►**B**

NÕUKOGU OTSUS,

23. september 2013,

ELi salastatud teabe kaitseks vajalike julgeolekueeskirjade kohta

(2013/488/EL)

(ELT L 274, 15.10.2013, lk 1)

Muudetud:

		Euroopa Liidu Teataja		
		nr	lehekülg	kuupäev
►**M1**	Nõukogu otsus 2014/233/EL, 14. aprill 2014	L 125	72	26.4.2014

▼B

NÕUKOGU OTSUS,

23. september 2013,

ELi salastatud teabe kaitseks vajalike julgeolekueeskirjade kohta

(2013/488/EL)

EUROOPA LIIDU NÕUKOGU,

võttes arvesse Euroopa Liidu toimimise lepingut, eriti selle artikli 240 lõiget 3,

võttes arvesse nõukogu 1. detsembri 2009. aasta otsust 2009/937/EL, millega võetakse vastu nõukogu kodukord, ([1]) eriti selle artiklit 24,

ning arvestades järgmist:

(1) Nõukogu töö arendamiseks valdkondades, mis eeldavad salastatud teabe töötlemist, on otstarbekas luua salastatud teabe kaitseks ulatuslik julgeolekusüsteem, mis hõlmaks nõukogu, selle peasekretariaati ja liikmesriike.

(2) Käesolevat otsust tuleks kohaldada juhtudel, kui nõukogu, selle ettevalmistavad organid või nõukogu peasekretariaat töötlevad ELi salastatud teavet.

(3) ELi salastatud teabe töötlemisel liikmesriikide pädevate asutuste, töötajate või lepinglaste poolt peaksid liikmesriigid järgima käesolevat otsust kooskõlas oma riigisiseste õigusaktidega ning nõukogu toimimiseks vajalikus ulatuses, et iga liikmesriik võiks olla kindel ELi salastatud teabe suhtes samaväärse kaitsetaseme kohaldamises.

(4) Nõukogu, komisjon ja Euroopa välisteenistus kohustuvad kohaldama ELi salastatud teabe kaitse suhtes samaväärse tasemega julgeolekustandardeid.

(5) Nõukogu rõhutab, et vajaduse korral tuleb ka Euroopa Parlament ja muud liidu institutsioonid, organid ja asutused kaasata liidu ja tema liikmesriikide huvide kaitsmiseks vajalike salastatud teabe kaitsmise põhimõtete, standardite ja eeskirjade kohaldamisse.

(6) Nõukogu peaks kindlaks määrama sobiva raamistiku nõukogu valduses oleva ELi salastatud teabe jagamiseks vajaduse korral teiste liidu institutsioonide, organite ja asutustega kooskõlas käesoleva otsusega ja kehtivate institutsioonidevaheliste kokkulepetega.

(7) Euroopa Liidu lepingu (ELi leping) V jaotise 2. peatüki alusel loodud liidu organid ja asutused ning Europol ja Eurojust peaksid kohaldama oma sisekorralduses ELi salastatud teabe kaitseks käesolevas otsuses sätestatud aluspõhimõtteid ja miinimumstandardeid, kui see on ette nähtud nende asutamist käsitlevates õigusaktides.

([1]) ELT L 325, 11.12.2009, lk 35.

▼B

(8) ELi lepingu V jaotise 2. peatüki alusel loodud kriisiohjamisoperatsioonid ja nende isikkoosseis peaksid kohaldama ELi salastatud teabe kaitseks nõukogu poolt vastuvõetud julgeolekueeskirju, kui see on ette nähtud nende asutamist käsitlevates nõukogu õigusaktides.

(9) ELi eriesindajad ja nende isikkoosseisu liikmed peaksid kohaldama ELi salastatud teabe kaitseks nõukogu poolt vastuvõetud julgeolekueeskirju, kui see on ette nähtud asjaomase nõukogu õigusaktiga.

