RAHVUSVAHELISTELE ORGANISATSIOONIDELE

### EUROOPA LIIDU SALASTATUD TEABE AVALDAMIST REGULEERIVAD PÕHIMÕTTED

1. Euroopa Liidu salastatud teabe avaldamise kolmandatele riikidele või rahvusvahelistele organisatsioonidele otsustab nõukogu järgmiste asjaolude põhjal:

   — sellise teabe laad ja sisu,

   — vastuvõtjate teadmisvajadus,

   — Euroopa Liidule toodava kasu ulatus.

   Euroopa Liidu salastatud teabe avaldamiseks küsitakse teabe koostanud liikmesriigi nõusolekut.

2. Sellised otsused tehakse igal üksikjuhul eraldi, võttes arvesse:

   — koostöö soovitavat ulatust asjaomaste kolmandate riikide või rahvusvaheliste organisatsioonidega,

   — nende usaldatavust, mis tuleneb kõnealustele riikidele või organisatsioonidele usaldatava Euroopa Liidu salastatud teabe salastatuse tasemest ja kõnealustes riikides või organisatsioonides kohaldatavate julgeolekueeskirjade vastavusest Euroopa Liidus kohaldatavatele eeskirjadele; nõukogu julgeolekukomitee esitab nõukogule selles küsimuses oma tehnilise seisukoha.

3. Võttes vastu Euroopa Liidu salastatud teabe, kinnitavad kolmandad riigid või rahvusvahelised organisatsioonid, et teavet ei kasutata ühelgi muul eesmärgil kui see, milleks teave avaldati või teavet vahetati, ja et nad tagavad teabe kaitsmise nõukogu nõutaval tasemel.

### TASEMED

4. Kui nõukogu on otsustanud, et salastatud teavet võib konkreetsele riigile või organisatsioonile avaldada või seda nendega vahetada, määrab ta kindlaks võimaliku koostöö taseme. Kõnealune tase sõltub eelkõige asjaomase riigi või organisatsiooni rakendatavatest julgeolekupõhimõtetest ja -eeskirjadest.

5. On olemas kolm koostöö taset:

   1. tase

   Koostöö kolmandate riikide või rahvusvaheliste organisatsioonidega, kelle julgeolekupõhimõtted ja -eeskirjad on väga sarnased Euroopa Liidu omadega.

   2. tase

   Koostöö kolmandate riikide või rahvusvaheliste organisatsioonidega, kelle julgeolekupõhimõtted ja -eeskirjad erinevad Euroopa Liidu omadest märkimisväärselt.

   3. tase

   Episoodiline koostöö kolmandate riikide ja rahvusvaheliste organisatsioonidega, kelle põhimõtteid ja julgeolekueeskirju ei ole võimalik hinnata.

6. Igal koostöö tasemel määratakse kindlaks julgeolekueeskirjad, mille võib konkreetsete juhtumite korral ümber sõnastada, pidades silmas nõukogu julgeolekukomitee tehnilist seisukohta, ja mida teabe saajatel palutakse neile avaldatud salastatud teabe kaitsmisel rakendada. Kõnealune kord ja julgeolekueeskirjad on täpsemalt sätestatud liidetes 4, 5 ja 6.

KOKKULEPPED

7. Kui nõukogu on otsustanud, et vajadus vahetada salastatud teavet Euroopa Liidu ja kolmandate riikide või rahvusvaheliste organisatsioonide vahel on alaline või pikaajaline, koostab ta koos kõnealuste riikide või organisatsioonidega "salastatud teabe vahetamise julgeolekukorra kokkuleppe" ja määratleb selles koostöö eesmärgi ja vahetatava teabe kaitsmise vastastikused eeskirjad.

8. 3. taseme episoodilise koostöö puhul, mis on oma kestuselt ja eesmärgilt piiratud, võib "salastatud teabe vahetamise julgeolekukorra kokkuleppe" asendada vastastikuse mõistmise memorandumiga, milles määratletakse vahetatava salastatud teabe laad ja vastastikused kohustused seoses kõnealuse teabega, kui kõnealune teave kuulub salastatuse kategooriasse RESTREINT UE või madalamasse kategooriasse.

9. Enne kui julgeolekukorra koguleppe või vastastikuse mõistmise memorandumi eelnõu esitatakse seisukoha saamiseks nõukogule, peab julgeolekukomitee selle heaks kiitma.

10. Liikmesriikide julgeolekuasutused abistavad peasekretäri/kõrget esindajat igal võimalikul viisil, et tagada avaldatava teabe kasutamine ja kaitsmine kooskõlas julgeolekukorra kokkuleppe või vastastikuse mõistmise memorandumi sätetega.

*Liide 1*

**Siseriiklike julgeolekuasutuste nimekiri**

BELGIA

Ministère des Affaires Étrangères, du Commerce Extérieur et de la Coopération au Développement
Direction de la sécurité — A 01
Rue des Petits Carmes, 15
B-1000 Bruxelles
Telefon: 32–2–501 85 14
Faks: 32–2–501 80 58
Teleks: 21376
Telegraafiaadress: Direction de Sécurité A01 — MINAFET

TAANI

Politiets Efterretningstjeneste
Borups Alle 266
DK-2400 Copenhagen NV
Telefon: 45-33 14 88 88
Faks: 45-38 19 07 05

Forsvarsministeriet
Forsvarets Efterretningstjeneste
Kastellet 30
DK-2100 Copenhagen Ø
Telefon: 45-33 32 55 66
Faks: 45-33 93 13 20

SAKSAMAA

Bundesministerium des Innern
Referat IS 4
Alt-Moabit 101D
D-10559 Berlin
Telefon: 49–30–39 81 15 28
Faks: 49–30–39 81 16 10

KREEKA

Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Υπηρεσία Στρατιωτικών Πληροφοριών (ΥΣΠ - Β' Κλάδος)
Γραφείο Ασφάλειας
ΣΤΓ 1020-Χολαργός (Αθήνα)
Ελλάδα
Τηλέφωνα: 30–1–655 22 03 (ώρες γραφείου)
30–1–655 22 05 (εικοσιτετράωρο)
Φαξ: 30–1–642 69 40

Hellenic National Defence
General Staff (HNDGS)
Intelligence Branch/Security
(INT. BR./SEC.)
STG 1020, Holargos-Athens
Greece
Telefon: 30–1–655 22 03 (vastuvõtuajal)
30–1–655 22 05 (ööpäevaringselt)
Faks: 30–1–642 69 40

HISPAANIA

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
Carretera Nacional Radial VI, km 8 500
E-28023 Madrid
Telefon: 34–91–372 57 07
Faks: 34–91–372 58 08
E-post: nsa-sp@areatec.com

PRANTSUSMAA

Secrétariat général de la Défense Nationale
Service de Sécurité de Défense (SGDN/SSD)
51 Boulevard de la Tour-Maubourg
F-75700 Paris 07 SP
Telefon: 33–0–144 18 81 80
Faks: 33–0–144 18 82 00
Teleks: SEGEDEFNAT 200019
Telegraafiaadress: SEGEDEFNAT PARIS

IIRIMAA

National Security Authority
Department of Foreign Affairs
80 St. Stephens Green
Dublin 2
Telefon: 353–1–478 08 22
Faks: 353–1–478 14 84

ITAALIA

Presidenza del Consiglio dei Ministri
Autorità Nazionale per la Sicurezza
Ufficio Centrale per la Sicurezza
Via della Pineta Sacchetti, 216
I-00168 Roma
Telefon: 39–06–627 47 75
Faks: 39–06–614 33 97
Teleks: 623876 AQUILA 1
Telegraafiaadress: ess: PCM-ANS-UCSI-ROMA