(10) Käesolev otsus ei piira Euroopa Liidu toimimise lepingu (ELi toimimise leping) artiklite 15 ja 16 ega neid rakendavate õigusaktide kohaldamist.

(11) Käesolev otsus ei piira liikmesriikide seniste tavade kohaldamist seoses liikmesriikide parlamentide teavitamisega liidu tegevustest.

(12) Selleks, et tagada ELi salastatud teabe kaitseks vajalike julgeolekueeskirjade õigeaegne kohaldamine, võttes arvesse Horvaatia Vabariigi ühinemist Euroopa Liiduga, peaks käesolev otsus jõustuma selle avaldamise kuupäeval,

ON VASTU VÕTNUD KÄESOLEVA OTSUSE:

Artikkel 1

Eesmärk, reguleerimisala ja mõisted

1. Käesoleva otsusega nähakse ette ELi salastatud teabe kaitseks vajalikud julgeoleku aluspõhimõtted ja miinimumstandardid.

2. Kõnealuseid aluspõhimõtteid ja miinimumstandardeid kohaldatakse nõukogu ja selle peasekretariaadi suhtes ning liikmesriigid peavad neid järgima kooskõlas oma vastavate riigisiseste õigusaktidega, et tagada kõigile ELi salastatud teabe samaväärne kaitsetase.

3. Käesolevas otsuses kohaldatakse A liites esitatud mõisteid.

Artikkel 2

ELi salastatud teabe, salastatuse tasemete ja märgete määratlus

1. „ELi salastatud teave” on teave või materjal, mis on tähistatud ELi salastusmärkega ja mille loata avaldamine võib eri määral kahjustada Euroopa Liidu või ühe või mitme liikmesriigi huve.

2. ELi salastatud teave liigitatakse ühte järgmistest tasemetest:

a) TRÈS SECRET UE/EU TOP SECRET: teave ja materjal, mille loata avaldamine võib väga tõsiselt kahjustada Euroopa Liidu või ühe või mitme liikmesriigi olulisi huve;

b) SECRET UE/EU SECRET: teave ja materjal, mille loata avaldamine võib tõsiselt kahjustada Euroopa Liidu või ühe või mitme liikmesriigi olulisi huve;

▼B

c) CONFIDENTIEL UE/EU CONFIDENTIAL: teave ja materjal, mille loata avaldamine võib kahjustada Euroopa Liidu või ühe või mitme liikmesriigi olulisi huve;

d) RESTREINT UE/EU RESTRICTED: teave ja materjal, mille loata avaldamine võib negatiivselt mõjutada Euroopa Liidu või ühe või mitme liikmesriigi huve.

3. ELi salastatud teave tähistatakse salastusmärkega vastavalt lõikele 2. See võib kanda täiendavat märget, nagu asjaomases dokumendis käsitletud valdkonda määratlevad, dokumendi koostajat tuvastavad, dokumendi levitamist või kasutamist piiravad või avaldatavuse märked.

Artikkel 3

Salastatuse tasemete haldamine

1. Pädevad asutused tagavad, et ELi salastatud teabele on määratud asjakohane salastatuse tase, teave on selgelt määratletud salastatud teabena ning see säilitab oma salastatuse taseme üksnes nii kaua kui vajalik.

2. ELi salastatud teabe salastatuse taset ei alandata, salastatust ei kustutata ja artikli 2 lõikes 3 osutatud märkeid ei muudeta ega kõrvaldata ilma dokumendi koostaja eelneva kirjaliku nõusolekuta.

3. Nõukogu kiidab heaks ELi salastatud teabe loomist käsitleva julgeolekupoliitika, mis sisaldab salastatuse taseme määramise praktilist juhendit.

Artikkel 4

Salastatud teabe kaitse

1. ELi salastatud teabe kaitsmine toimub käesoleva otsuse kohaselt.

2. ELi salastatud teabe ühiku valdaja vastutab selle kaitsmise eest käesoleva otsuse kohaselt.

3. Kui liikmesriigid sisestavad liidu struktuuridesse või võrkudesse riigisisest salastusmärget kandva salastatud teabe, kaitsevad nõukogu ja nõukogu peasekretariaat seda teavet kooskõlas nõuetega, mida kohaldatakse samaväärse salastatuse tasemega ELi salastatud teabe suhtes vastavalt B liites esitatud salastatuse tasemete vastavustabelile.

4. ELi salastatud teabe kogumi puhul võib vajalikuks osutuda kõrgemale salastatuse tasemele vastav kaitse tase, kui selle üksikkomponentide puhul.

▼B

Artikkel 5

Turvariski juhtimine

1. ELi salastatud teabe turvariski juhitakse protsessina. Nimetatud protsessi eesmärk on teha kindlaks teadaolevad turvariskid, määrata vastavalt käesolevas otsuses sätestatud aluspõhimõtetele ja miinimumstandarditele kindlaks selliste riskide vastuvõetava tasemeni vähendamise turvameetmed ja kohaldada kõnealuseid meetmeid kooskõlas A liites määratletud süvakaitse põhimõttega. Selliste meetmete tõhusust hinnatakse pidevalt.

2. Turvameetmed, mis on vajalikud ELi salastatud teabe kaitsmiseks kogu kasutusaja jooksul, on vastavuses eelkõige asjaomase teabe või materjali salastatuse taseme, vormi ja hulgaga, ELi salastatud teavet sisaldavate rajatiste asukoha ja ülesehitusega ning kohapeal antud hinnanguga kuritahtlikust ja/või kriminaalsest tegevusest, sealhulgas spionaažist, sabotaažist või terrorismist tulenevale ohule.

3. Situatsiooniplaanides võetakse arvesse vajadust kaitsta ELi salastatud teavet hädaolukordades, et vältida volitamata juurdepääsu teabele, teabe loata avaldamist või teabe tervikluse või käideldavuse kadumist.

4. Talitluspidevuse tagamise plaanidesse lisatakse ennetus- ja taastamismeetmed, et minimeerida ulatuslike rikete või intsidentide mõju ELi salastatud teabe töötlemisele ja säilitamisele.

Artikkel 6

Käesoleva otsuse rakendamine

1. Vajaduse korral kiidab nõukogu julgeolekukomitee soovituse alusel heaks julgeolekupoliitikad, milles sätestatakse meetmed käesoleva otsuse rakendamiseks.

2. Julgeolekukomitee võib oma tasandil kokku leppida julgeolekusuunistes, mille eesmärk on täiendada või toetada käesolevat otsust ja nõukogu poolt heaks kiidetud julgeolekupoliitikaid.

Artikkel 7

Töötajatega seotud julgeolek

1. Töötajatega seotud julgeolek tähendab selliste meetmete kohaldamist, millega tagatakse juurdepääs ELi salastatud teabele ainult isikutele:

— kellel on teadmisvajadus,

— kes on läbinud vajalikul tasemel julgeolekukontrolli, kui see on asjakohane, ning

— keda on teavitatud nende vastutusest.

2. Töötajatega seotud julgeolekukontrolli kord on selline, et selle alusel on võimalik kindlaks teha, kas isikule võib tema lojaalsust ja usaldusväärsust arvesse võttes lubada juurdepääsu ELi salastatud teabele.

▼B

3. Kõik nõukogu peasekretariaadis töötavad isikud, kes vajavad oma tööülesannete tõttu juurdepääsu CONFIDENTIEL UE/EU CONFIDENTIAL või kõrgemal tasemel ELi salastatud teabele või kelle tööülesanded nõuavad sellise teabe käitlemist, peavad enne, kui neile antakse juurdepääs sellisele ELi salastatud teabele, läbima asjakohase taseme julgeolekukontrolli. Sellised isikud peavad saama nõukogu peasekretariaadi ametisse nimetavalt asutuselt loa juurdepääsuks kuni teatud salastatuse tasemel ELi salastatud teabele kindlaksmääratud kuupäevani.