LUKSEMBURG

Autorité Nationale de Sécurité
Ministère d'État
Boîte Postale 2379
L-1023 Luxembourg
Telefon: 352-478 22 10 keskus
352-478 22 35 otseliin
Faks: 352-478 22 43
352-478 22 71
Teleks: 3481 SERET LU
Telegraafiaadress: MIN D'ETAT — ANS

MADALMAAD

Ministerie van Binnenlandse Zaken
Postbus 20010
NL-2500 EA Den Haag
Telefon: 31–70–320 44 00
Faks: 31–70–320 07 33
Teleks: 32166 SYTH NL

Ministerie van Defensie
Militaire Inlichtingendienst (MID)
Postbus 20701
NL-2500 ES Den Haag
Telefon: 31–70–318 70 60
Faks: 31–70–318 79 51

AUSTRIA

Bundesministerium für auswärtige Angelegenheiten
Abteilung I.9
Ballhausplatz 2
A-1014 Wien
Telefon: 43–1–531 15 34 64
Faks: 43–1–531 8 52 19

PORTUGAL

Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Avenida Ilha da Madeira, 1
P-1449-004 Lisboa
Telefon: 351–21–301 55 10
351–21–301 00 01, sisenumber 20 45 37
Faks: 351–21–302 03 50

SOOME

Alivaltiosihteeri (Hallinto)/Understatssekreteraren (Administration)
Ulkoasiainministeriö/Utrikesministeriet
Laivastokatu/Maringatan 22
PL/PB 176
FIN-00161 Helsinki/Helsingfors
Telefon: 358–9–13 41 53 38
Faks: 358–9–13 41 53 03

ROOTSI

Utrikesdepartementet
SSSB
S-103 39 Stockholm
Telefon: 46–8–405 54 44
Faks: 46–8–723 11 76

ÜHENDKUNINGRIIK

The secretary (for DIR/5)
PO Box 5656
London EC1A 1AH
Telefon: 44–20–72 70 87 51
Faks: 44–20–76 30 14 28
Telegraafiaadress: UK Delegation to Security Policy Dept FCO, tähistusega “in Box 5656 for DIR/5”.

*Liide 2*

**Siseriiklike salastatuse tasemete võrdlus**

| Euroopa Liidu salastatuse tase | Très secret UE/EU Top Secret | Secret UE | Confidentiel UE | Restreint UE |
|---|---|---|---|---|
| NATO salastatuse tase (1) | | | | |
| Lääne-Euroopa Liidu salastatuse tase | Focal Top Secret | WEU Secret | WEU Confidential | WEU Restricted |
| Belgia | Très Secret<br>Zeer Geheim | Secret<br>Geheim | Confidentiel<br>Vertrouwelijk | Diffusion restreinte<br>Beperkte Verspreiding |
| Taani | Yderst hemmeligt | Hemmeligt | Fortroligt | Til tjenestebrug |
| Saksamaa | Streng Geheim | Geheim | VS (2) — Vertraulich | VS — Nur für den Dienstgebrauch |
| Kreeka | Άκρως Απόρρητο | Απόρρητο | Εμπιστευτικό | Περιορισμένης χρήσης |
| Hispaania | Secreto | Reservado | Confidencial | Difusion Limitada |
| Prantsusmaa | Très Secret Défense (3) | Secret Défense | Confidentiel Défense | Diffusion restreinte |
| Iirimaa | Top Secret | Secret | Confidential | Restricted |
| Itaalia | Segretissimo | Segreto | Riservatissimo | Riservato |
| Luksemburg | Très Secret | Secret | Confidentiel | Diffusion restreinte |
| Madalmaad | STG Zeer Geheim | STG Geheim | STG Confidentieel | |
| Austria | Streng Geheim | Geheim | Vertraulich | Eingeschränkt |
| Portugal | Muito Secreto | Secreto | Confidencial | Reservado |
| Soome | Erittäin salainen | Erittäin salainen | Salainen | Luottamuksellinen |
| Rootsi | Kvalificerat hemlig | Hemlig | Hemlig | Hemlig |
| Ühendkuningriik | Top Secret | Secret | Confidential | Restricted |

(1) NATO: vastavus NATO salastatuse tasemetega tehakse kindlaks pärast Euroopa Liidu ja NATO vahelise julgeolekukokkuleppe sõlmimist.

(2) Saksamaa: VS = Verschlusssache.

(3) Prantsusmaa: salastatuse taset "Très Secret Défense", mis hõlmab valitsuse prioriteetseid küsimusi, võib muuta ainult peaministri loal.

*Liide 3*

**Salastatuse kategooriate määramise praktiline juhend**

Käesolev juhend on soovituslik ja selle tõlgendamisega ei tohi muuta II ja III jaos ettenähtud olulisi sätteid.

| Salastatuse tase | Millal | Kes | Tähistus | Salastatuse taseme vähendamine/salastatuse taseme kaotamine/hävitamine | |
|---|---|---|---|---|---|
| | | | | Kes | Millal |
| TRÈS SECRET UE/EU TOP SECRET:<br><br>Sellist kategooriat kasutatakse ainult sellise teabe ja materjali puhul, mille loata avaldamine võib väga tõsiselt kahjustada Euroopa Liidu või ühe või mitme Euroopa Liidu liikmesriigi olulisi huve [II jao punkt 1]. | Kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluvate varade kahjustamine võib:<br><br>— seada otsesesse ohtu Euroopa Liidu või ühe selle liikmesriigi või sõbralike riikide sisemise stabiilsuse<br><br>— tekitada erakordselt tõsist kahju suhetele sõbralike valitsustega<br><br>— põhjustada otseselt hulgaliselt surmajuhtumeid<br><br>— tekitada erakordselt tõsist kahju liikmesriikide töö tulemuslikkusele või julgeolekule või muude osaliste jõududele või eriti väärtuslike julgeoleku- või luureoperatsioonide jätkuvale tõhususele<br><br>— tekitada tõsist pikaajalist kahju Euroopa Liidu või selle liikmesriikide majandusele. | Liikmesriigid:<br><br>nõuetekohase loa saanud isikud (koostajad) [III jao punkt 4];<br><br>peasekretariaat:<br><br>nõuetekohase loa saanud isikud (koostajad) [III jao punkt 4], peasekretär/kõrge esindaja ja peasekretäri asetäitja.<br><br>Dokumentide koostajad määravad kuupäeva või ajavahemiku, mille jooksul võib salastatuse kategooriat alandada või selle kaotada. Kui see ei ole võimalik, vaatavad nad dokumendid hiljemalt iga viie aasta järel läbi, et teha kindlaks, kas esialgne salastatuse kategooria on endiselt vajalik [III jao punkt 10]. | Salastatuse kategooria TRÈS SECRET UE/EU TOP SECRET kantakse salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluvatele dokumentidele ja vajaduse korral kantakse neile mehaaniliselt ja käsitsi kaitsetähistus ESDP [II jao punkt 8].<br><br>Euroopa Liidu salastatuse kategooria nimetus märgitakse iga lehekülje ülemisse ja alumise serva ning kõik lehed nummerdatakse. Igal dokumendil peab olema kirjas viitenumber ja kuupäev; viitenumber tuleb märkida igale lehele.<br><br>Kui dokumente levitatakse mitme koopiana, peab iga koopia esilehel olema kirjas koopia number ja dokumendi lehekülgede arv. Esimesel leheküljel tuleb loetleda kõik lisad ja manustatud materjalid [VII jao punkt 1]. | Salastatuse taset võib alandada või selle kaotada ainult koostaja või peasekretär/kõrge esindaja või peasekretäri asetäitja, kes teatab muudatusest kõigile adressaatidele, kellele dokument või selle koopia saadeti [VIII jao punkt 9].<br><br>Salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluvaid dokumente hävitab nende dokumentide eest vastutav keskregister või alamregister. Iga hävitatud dokumendi kohta koostatakse hävitamisakt, millele kirjutavad alla salastatuse kategooria TRÈS SECRET UE/EU TOP SECRET kontrolliametnik ja hävitamist tunnistama kutsutud ametnik, kes peab olema läbinud julgeolekukontrolli salastatuse kategooria TRÈS SECRET UE/EU TOP SECRET jaoks. Logiraamatusse tehakse vastav märkus. Register säilitab hävitamisakte koos ringkäigulehega kümme aastat [VII jao punkt 31]. | Ülejäänud koopiad ja dokumendid, mida enam ei vajata, tuleb hävitada [VII jao punkt 31].<br><br>Salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluvad dokumendid, kaasa arvatud salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluvate dokumentide koostamise käigus tekkinud salastatud jäätmed (näiteks vigased koopiad, mustandid, trükitud märkmed ja koopiapaber) hävitatakse salastatuse kategooria TRÈS SECRET UE/EU TOP SECRET ametniku järelevalve all kas põletamise, paberimassiks muutmise või narmastamise teel või muutes need muul viisil loetamatuks nii, et neid ei ole võimalik enam kokku panna. |