4. Artikli 15 lõikes 3 osutatud liikmesriikide töötajad, kes võivad oma tööülesannete tõttu vajada juurdepääsu CONFIDENTIEL UE/EU CONFIDENTIAL või kõrgemal tasemel ELi salastatud teabele, läbivad enne, kui neile antakse juurdepääs sellisele ELi salastatud teabele, asjakohase taseme julgeolekukontrolli või omavad ametiülesannetest tulenevat juurdepääsuõigust vastavalt riigisisestele õigusaktidele.

5. Enne ELi salastatud teabele juurdepääsu andmist ja pärast seda regulaarsete ajavahemike järel teavitatakse kõiki isikuid nende kohustusest kaitsta ELi salastatud teavet vastavalt käesolevale otsusele, ning nad kinnitavad oma vastutust seoses kõnealuse teabe kaitsmisega.

6. Sätted käesoleva artikli rakendamise kohta on esitatud I lisas.

Artikkel 8

Füüsiline julgeolek

1. Füüsiline julgeolek on füüsiliste ja tehniliste kaitsemeetmete rakendamine, et vältida volitamata juurdepääsu ELi salastatud teabele.

2. Füüsilise julgeoleku meetmete eesmärk on välistada salajane või jõuga sissetung, hoida ära, takistada ja avastada lubamatuid toiminguid ning võimaldada töötajate eristamist seoses juurdepääsuga ELi salastatud teabele teadmisvajaduse põhimõtte alusel. Sellised meetmed määratakse kindlaks riskijuhtimisprotsessi alusel.

3. Füüsilise julgeoleku meetmeid kohaldatakse kõikide objektide, hoonete, ametiruumide ning muude ruumide ja alade suhtes, kus töödeldakse või säilitatakse ELi salastatud teavet, sealhulgas alade suhtes, kus paiknevad artikli 10 lõikes 2 määratletud side- ja infosüsteemid.

4. Alad, kus säilitatakse CONFIDENTIEL UE/EU CONFIDENTIAL või kõrgemal tasemel ELi salastatud teavet, luuakse turvaaladena vastavalt II lisale ning need kiidab heaks pädev julgeolekuasutus.

5. CONFIDENTIEL UE/EU CONFIDENTIAL või kõrgemal tasemel salastatud teabe kaitseks kasutatakse üksnes heakskiidetud seadmeid ja vahendeid.

6. Sätted käesoleva artikli rakendamise kohta on esitatud II lisas.

▼B

Artikkel 9

Salastatud teabe haldamine

1. Salastatud teabe haldamine tähendab haldusmeetmete kohaldamist ELi salastatud teabe kontrollimiseks kogu selle kasutusaja jooksul, et täiendada artiklites 7, 8 ja 10 sätestatud meetmeid ja aidata seeläbi ära hoida ja avastada sellise teabe tahtlikku või juhuslikku ohtu sattumist või kadumist. Sellised meetmed on eelkõige seotud ELi salastatud teabe loomise, registreerimise, kopeerimise, tõlkimise, salastatuse taseme alandamise, salastatuse kustutamise, veo ja hävitamisega.

2. CONFIDENTIEL UE/EU CONFIDENTIAL või kõrgemal tasemel salastatud teave registreeritakse julgeolekukaalutlustel enne levitamist ja selle vastuvõtmisel. Nõukogu peasekretariaadi ja liikmesriikide pädevad asutused loovad selleks registrite süsteemi. TRÈS SECRET UE/EU TOP SECRET tasemel salastatud teave registreeritakse selleks ettenähtud registrites.

3. Pädev julgeolekuasutus kontrollib regulaarselt teenistusi ja tööruume, kus toimub ELi salastatud teabe töötlemine või säilitamine.