| Salastatuse tase | Millal | Kes | Tähistus | Salastatuse taseme vähendamine/salastatuse taseme kaotamine/hävitamine | |
|---|---|---|---|---|---|
| | | | | Kes | Millal |
| SECRET:<br><br>Sellist kategooriat kasutatakse ainult sellise teabe ja materjali puhul, mille loata avaldamine võib tõsiselt kahjustada Euroopa Liidu või ühe või mitme Euroopa Liidu liikmesriigi olulisi huve [II jao punkt 2]. | Kategooriasse SECRET UE kuuluvate varade kahjustamine võib:<br><br>— tekitada rahvusvahelisi pingeid<br><br>— kahjustada tõsiselt suhteid sõbralike valitsustega<br><br>— seada otseselt ohtu elu või kahjustada tõsiselt avalikku korda või üksikisikute julgeolekut või vabadust<br><br>— tekitada tõsist kahju liikmesriikide töö tulemuslikkusele või julgeolekule või muude osaliste jõududele või väga väärtuslike julgeoleku- või luureoperatsioonide jätkuvale tõhususele<br><br>— tekitada märkimisväärset materiaalset kahju Euroopa Liidu või ühe tema liikmesriigi finants-, monetaar-, majandus- ja kaubandushuvidele. | Liikmesriigid:<br><br>volitatud isikud (koostajad) [III jao punkt 2];<br><br>peasekretariaat ja Euroopa Liidu detsentraliseeritud asutused:<br><br>nõuetekohase loa saanud isikud (koostajad) [III jao punkt 2], peadirektorid, peasekretär/kõrge esindaja ja peasekretäri asetäitja.<br><br>Dokumentide koostajad määravad kuupäeva või ajavahemiku, mille jooksul võib salastatuse kategooriat alandada või selle kaotada. Kui see ei ole võimalik, vaatavad nad dokumendid hiljemalt iga viie aasta järel läbi, et teha kindlaks, kas esialgne salastatuse kategooria on endiselt vajalik [VII jao punkt 1]. | Salastatuse kategooria SECRET UE kantakse salastatuse kategooriasse SECRET UE kuuluvatele dokumentidele ja vajaduse korral kantakse neile mehaaniliselt ja käsitsi kaitsetähistus ESDP [III jao punkt 8].<br><br>Euroopa Liidu salastatuse kategooria nimetus märgitakse iga lehekülje ülemisse ja alumise serva ning kõik lehed nummerdatakse. Igal dokumendil peab olema kirjas viitenumber ja kuupäev; viitenumber tuleb märkida igale lehele.<br><br>Kui dokumente levitatakse mitme koopiana, peab iga koopia esilehel olema kirjas koopia number ja dokumendi lehekülgede arv. Esimesel leheküljel tuleb loetleda kõik lisad ja manustatud materjalid [VII jao punkt 1]. | Salastatuse taset võib vähendada või selle kaotada ainult koostaja või peasekretär/kõrge esindaja või peasekretäri asetäitja, kes teatab muudatusest kõigile adressaatidele, kellele dokument või selle koopia saadeti [VII jao punkt 9].<br><br>Salastatuse kategooriasse SECRET UE kuuluvaid dokumente hävitab nende dokumentide eest vastutav register sellise isiku järelevalve all, kes on läbinud julgeolekukontrolli. Salastatuse kategooriasse SECRET UE kuuluvate hävitatud dokumentide loetelu kantakse allakirjutatud hävitamisaktile, mida register säilitab koos hävitamislehtedega vähemalt kolm aastat [VII jao punkt 32]. | Ülejäänud koopiad ja dokumendid, mida enam ei vajata, tuleb hävitada [VII jao punkt 31].<br><br>Salastatuse kategooriasse SECRET UE kuuluvad dokumendid, kaasa arvatud kõik salastatuse kategooriasse SECRET UE kuuluvate dokumentide koostamise käigus tekkinud salastatud jäätmed (näiteks vigased koopiad, mustandid, trükitud märkmed ja koopiapaber) hävitatakse kas põletamise, paberimassiks muutmise või narmastamise teel või muutes need muul moel loetamatuks selliselt, et neid ei ole võimalik enam kokku panna [VII jao punktid 31 ja 32]. |

| Salastatuse tase | Millal | Kes | Tähistus | Salastatuse taseme vähendamine/salastatuse taseme kaotamine/hävitamine | |
|---|---|---|---|---|---|
| | | | | Kes | Millal |
| CONFIDENTIEL UE:<br><br>Sellist kategooriat kasutatakse sellise teabe ja materjali puhul, mille loata avaldamine võib kahjustada Euroopa Liidu või ühe või mitme Euroopa Liidu liikmesriigi olulisi huve [II jao punkt 3]. | Kategooriasse CONFIDENTIEL UE kuuluvate varade kahjustamine võib:<br><br>— kahjustada oluliselt diplomaatilisi suhteid, st anda alust ametlikuks protestiks või muudeks sanktsioonideks<br><br>— piirata üksikisikute julgeolekut või vabadust<br><br>— tekitada kahju liikmesriikide töö tulemuslikkusele või julgeolekule või muude osaliste jõududele või väärtuslike julgeoleku- või luureoperatsioonide tõhususele<br><br>— õõnestada märkimisväärselt suurorganisatsioonide rahalist elujõudu<br><br>— takistada raskete kuritegude uurimist või soodustada nende toimepanekut<br><br>— olla märkimisväärses vastuolus Euroopa Liidu või selle liikmesriikide finants-, monetaar-, majandus- ja kaubandushuvidega<br><br>— takistada tõsiselt Euroopa Liidu oluliste põhimõtete väljatöötamist või toimimist<br><br>— peatada või muul viisil märkimisväärselt häirida olulisi Euroopa Liidu toiminguid. | Liikmesriigid:<br><br>volitatud isikud (koostajad) [III jao punkt 2];<br><br>peasekretariaat ja Euroopa Liidu detsentraliseeritud asutused:<br><br>nõuetekohase loa saanud isikud (koostajad) [III jao punkt 2], peadirektorid, peasekretär/kõrge esindaja ja peasekretäri asetäitja.<br><br>Dokumentide koostajad määravad kuupäeva või ajavahemiku, mille jooksul võib salastatuse kategooriat alandada või selle kaotada. Kui see ei ole võimalik, vaatavad nad dokumendid hiljemalt iga viie aasta järel läbi, et teha kindlaks, kas esialgne salastatuse kategooria on endiselt vajalik [III jao punkt 10]. | Salastatuse kategooria CONFIDENTIEL UE kantakse salastatuse kategooriasse CONFIDENTIEL UE kuuluvatele dokumentidele ja vajaduse korral kantakse neile kaitsetähistus ESDP mehaaniliselt ja käsitsi või trükkides eelnevalt tembeldatud ja registreeritud paberile [II jao punkt 8].<br><br>Euroopa Liidu salastatuse kategooria nimetus märgitakse iga lehekülje ülemisse ja alumise serva ning kõik lehed nummerdatakse. Igal dokumendil peab olema kirjas viitenumber ja kuupäev.<br><br>Esimesel leheküljel tuleb loetleda kõik lisad ja manustatud materjalid [VII jao punkt 1]. | Salastatuse taset võib alandada või selle kaotada ainult koostaja või peasekretär/kõrge esindaja või peasekretäri asetäitja, kes teatab muudatusest kõigile adressaatidele, kellele dokument või selle koopia saadeti [VII jao punkt 31].<br><br>Salastatuse kategooriasse CONFIDENTIEL UE kuuluvaid dokumente hävitab nende dokumentide eest vastutav register sellise isiku järelevalve all, kes on läbinud julgeolekukontrolli. Nende hävitamine dokumenteeritakse siseriiklike õigusnormide kohaselt ning peasekretariaadi ja Euroopa Liidu detsentraliseeritud asutuste puhul peasekretäri/kõrge esindaja või peasekretäri asetäitja juhtnööride kohaselt [VII jao punkt 33]. | Ülejäänud koopiad ja dokumendid, mida enam ei vajata, tuleb hävitada [VII jao punkt 31].<br><br>Salastatuse kategooriasse CONFIDENTIEL UE kuuluvad dokumendid, kaasa arvatud kõik salastatuse kategooriasse CONFIDENTIEL UE kuuluvate dokumentide koostamise käigus tekkinud salastatud jäätmed (näiteks vigased koopiad, mustandid, trükitud märkmed ja koopiapaber) hävitatakse kas põletamise, paberimassiks muutmise või narmastamise teel või muutes need muul moel loetamatuks selliselt, et neid ei ole võimalik enam kokku panna [VII jao punktid 31 ja 33]. |