4. ELi salastatud teabe edastamine teenistuste ja tööruumide vahel väljaspool füüsiliselt kaitstud alasid toimub järgmiselt:

a) üldjuhul edastatakse ELi salastatud teave elektrooniliselt, kaitstuna artikli 10 lõike 6 kohaselt heakskiidetud krüptovahenditega;

b) kui punktis a osutatud edastusviisi ei kasutata, veetakse ELi salastatud teavet:

   i) elektroonilisel andmekandjal (nt USB mälupulk, CD, kõvaketas), kaitstuna artikli 10 lõike 6 kohaselt heakskiidetud krüptovahenditega, või

   ii) kõikidel muudel juhtudel pädeva julgeolekuasutuse ettenähtud korras vastavalt III lisas sätestatud asjakohastele kaitsemeetmetele.

5. Sätted käesoleva artikli rakendamise kohta on esitatud III ja IV lisas.

Artikkel 10

Side- ja infosüsteemides töödeldava ELi salastatud teabe kaitse

1. Infokindlus side- ja infosüsteemide valdkonnas tähendab kindlust, et sellised süsteemid kaitsevad neis töödeldavat teavet ning toimivad ettenähtud korras, ettenähtud ajal ja õiguspäraste kasutajate kontrolli all. Tõhus infokindlus tagab asjakohasel tasemel salajasuse, tervikluse, käideldavuse, salgamise vääramise ja autentsuse. Infokindluse aluseks on riskijuhtimisprotsess.

▼B

2. Side- ja infosüsteem tähendab süsteemi, mis võimaldab elektroonilises vormis oleva teabe töötlemist. Side- ja infosüsteem hõlmab kõiki selle toimimiseks vajalikke vahendeid, sealhulgas infrastruktuuri, töökorralduse, töötajate ja teabega seotud ressursse. Käesolevat otsust kohaldatakse side- ja infosüsteemide suhtes, milles töödeldakse ELi salastatud teavet.

3. Side- ja infosüsteemid töötlevad ELi salastatud teavet kooskõlas infokindluse kontseptsiooniga.

4. Kõik side- ja infosüsteemid läbivad akrediteerimisprotsessi. Akrediteerimise eesmärk on tagada, et kooskõlas käesoleva otsusega on rakendatud kõiki asjakohaseid turvameetmeid ning on saavutatud ELi salastatud teabe ning side- ja infosüsteemi piisava tasemega kaitse. Akrediteerimisteatises määratakse kindlaks teabe maksimaalne salastatuse tase, millesse kuuluvat teavet side- ja infosüsteem võib töödelda, ning vastavad tingimused.

5. Rakendatakse turvameetmeid, et kaitsta CONFIDENTIEL UE/EU CONFIDENTIAL ja kõrgemal tasemel salastatud teavet töötlevaid side- ja infosüsteeme sellise teabe ohtu sattumise eest tahtmatu elektromagnetkiirguse kaudu („TEMPEST-turvameetmed”). Sellised turvameetmed peavad olema vastavuses teabe kasutusriski ja salastatuse tasemega.

6. Kui ELi salastatud teavet kaitstakse krüptovahenditega, kiidetakse sellised vahendid heaks järgmiselt:

a) SECRET UE/EU SECRET ja kõrgemal tasemel salastatud teabe salajasust kaitstakse krüptovahenditega, mille nõukogu kui krüptovahendite heakskiitmise asutus on julgeolekukomitee soovitusel heaks kiitnud;

b) CONFIDENTIEL UE/EU CONFIDENTIAL või RESTREINT UE/EU RESTRICTED tasemel salastatud teabe salajasust kaitstakse krüptovahenditega, mille nõukogu peasekretär („peasekretär”) kui krüptovahendite heakskiitmise asutus on julgeolekukomitee soovitusel heaks kiitnud.

Olenemata punktist b võib liikmesriikide riigisisestes süsteemides kaitsta CONFIDENTIEL UE/EU CONFIDENTIAL või RESTREINT UE/EU RESTRICTED tasemel ELi salastatud teabe salajasust krüptovahenditega, mille on heaks kiitnud liikmesriigi krüptovahendite heakskiitmise asutus.