| Salastatuse tase | Millal | Kes | Tähistus | Salastatuse taseme vähendamine/salastatuse taseme kaotamine/hävitamine | |
|---|---|---|---|---|---|
| | | | | Kes | Millal |
| RESTREINT UE:<br><br>Sellist kategooriat kasutatakse sellise teabe ja materjali puhul, mille loata avaldamine võib negatiivselt mõjutada Euroopa Liidu või ühe või mitme Euroopa Liidu liikmesriigi huve [II jao punkt 4]. | Kategooriasse RESTREINT UE kuuluvate varade kahjustamine võib:<br><br>— kahjustada diplomaatilisi suhteid<br><br>— tekitada üksikisikutele märkimisväärseid ebameeldivusi<br><br>— raskendada liikmesriikide või muude osaliste jõudude töö tulemuslikkuse või julgeoleku säilitamist<br><br>— tekitada üksikisikutele või ettevõtetele finantskahju või soodustada sobimatu kasu või edu saamist<br><br>— rikkuda nõuetekohaseid kohustusi säilitada kolmandate isikute avaldatud teabe salajasus<br><br>— rikkuda õiguspäraseid piiranguid teabe avaldamise kohta<br><br>— piirata kuritegude uurimist või soodustada nende toimepanekut<br><br>— seada Euroopa Liidu või selle liikmesriigid ebasoodsasse olukorda kolmandate isikutega toimuvatel kaubanduslikel või poliitilistel läbirääkimistel<br><br>— takistada Euroopa Liidu oluliste põhimõtete tulemuslikku väljatöötamist või toimimist<br><br>— õõnestada Euroopa Liidu ja selle toimingute nõuetekohast juhtimist. | Liikmesriigid:<br><br>volitatud isikud (koostajad) [III jao punkt 2];<br><br>peasekretariaat ja Euroopa Liidu detsentraliseeritud asutused:<br><br>nõuetekohase loa saanud isikud (koostajad) [III jao punkt 2], peadirektorid, peasekretär/kõrge esindaja ja peasekretäri asetäitja.<br><br>Dokumentide koostajad määravad kuupäeva või ajavahemiku, mille jooksul võib salastatuse kategooriat alandada või selle kaotada. Kui see ei ole võimalik, vaatavad nad dokumendid hiljemalt iga viie aasta järel läbi, et teha kindlaks, kas esialgne salastatuse kategooria on endiselt vajalik [III jao punkt 10]. | Salastatuse kategooria RESTREINT UE kantakse salastatuse kategooriasse RESTREINT UE kuuluvatele dokumentidele ja vajaduse korral kantakse neile mehaanilisel või elektroonilisel teel kaitsetähistus ESDP [II jao punkt 8].<br><br>Euroopa Liidu salastatuse kategooria nimetus märgitakse iga lehekülje ülemisse ja alumise serva ning kõik lehed nummerdatakse. Igal dokumendil peab olema kirjas viitenumber ja kuupäev [VII jao punkt 1]. | Salastatuse taset võib alandada või selle kaotada ainult koostaja või peasekretär/kõrge esindaja või peasekretäri asetäitja, kes teatab muudatusest kõigile adressaatidele, kellele dokument või selle koopia saadeti [III jao punkt 9].<br><br>Salastatuse kategooriasse RESTREINT UE kuuluvaid dokumente hävitab nende eest vastutav register siseriiklike õigusnormide kohaselt ning peasekretariaadi ja Euroopa Liidu detsentraliseeritud asutuste puhul peasekretäri/kõrge esindaja või peasekretäri asetäitja juhtnööride kohaselt [VII jao punkt 34]. | Ülejäänud koopiad ja dokumendid, mida enam ei vajata, tuleb hävitada [VII jao punkt 31]. |

*Liide 4*

**Juhtnöörid Euroopa Liidu salastatud teabe avaldamiseks kolmandatele riikidele või rahvusvahelistele organisatsioonidele**

1. taseme koostöö

MENETLUSED

1. Nõukogu on volitatud avaldama Euroopa Liidu salastatud teavet riikidele, kes ei ole kirjutanud alla Euroopa Liidu lepingule, ja muudele rahvusvahelistele organisatsioonidele, mille julgeolekupõhimõtted ja -eeskirjad on võrreldavad Euroopa Liidu omadega.

2. Nõukogu võib salastatud teabe avaldamise otsuse delegeerida. Delegeerimises tuleb märkida avaldatava teabe laad ja salastatuse tase, mis ei tohiks üldjuhul olla kõrgem kui CONFIDENTIEL UE.

3. Kui sõlmitavas julgeolekukokkuleppes ei sätestata teisiti, peavad asjaomaste riikide või rahvusvaheliste organisatsioonide julgeolekuorganid esitama Euroopa Liidu salastatud teabe avaldamise taotluse peasekretärile/kõrgele esindajale ja täpsustama taotluses eesmärgid, milleks salastatud teavet on vaja, ja avaldatava salastatud teabe laadi.

   Soovi korral võib Euroopa Liidu salastatud teabe avaldamise taotluse esitada ka liikmesriik või Euroopa Liidu detsentraliseeritud asutus; sellises taotluses tuleb märkida sellise teabe avaldamise eesmärk ja sellest Euroopa Liidule tulenev kasu ning täpsustada avaldatava teabe laad ja salastatuse kategooria.

4. Taotluse vaatab läbi peasekretariaat, kes:

   — küsib avaldatava teabe koostanud liikmesriigi või vajaduse korral Euroopa Liidu detsentraliseeritud asutuse seisukohta,

   — loob vajalikud sidemed julgeolekuorganitega taotluse esitanud riikides või rahvusvahelistes organisatsioonides, et kontrollida, kas nende julgeolekupõhimõtted ja -eeskirjad on sellised, mis tagaksid avaldatava salastatud teabe kaitsmise käesolevate julgeolekueeskirjade kohaselt,

   — küsivad liikmesriikide siseriiklike julgeolekuasutuste tehnilisi seisukohti selle kohta, kui usaldusväärsed on teavet kasutada soovivad riigid või rahvusvahelised organisatsioonid.

5. Peasekretariaat edastab taotluse ja julgeolekubüroode soovitused otsuse saamiseks nõukogule.

JULGEOLEKUEESKIRJAD, MIDA PEAVAD KOHALDAMA TEABESAAJAD

6. Peasekretär/kõrge esindaja teatab teabesaajatele riikidele või rahvusvahelistele organisatsioonidele nõukogu otsusest lubada avaldada Euroopa Liidu salastatud teavet ja edastab vajalikul hulgal käesolevate julgeolekueeskirjade koopiaid. Kui taotluse esitas liikmesriik, teatab kõnealune riik teabesaajat avaldamise lubamisest.

   Avaldamise otsus jõustub ainult juhul, kui teabesaajad kinnitavad kirjalikult, et nad:

   — kasutavad teavet ainult kokkulepitud eesmärgil,

   — kaitsevad teavet käesolevate julgeolekueeskirjade ja eelkõige allpool esitatud erisätete kohaselt.

7. *Töötajad*

   a) Euroopa Liidu salastatud teabele juurdepääsu omavate ametnike hulk peab teadmisvajaduse põhimõttest lähtuvalt olema rangelt piiratud nende isikutega, kelle tööülesanded eeldavad sellist juurdepääsu.

b) Kõigil ametnikel ja kodanikel, kellel on luba juurdepääsuks salastatuse kategooriasse CONFIDENTIEL UE või rangemasse salastatuse kategooriasse kuuluvale teabele, peab olema kas vastava taseme julgeolekusertifikaat või nad peavad olema läbinud vastava taseme julgeolekukontrolli, kusjuures mõlemaga tegeleb asjaomase isiku oma riigi valitsus.

8. *Dokumentide edastamine*

a) Dokumentide edastamise praktiline kord otsustatakse kokkuleppe kohaselt nõukogu julgeolekueeskirjade VII jao põhjal. Eelkõige nimetatakse selles registrid, millesse Euroopa Liidu salastatud teave tuleb edastada.

b) Kui teabe hulka, mille avaldamiseks nõukogu on loa andnud, kuulub ka salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluvat teavet, loob teabesaaja riik või rahvusvaheline organisatsioon keskregistri Euroopa Liidu küsimuste jaoks ja vajaduse korral ka alamregistrid. Kõnealuste registrite suhtes kohaldatakse käeolevate julgeolekueeskirjade VIII jao sätteid.

9. *Registreerimine*

Niipea kui register saab Euroopa Liidu dokumendi, mis kuulub salastatuse kategooriasse CONFIDENTIEL UE või kõrgemasse salastatuse kategooriasse, teeb ta selle dokumendi kohta kande organisatsiooni peetavasse eriregistrisse, milles on eraldi veerud kättesaamiskuupäeva, dokumenti iseloomustavate andmete (kuupäev, viitenumber ja koopia number), salastatuse kategooria, pealkirja, saaja nime või ametinimetuse ja vastuvõtmistõendi tagastamiskuupäeva jaoks ning kuupäeva jaoks, mil dokument tagastatakse Euroopa Liiduga seotud koostajale või hävitatakse.

10. *Hävitamine*

a) Euroopa Liidu salastatud dokumendid hävitatakse käesolevate julgeolekueeskirjade VI jaos sätestatud juhtnööride kohaselt. Salastatuse kategooriatesse SECRET UE ja TRÈS SECRET UE/EU TOP SECRET kuuluvate dokumentide hävitamisaktide koopiad saadetakse sellele Euroopa Liidu registrile, kes dokumendid edastas.

b) Euroopa Liidu salastatud dokumendid hõlmatakse teabesaaja enda salastatud dokumentide hädaolukorras hävitamise kavasse.

11. *Dokumentide kaitsmine*

Võetakse kõik meetmed, et välistada volitamata isikute juurdepääs Euroopa Liidu salastatud teabele.

12. *Koopiad, tõlked ja väljavõtted*

Salastatuse kategooriatesse CONFIDENTIEL UE ja SECRET UE kuuluvatest dokumentidest ei tohi teha koopiaid, neid ei tohi tõlkida ega neist väljavõtteid teha ilma asjaomase julgeolekuorganisatsiooni juhi loata; kõnealune juht registreerib need koopiad, tõlked või väljavõtted, kontrollib need ja lööb neile vajaduse korral templi.

Salastatuse kategooriasse TRÈS SECRET UE/EU TOP SECRET kuuluvate dokumentide paljundamine ja tõlkimine on lubatud ainult juhul, kui selleks on andnud loa dokumendi koostaja, kes täpsustab lubatud koopiate arvu; kui dokumendi koostanud asutust või ametiisikut ei ole võimalik kindlaks teha, saadetakse taotlus edasi peasekretariaadi julgeolekubüroosse.

13. *Julgeoleku rikkumine*

Kui julgeolekut on rikutud või kui kahtlustatakse sellist rikkumist seoses Euroopa Liidu salastatud dokumendiga, tuleb julgeolekukokkuleppe sõlmimist arvestades võtta viivitamata järgmised meetmed:

a) korraldada uurimine, et teha kindlaks julgeoleku rikkumise asjaolud;

b) teatada sellest peasekretariaadi julgeolekubüroole, siseriiklikule julgeolekuasutusele ja dokumendi koostanud asutusele või ametiisikule, või kui viimasena nimetatut ei ole teavitatud, siis selgelt teatada, et seda ei ole tehtud;

c) võtta meetmeid julgeoleku rikkumise tagajärgede minimeerimiseks;

d) vaadata läbi ja rakendada meetmed, et välistada samasuguse sündmuse kordumine;

e) rakendada peasekretariaadi julgeolekubüroo soovitatud meetmeid, et välistada samasuguse sündmuse kordumine.

14. *Kontrollimine*

Kokkuleppel asjaomaste riikide või rahvusvaheliste organisatsioonidega on peasekretariaadi julgeolekubürool lubatud hinnata avaldatud Euroopa Liidu salastatud teabe kaitsmise meetmete tõhusust.

15. *Aruandlus*

Julgeolekukokkuleppe sõlmimist arvestades peab riik või rahvusvaheline organisatsioon, kelle valduses on Euroopa Liidu salastatud teave, esitama kord aastas kuupäevaks, mis sätestatakse siis, kui antakse luba teabe avaldamiseks, aruande käesolevate julgeolekueeskirjade täitmise kohta.

*Liide 5*

**Juhtnöörid Euroopa Liidu salastatud teabe avaldamiseks kolmandatele riikidele või rahvusvahelistele organisatsioonidele**

2. taseme koostöö

MENETLUSED

1. Nõukogu on volitatud avaldama Euroopa Liidu salastatud teavet kolmandatele riikidele ja rahvusvahelistele organisatsioonidele, mille julgeolekupõhimõtted ja -eeskirjad erinevad märkimisväärselt Euroopa Liidu omadest. Põhimõtteliselt on tegemist teabega, mis kuulub salastatuse kategooriasse SECRET UE või madalamasse salastatuse kategooriasse; selle hulka ei kuulu spetsiaalselt liikmesriikidele mõeldud siseriiklik teave ja eritähistusega kaitstud kategooriatesse kuuluv Euroopa Liidu salastatud teabe.