7. ELi salastatud teabe elektroonilise edastamise ajal kasutatakse heakskiidetud krüptovahendeid. Olenemata nimetatud nõudest võib erakorraliste asjaolude või IV lisas nimetatud spetsiifiliste tehniliste tingimuste korral rakendada erimenetlusi.

▼B

8. Nõukogu peasekretariaadi ja liikmesriikide pädevad asutused loovad järgmised infokindlusega tegelevad asutused:

a) infokindluse asutus;

b) TEMPEST-asutus;

c) krüptovahendite heakskiitmise asutus;

d) krüptomaterjalide jaotamise asutus.

9. Nõukogu peasekretariaadi ja liikmesriikide pädevad asutused loovad iga süsteemi jaoks järgmised asutused:

a) turvalisuse akrediteerimise asutus;

b) infokindluse rakendusasutus.

10. Sätted käesoleva artikli rakendamise kohta on esitatud IV lisas.

Artikkel 11

Tööstusjulgeolek

1. Tööstusjulgeolek tähendab meetmete kohaldamist selleks, et tagada ELi salastatud teabe kaitsmine lepinglaste ja all-lepinglaste poolt lepingueelsetel läbirääkimistel ja salastatud lepingute kogu kehtivusaja jooksul. Selliste lepingutega ei kaasne juurdepääsu TRÈS SECRET UE/EU TOP SECRET tasemel salastatud teabele.

2. Nõukogu peasekretariaat võib lepinguga usaldada ülesanded, millega kaasneb juurdepääs ELi salastatud teabele või sellise teabe töötlemine või säilitamine, tööstus- või muudele üksustele, mis on registreeritud liikmesriigis või kolmandas riigis, mis on sõlminud lepingu või halduskokkuleppe vastavalt artikli 13 lõike 2 punktile a või b.

3. Nõukogu peasekretariaat kui lepingu sõlmija tagab, et salastatud lepingute sõlmimisel tööstus- või muude üksustega järgitakse käesolevas otsuses sätestatud ja lepingus viidatud tööstusjulgeoleku miinimumstandardeid.

4. Liikmesriigi riiklik julgeolekuasutus, määratud julgeolekuasutus või muu pädev asutus tagab riigisiseste õigusaktidega lubatud ulatuses, et nende territooriumil registreeritud lepinglased ja all-lepinglased võtavad lepingueelsetel läbirääkimistel ja salastatud lepingu täitmisel kõik asjakohased meetmed ELi salastatud teabe kaitsmiseks.

5. Liikmesriigi riiklik julgeolekuasutus, määratud julgeolekuasutus või muu pädev julgeolekuasutus tagab vastavalt riigisisestele õigusaktidele, et asjaomase liikmesriigi territooriumil registreeritud lepinglased ja all-lepinglased, kes osalevad sellistes salastatud lepingutes või all-lepingutes, mis eeldavad juurdepääsu CONFIDENTIEL UE/EU CONFIDENTIAL või SECRET UE/EU SECRET tasemel salastatud teabele oma valdustes, kas selliste lepingute täitmise käigus või lepingueelses etapis, omavad asjakohase tasemega töötlemisluba.

▼B

6. Lepinglase või all-lepinglase töötajatele, kes vajavad salastatud lepingu täitmiseks juurdepääsu CONFIDENTIEL UE/EU CONFIDENTIAL või SECRET UE/EU SECRET tasemel salastatud teabele, väljastab juurdepääsuloa asjaomane riiklik julgeolekuasutus, määratud julgeolekuasutus või muu pädev julgeolekuasutus vastavalt riigisisestele õigusaktidele ja I lisas sätestatud miinimumstandarditele.