2. Nõukogu võib otsuse delegeerida: delegeerimise puhul teatab ta punktis 1 osutatud piires avaldada lubatud teabe laadi ja salastatuse kategooria, mis ei või olla kõrgem kui RESTREINT UE.

3. Kui sõlmitavas julgeolekukokkuleppes ei sätestata teisiti, peavad asjaomaste riikide või rahvusvaheliste organisatsioonide julgeolekuorganid esitama Euroopa Liidu salastatud teabe avaldamise taotluse peasekretärile/kõrgele esindajale ja täpsustama taotluses eesmärgid, milleks salastatud teavet on vaja, ning avaldatava teabe laadi ja salastatuse kategooria.

   Soovi korral võib Euroopa Liidu salastatud teabe avaldamise taotluse esitada ka liikmesriik või Euroopa Liidu detsentraliseeritud asutus; sellises taotluses tuleb märkida sellise teabe avaldamise eesmärk ja sellest Euroopa Liidule tulenev kasu ning täpsustada avaldatava teabe laad ja salastatuse kategooria.

4. Taotluse vaatab läbi peasekretariaat, kes:

   — küsib avaldatava teabe koostanud liikmesriigi või vajaduse korral Euroopa Liidu detsentraliseeritud asutuse seisukohta,

   — loob esialgsed sidemed teabesaajate riikide või rahvusvaheliste organisatsioonide julgeolekuasutustega, et saada teavet nende julgeolekupõhimõtete ja -eeskirjade kohta ja eelkõige selleks, et koostada tabel võrdlemaks Euroopa Liidus kasutatavaid salastatuse kategooriaid asjaomases riigis või rahvusvahelises organisatsioonis kasutatavatega,

   — korraldab nõukogu julgeolekukomitee koosoleku või küsitleb, vajaduse korral vaikiva menetluse alusel, liikmesriikide siseriiklikke julgeolekuasutusi, et koostada julgeolekukomitee tehniline seisukoht.

5. Nõukogu julgeolekukomitee tehniline seisukoht käsitleb järgmisi küsimusi:

   — teabesaajate riikide või rahvusvaheliste organisatsioonide usaldatavus, et hinnata Euroopa Liidule või selle liikmesriikidele tulenevaid julgeolekuriske,

   — hinnang selle kohta, kuivõrd teabesaajad suudavad kaitsta Euroopa Liidu avaldatud salastatud teavet,

   — ettepanekud Euroopa Liidu salastatud teabe käitlemise (näiteks selliste versioonide koostamine, millest on teatavad osad välja jäetud) ja dokumentide edastamise (Euroopa Liidu salastatuse kategooria märgete säilitamine või kustutamine, eritähised jne) praktilise korra kohta,

   — dokumentide salastatuse kategooria vähendamine või kaotamine dokumendi koostanud asutuse või ametiisiku poolt enne, kui dokument avaldatakse teabesaajale riigile või rahvusvahelisele organisatsioonile. ([1])

([1]) Sel juhul peab dokumendi koostanud asutus või ametiisik rakendama III jao punktis 9 määratletud korda kõigi Euroopa Liidus ringlevate koopiate suhtes.

6. Peasekretär/kõrge esindaja edastab nõukogule otsuse saamiseks taotluse ja peasekretariaadi julgeolekubüroole esitatud nõukogu julgeolekukomitee tehnilise seisukoha.

JULGEOLEKUEESKIRJAD, MIDA PEAVAD KOHALDAMA TEABESAAJAD

7. Peasekretär/kõrge esindaja teatab teabesaajatele riikidele või rahvusvahelistele organisatsioonidele nõukogu otsusest lubada avaldada Euroopa Liidu salastatud teavet ja edastab samal ajal tabeli, milles võrreldakse Euroopa Liidus ja asjaomastes riikides või organisatsioonides kasutatavaid salastatuse kategooriaid. Kui taotluse esitas liikmesriik, teatab kõnealune riik teabesaajat avaldamise lubamisest.

Avaldamise otsus jõustub ainult juhul, kui teabesaajad kinnitavad kirjalikult, et nad:

— kasutavad teavet ainult kokkulepitud eesmärgil,

— kaitsevad teavet nõukogu kehtestatud eeskirjade kohaselt.

8. Kui nõukogu ei otsusta pärast nõukogu julgeolekukomitee tehnilise seisukoha saamist kehtestada Euroopa Liidu salastatud dokumentide käitlemiseks (Euroopa Liidu salastatuse kategooria märke kustutamine, eritähised jne) erikorda, kehtestatakse kaitse kohta järgmised eeskirjad.

Sellisel juhul eeskirju kohandatakse.

9. *Töötajad*

a) Euroopa Liidu salastatud teabele juurdepääsu omavate ametnike hulk peab teadmisvajaduse põhimõttest lähtuvalt olema rangelt piiratud nende isikutega, kelle tööülesanded eeldavad sellist juurdepääsu.

b) Kõik ametnikud ja kodanikud, kellel on luba juurdepääsuks Euroopa Liidu avaldatud salastatud teabele, peavad olema läbinud siseriikliku julgeolekukontrolli või siseriikliku salastatud teabe puhul peab neil olema luba juurdepääsuks sellisesse salastatuse kategooriasse kuuluvale teabele, mis on vastavalt võrdlustabelile samaväärne asjaomase Euroopa Liidu omaga.

c) Kõnealused siseriiklikud julgeolekusertifikaadid või load tuleb edastada teadmiseks peasekretärile/kõrgele esindajale.

10. *Dokumentide edastamine*

a) Dokumentide edastamise praktilises korras lepivad kokku peasekretariaadi julgeolekubüroo ja teabesaajate riikide või rahvusvaheliste organisatsioonide julgeolekuasutused käesolevate eeskirjade VII jaos sätestatud reeglite kohaselt. Eelkõige nimetatakse täpne aadress, kuhu dokumendid tuleb edastada, ning Euroopa Liidu salastatud teabe edastamiseks kasutatav kuller- või postiteenistus.

b) Salastatuse kategooriasse CONFIDENTIEL UE ja kõrgemasse salastatuse kategooriasse kuuluvad dokumendid edastatakse kahekordses ümbrikus. Sisemisele ümbrikule tuleb märkida tähed "UE" ja salastatuse kategooria. Iga salastatud dokumendi kohta lisatakse kättesaamistõendi vorm. Kättesaamistõendi vormil, mis ei ole salastatud, märgitakse dokumendi kohta ainult teatavad andmed (viitenumber, kuupäev, koopia number) ja keel, milles dokument on koostatud, mitte aga dokumendi pealkirja.

c) Seejärel pannakse sisemine ümbrik välimisse ümbrikku, millel on arvepidamiseks kirjas paki number. Välimisele ümbrikule salastatuse kategooriat ei märgita.

d) Kullerile antakse alati kättesaamiskinnitus, millel on kirjas paki number.

11. *Registreerimine saabumisel*

Adressaatriigi julgeolekuasutus või sellega samaväärne asutus riigis, mis võtab Euroopa Liidu edastatud salastatud teabe vastu oma valitsuse nimel, või vastuvõtva rahvusvahelise organisatsiooni julgeolekubüroo avab eraldi registri, et registreerida Euroopa Liidu salastatud teave selle saabumisel. Registris on veerud saabumiskuupäeva, dokumendi andmete (kuupäev, viitenumber ja koopia number), salastatuse kategooria, pealkirja, adressaadi nime või ametinimetuse ja vastuvõtmistõendi tagastamiskuupäeva jaoks ning kuupäeva jaoks, mil dokument tagastatakse Euroopa Liidule või hävitatakse.