7. Sätted käesoleva artikli rakendamise kohta on esitatud V lisas.

Artikkel 12

ELi salastatud teabe jagamine

1. Nõukogu kehtestab tingimused, mille alusel ta võib oma valduses olevat ELi salastatud teavet jagada teiste liidu institutsioonide, organite ja asutustega. Sel eesmärgil võib kehtestada asjakohase raamistiku, sealhulgas vajaduse korral sõlmida institutsioonidevahelisi kokkuleppeid või muid kokkuleppeid.

2. Selline raamistik tagab, et ELi salastatud teavet kaitstakse vastavalt selle salastatuse tasemele ning kooskõlas selle aluspõhimõtete ja miinimumstandarditega, mis on samaväärsed käesolevas otsuses sätestatuga.

Artikkel 13

Salastatud teabe vahetamine kolmandate riikide ja rahvusvaheliste organisatsioonidega

1. Kui nõukogu otsustab, et on vaja vahetada ELi salastatud teavet kolmanda riigi või rahvusvahelise organisatsiooniga, kehtestatakse selleks asjakohane raamistik.

2. Sellise raamistiku kehtestamiseks ning vahetatava salastatud teabe kaitsmise vastastikuste eeskirjade määratlemiseks:

a) sõlmib liit kolmandate riikide või rahvusvaheliste organisatsioonidega lepingu salastatud teabe kaitse ja vahetamise julgeolekukorra kohta („salastatud teabe kaitse leping”) või

b) võib peasekretär sõlmida nõukogu peasekretariaadi nimel VI lisa punkti 17 kohaselt halduskokkuleppe, kui avalikustatav ELi salastatud teave ei ole üldjuhul kõrgemal salastatuse tasemel kui RESTREINT UE/EU RESTRICTED.

3. Lõikes 2 osutatud salastatud teabe kaitse lepingud või halduskokkulepped sisaldavad sätteid, millega tagatakse, et juhul kui kolmandad riigid või rahvusvahelised organisatsioonid saavad ELi salastatud teavet, kaitstakse kõnealust teavet asjakohase salastatuse taseme kohaselt ja vastavalt miinimumstandarditele, mis on vähemalt sama ranged kui käesolevas otsuses sätestatud miinimumstandardid.

▼B

4. Nõukogu teeb otsuse nõukogust pärineva ELi salastatud teabe kolmandale riigile või rahvusvahelisele organisatsioonile avaldamise kohta igal üksikjuhul eraldi, võttes arvesse kõnealuse teabe laadi ja sisu, selle vastuvõtja teadmisvajadust ning liidule teabe avaldamisest tuleneva kasu ulatust. Kui salastatud teave, mida soovitakse avaldada, ei ole pärit nõukogust, küsib nõukogu peasekretariaat avaldamiseks kõigepealt teabe koostaja kirjalikku nõusolekut. Kui teabe koostajat ei ole võimalik kindlaks teha, võtab nõukogu vastutuse teabe eest endale.

5. Esitatava või vahetatava ELi salastatud teabe kaitseks kolmanda riigi või rahvusvahelise organisatsiooni poolt rakendatavate turvameetmete tõhususe hindamiseks korraldatakse hindamiskülastusi.

6. Sätted käesoleva artikli rakendamise kohta on esitatud VI lisas.

Artikkel 14

Julgeolekunõuete rikkumine ja ELi salastatud teabe ohtu sattumine

1. Julgeolekunõuete rikkumine toimub isiku sellise tegevuse või tegevusetuse tagajärjel, mis on vastuolus käesolevas otsuses sätestatud julgeolekueeskirjadega.

2. ELi salastatud teave satub ohtu siis, kui julgeolekunõuete rikkumise tulemusena on kõnealune teave tervikuna või osaliselt avalikustatud volitamata isikutele.

3. Igast julgeolekunõuete rikkumisest või julgeolekunõuete rikkumise kahtlusest teatatakse viivitamata pädevale julgeolekuasutusele.