12. *Dokumentide tagastamine*

Kui saaja tagastab salastatud dokumendi nõukogule või dokumendi välja andnud liikmesriigile, tegutseb ta punktis 10 sätestatud korras.

13. *Kaitse*

a) Kui dokumente ei kasutata, hoitakse neid turvakonteineris, mis on heaks kiidetud sama kategooria siseriiklike salastatud materjalide säilitamiseks. Turvakonteineril ei ole mingit märget selle kohta, mida ta sisaldab, ning konteineri sisule pääsevad juurde ainult isikud, kellel on Euroopa Liidu salastatud teabe käitlemise luba. Kui kasutatakse kombinatsioonlukke, võivad luku kombinatsiooni teada ainult need riigi või organisatsiooni ametnikud, kellel on luba juurdepääsuks Euroopa Liidu salastatud teabele, mida konteineris säilitatakse, ning kombinatsioone muudetakse kord kuue kuu jooksul või sagedamini, kui ametnik viiakse üle teisele ametikohale, kui tühistatakse ühe kombinatsiooni teadva ametniku julgeolekusertifikaat või kui on julgeoleku ohustamise risk.

b) Euroopa Liidu salastatud dokumente võivad turvakonteinerist võtta ainult need ametnikud, kes on läbinud julgeolekukontrolli Euroopa Liidu salastatud dokumentide jaoks ja kellel on teadmisvajadus. Kuni dokumendid on nende valduses, vastutavad need isikud kõnealuste dokumentide turvalise säilitamise eest ja eelkõige selle eest, et dokumentidele ei pääseks ligi selleks volitamata isikud. Need isikud tagavad ka, et dokumente hoitakse turvakonteineris, kui nad on lõpetanud töö dokumentidega, samuti väljaspool tööaega.

c) Salastatuse kategooriasse CONFIDENTIEL UE ja kõrgemasse kategooriasse kuuluvatest dokumentidest võib teha koopiaid ja väljavõtteid ainult peasekretariaadi julgeolekubüroo loal.

d) Tuleks määratleda dokumentide kiire ja täieliku hävitamise kord hädaolukorras ning selle korra peaks kinnitama peasekretariaadi julgeolekubüroo.

14. *Füüsiline julgeolek*

a) Kui Euroopa Liidu salastatud dokumentide säilitamiseks kasutatavaid turvakonteinereid ei kasutata, peavad need olema alati lukustatud.

b) Kui hoolduspersonal või koristajad peavad sisenema ruumi, kus on sellised turvakonteinerid, või töötama sellises ruumis, saadab neid alati riigi või organisatsiooni julgeolekuteenistuse liige või selle ruumi julgeoleku eest vastutav ametnik.

c) Väljaspool tavapärast tööaega (öösiti, nädalavahetustel ja riigipühadel) kaitseb Euroopa Liidu salastatud dokumente sisaldavaid turvakonteinereid kas valvur või automaatne häiresüsteem.

15. *Julgeoleku rikkumine*

Kui on rikutud julgeolekut või kui kahtlustatakse sellist rikkumist seoses Euroopa Liidu salastatud dokumendiga, tuleb viivitamata võtta järgmised meetmed:

a) edastada viivitamata aruanne peasekretariaadi julgeolekubüroole või liikmesriigi siseriiklikule julgeolekuasutusele, kes tegeleb dokumentide edastamisega (koos koopiaga peasekretariaadi julgeolekubüroole);

b) teostada uurimine ja edastada selle lõpetamisel täiemahuline aruanne julgeolekuorganile (vt punkt a eespool). Seejärel tuleks võtta vajalikud meetmed olukorra heastamiseks.

16. *Kontrollimine*

Kokkuleppel asjaomaste riikide või rahvusvaheliste organisatsioonidega on peasekretariaadi julgeolekubürool lubatud hinnata avaldatud Euroopa Liidu salastatud teabe kaitsmise meetmete tõhusust.

17. *Aruandlus*

Riik või organisatsioon, kelle valduses on Euroopa Liidu salastatud teave, peab esitama kord aastas kuupäevaks, mis sätestatakse siis, kui antakse luba teabe avaldamiseks, aruande käesolevate julgeolekueeskirjade täitmise kohta.

*Liide 6*

**Juhtnöörid Euroopa Liidu salastatud teabe avaldamiseks kolmandatele riikidele või rahvusvahelistele organisatsioonidele**

3. taseme koostöö

MENETLUSED

1. Aeg-ajalt võib nõukogu teatavate eriliste asjaolude korral soovida teha koostööd riikide või organisatsioonidega, kes ei saa tagada käesolevate julgeolekueeskirjadega nõutavat turvalisust, kuid kõnealune koostöö võib siiski eeldada Euroopa Liidu salastatud teabe avaldamist. Sellise avaldamise hulka ei kuulu spetsiaalselt liikmesriikidele mõeldud siseriiklik teave.

2. Selliste eriliste asjaolude korral vaatab kolmandate riikide või rahvusvaheliste organisatsioonide taotlused koostöö kohta Euroopa Liiduga või liikmesriikide või vajaduse korral Euroopa Liidu detsentraliseeritud asutuste esitatud ettepanekud selleks esmalt sisuliselt läbi nõukogu, kes küsib vajaduse korral teabe koostanud liikmesriigi või detsentraliseeritud asutuse seisukohta. Nõukogu kaalub, kuivõrd põhjendatud on salastatud teabe avaldamine, hindab teabetaotlejate teadmisvajadust ja otsustab selle salastatud teabe laadi, mida võib edastada.

3. Kui nõukogu on teabe avaldamisega nõus, vastutab peasekretär/kõrge esindaja nõukogu julgeolekukomitee kokkukutsumise eest või küsitleb, vajaduse korral vaikiva menetluse alusel, liikmesriikide siseriiklikke julgeolekuasutusi, et koostada julgeolekukomitee tehniline seisukoht.

4. Nõukogu julgeolekukomitee tehniline seisukoht käsitleb järgmisi küsimusi:

   a) Euroopa Liidule või selle liikmesriikidele tulenevate julgeolekuriskide hinnang;

   b) selle teabe salastatuse kategooria, mida võib avaldada, vajaduse korral silmas pidades teabe laadi;

   c) dokumentide salastatuse kategooria alandamine või kaotamine dokumendi koostanud asutuse või ametiisiku poolt enne, kui see avaldatakse asjaomasele riigile või rahvusvahelisele organisatsioonile; ([1])

   d) avaldatavate dokumentide käitlemise kord (vt punkt 5 allpool);

   e) võimalikud edastusviisid (avaliku postiteenistuse, üldkasutatavate või turvaliste sidesüsteemide, diplomaatilise posti, julgeolekukontrolli läbinud kullerite jms kasutamine).

5. Käesolevas liites käsitletavatele riikidele või organisatsioonidele avaldatavad dokumendid ei sisalda põhimõtteliselt viiteid dokumendi allikale ega Euroopa Liidu salastatusele tasemele. Nõukogu julgeolekukomitee võib soovitada järgmist:

   — kasutada spetsiifilist märgistust või koodnimetust,

   — kasutada spetsiifilist salastamissüsteemi, mille puhul oleks teabe tundlikkus seotud kontrollimeetmetega, mida eeldatakse vastuvõtja kasutatavatelt edastusviisidelt (vt näiteks punkt 14).

6. Peasekretariaadi julgeolekubüroo esitab julgeolekukomitee tehnilise seisukoha nõukogule ja lisab sellele vajaduse korral ettepaneku volituste delegeerimiseks, mis on vajalikud tööülesannete täitmiseks eelkõige kiiret reageerimist nõudvates olukordades.

7. Kui nõukogu on heaks kiitnud Euroopa Liidu salastatud teabe avaldamise ja praktilise rakenduskorra, loob peasekretariaadi julgeolekubüroo vajalikud sidemed asjaomase riigi või organisatsiooni julgeolekuorganiga, et soodustada kavandatud julgeolekumeetmete rakendamist.

([1]) Sel juhul peab dokumendi koostanud asutus või ametiisik rakendama III jao punktis 9 määratletud korda kõigi Euroopa Liidus ringlevate koopiate suhtes.

8. Peasekretariaadi julgeolekubüroo edastab kõigile asjaomastele liikmesriikidele ja vajaduse korral Euroopa Liidu detsentraliseeritud asutustele täiendavaks infoks tabeli, milles on kokku võetud teabe laad ja salastatuse kategooriad ning loetletud organisatsioonid ja riigid, kellele võib teabe avaldada vastavalt sellele, mida nõukogu on otsustanud.

9. Teabe avaldamisega tegeleva liikmesriigi julgeolekuasutus või peasekretariaadi julgeolekubüroo võtab kõik vajalikud meetmed, et aidata kaasa võimalike kahjude hindamisele ja menetluste läbivaatamisele.

10. Koostöö tingimuste muutumisest tuleb nõukogule alati teatada.

JULGEOLEKUEESKIRJAD, MIDA PEAVAD KOHALDAMA TEABESAAJAD

11. Peasekretär/kõrge esindaja teatab teabesaajatele riikidele või rahvusvahelistele organisatsioonidele nõukogu otsusest lubada avaldada Euroopa Liidu salastatud teavet ja edastab samal ajal nõukogu julgeolekukomitee soovitatud ja nõukogus heakskiidetud üksikasjalikud reeglid kaitsmise kohta. Kui taotluse esitas liikmesriik, teatab kõnealune riik teabesaajat avaldamise lubamisest.

Otsus jõustub ainult juhul, kui teabesaajad kinnitavad kirjalikult, et nad:

— kasutavad teavet ainult nõukogu otsuse kohase koostöö eesmärgil,

— tagavad teabele nõukogu nõutava kaitse.

12. *Dokumentide edastamine*

a) Dokumentide edastamise praktilises korras lepivad kokku peasekretariaadi julgeolekubüroo ja teabesaajate riikide või rahvusvaheliste organisatsioonide julgeolekuasutused. Eelkõige nimetatakse täpsed aadressid, kuhu dokumendid tuleb saata.

b) Salastatuse kategooriasse CONFIDENTIEL UE ja kõrgemasse salastatuse kategooriasse kuuluvad dokumendid edastatakse kahekordses ümbrikus. Sisemisel ümbrikul on kokkulepitud eritempel või koodnimetus ja märge dokumendi jaoks vastuvõetud salastatuse erikategooria kohta. Iga salastatud dokumendi kohta lisatakse kättesaamistõendi vorm. Kättesaamistõendi vormil, mis ei ole salastatud, märgitakse dokumendi kohta ainult teatavad andmed (viitenumber, kuupäev, koopia number) ja keel, milles dokument on koostatud, mitte aga dokumendi pealkirja.

c) Seejärel pannakse sisemine ümbrik välimisse ümbrikku, millel on arvepidamiseks kirjas paki number. Välimisele ümbrikule salastatuse kategooriat ei märgita.

d) Kullerile antakse alati kättesaamiskinnitus, millel on kirjas paki number.

13. *Registreerimine saabumisel*

Adressaatriigi julgeolekuasutus või sellega samaväärne asutus riigis, mis võtab Euroopa Liidu edastatud salastatud teabe vastu oma valitsuse nimel, või vastuvõtva rahvusvahelise organisatsiooni julgeolekubüroo avab eraldi registri, et registreerida Euroopa Liidu salastatud teave selle saabumisel. Registris on veerud saabumiskuupäeva, dokumendi andmete (kuupäev, viitenumber ja koopia number), salastatuse kategooria, pealkirja, adressaadi nime või ametinimetuse ja vastuvõtmistõendi tagastamiskuupäeva jaoks ning kuupäeva jaoks, mil vastuvõtmistõend tagastatakse Euroopa Liidule või hävitatakse.

14. *Vahetatud salastatud teabe kasutamine ja kaitsmine*

a) Salastatuse kategooriasse SECRET UE kuuluvat teavet käitlevad spetsiaalselt määratud ametnikud, kellel on luba juurdepääsuks sellise salastatuse tasemega teabele. Sellist teavet säilitatakse kvaliteetsetes turvakappides, mida saavad avada ainult isikud, kellel on luba juurdepääsuks neis sisalduvale teabele. Aladel, kus sellised kapid asuvad, peab olema alaline valve ning tuleb luua kontrollsüsteem tagamaks, et sinna lubatakse siseneda ainult nõuetekohaselt volitatud isikutel. Salastatuse kategooriasse SECRET UE kuuluvat teavet võib edastada diplomaatilise posti, turvalise postiteenuse ja turvaliste sideteenuste abil. Salastatuse kategooriasse SECRET UE kuuluvatest dokumentidest võib koopiaid teha ainult nende koostaja kirjalikul loal. Kõik koopiad registreeritakse ja neid jälgitakse. Kõigi salastatuse kategooriasse SECRET UE kuuluvate dokumentidega seotud toimingute kohta väljastatakse tõendid.

b) Salastatuse kategooriasse CONFIDENTIEL UE kuuluvat teavet käitlevad nõuetekohaselt määratud ametnikud, kellel on luba saada teavet asjaomase teema kohta. Dokumente säilitatakse kontrollitud alal asuvates lukustatud turvakappides.

Salastatuse kategooriasse CONFIDENTIEL UE kuuluvat teavet võib edastada diplomaatilise posti, sõjaväelise postiteenuse ja turvaliste sideteenuste abil. Vastuvõtja või teha teabest koopiaid ning nende arv ja andmed nende levitamise kohta tuleb registreerida eriregistris.

c) Salastatuse kategooriasse RESTREINT UE kuuluvat teavet käideldakse ruumides, kuhu ei pääse volitamata isikud, ja säilitatakse lukustatud konteinerites. Dokumente võib edastada üldkasutatava postiteenistuse kaudu kahekordses ümbrikus tähitud kirjana ja hädaolukorras turvamata üldkasutatavate sidesüsteemide kaudu. Vastuvõtjad võivad teha koopiaid.

d) Salastamata teabe puhul ei ole spetsiaalsed kaitsemeetmed vajalikud ning sellist teavet võib edastada posti teel ja üldkasutatavate sidesüsteemide kaudu. Adressaadid võivad teha koopiaid.

15. *Hävitamine*

Dokumendid, mida enam ei vajata, tuleb hävitada. Salastatuse kategooriatesse kuuluvate dokumentide puhul tehakse vajalik märge eriregistrisse. Salastatuse kategooriasse SECRET UE kuuluvate dokumentide puhul antakse välja hävitamisakt, millele kirjutavad alla kaks hävitamise tunnistajaks olnud isikut.

16. *Julgeoleku rikkumine*

Kui kahjustatakse salastatuse kategooriasse CONFIDENTIEL UE või SECRET UE kuuluvat teavet või kui kahtlustatakse sellist kahjustamist, teostab riigi siseriiklik julgeolekuasutus või organisatsiooni julgeolekujuht kahjustamise asjaolude uurimise. Kui uurimistulemused on positiivsed, teatatakse sellest dokumendi koostanud asutusele või ametiisikule. Kui kahjustamise on põhjustanud mitterahuldavad menetlused või säilitamismeetodid, võetakse vajalikud meetmed nende parandamiseks. Nõukogu peasekretär/kõrge esindaja või selle liikmesriigi julgeolekuasutus, kes avaldas kahjustatud andmed, võib teabesaajalt küsida üksikasju uurimise kohta.