4. Kui on teada või kui on põhjendatult alust eeldada, et ELi salastatud teave on ohtu sattunud või kadunud, võtab riiklik julgeolekuasutus või muu pädev asutus kooskõlas vastavate õigusaktidega kõik asjakohased meetmed, et:

a) teavitada teabe koostajat;

b) tagada asjaolude kindlakstegemiseks juhtumi uurimine töötajate poolt, kes ei ole rikkumisega vahetult seotud;

c) hinnata liidu või liikmesriikide huvidele tekitatud võimalikku kahju;

d) võtta sobivaid meetmeid rikkumise kordumise ärahoidmiseks ning

e) teavitada asjaomaseid asutusi võetud meetmetest.

5. Iga isiku suhtes, kes on vastutav käesolevas otsuses sätestatud julgeolekueeskirjade rikkumise eest, võib kohaldada distsiplinaarmeetmeid vastavalt kohaldatavatele õigus- ja haldusnormidele. Iga isiku suhtes, kes on vastutav ELi salastatud teabe ohtu sattumise või kadumise eest, kohaldatakse distsiplinaar- ja/või õiguslikke meetmeid vastavalt kohaldatavatele õigus- ja haldusnormidele.

▼B

Artikkel 15

Vastutus rakendamise eest

1. Nõukogu võtab kõik vajalikud meetmed, et tagada üldine järjepidevus käesoleva otsuse kohaldamisel.

2. Peasekretär võtab kõik vajalikud meetmed tagamaks, et ELi salastatud teabe või muu salastatud teabe töötlemisel või säilitamisel nõukogu poolt kasutatavates ruumides ja nõukogu peasekretariaadis kohaldavad nõukogu peasekretariaadi ametnikud ja muud teenistujad, nõukogu peasekretariaati lähetatud töötajad ja nõukogu peasekretariaadiga lepingu sõlminud lepinglased käesolevat otsust.

3. Liikmesriigid võtavad kooskõlas vastavate riigisiseste õigusaktidega kõik asjakohased meetmed tagamaks, et ELi salastatud teabe töötlemisel ja säilitamisel järgivad järgmised isikud käesolevat otsust:

a) Euroopa Liidu juures olevate liikmesriikide alaliste esinduste töötajad ning nõukogu või selle ettevalmistavate organite istungitel või muus nõukogu tegevuses osalevate riiklike delegatsioonide liikmed;

b) muud liikmesriikide valitsusasutuste töötajad, sealhulgas nendesse valitsusasutustesse lähetatud töötajad olenemata sellest, kas nad täidavad oma tööülesandeid asjaomaste liikmesriikide territooriumil või välismaal;

c) muud isikud, kellel on liikmesriikides oma tööülesannete tõttu nõuetekohased volitused juurdepääsuks ELi salastatud teabele, ning

d) liikmesriikidega lepingu sõlminud lepinglased olenemata sellest, kas nad tegutsevad asjaomaste liikmesriikide territooriumil või välismaal.

Artikkel 16

Julgeolekukorraldus nõukogus

1. Selleks et täita oma ülesannet tagada üldine järjepidevus käesoleva otsuse kohaldamisel, kiidab nõukogu heaks:

a) artikli 13 lõike 2 punktis a osutatud lepingud;

b) otsused, millega lubatakse või antakse nõusolek avaldada nõukogust pärit või nõukogus säilitatavat ELi salastatud teavet kolmandatele riikidele ja rahvusvahelistele organisatsioonidele kooskõlas koostaja nõusoleku põhimõttega;

c) julgeolekukomitee soovitatud iga-aastase hindamiskülastuste kava, mis on mõeldud hindamiskülastuste tegemiseks liikmesriikide teenistustesse ja tööruumidesse, käesolevat otsust või selle põhimõtteid kohaldavatesse liidu organitesse, asutustesse ja üksustesse ning hindamiskülastuste tegemiseks kolmandatesse riikidesse ja rahvusvahelistesse organisatsioonidesse, et hinnata ELi salastatud teabe kaitseks rakendatud meetmete tõhusust, ning

▼B

d) artikli 6 lõikes 1 sätestatud julgeolekupoliitikad.

2. Nõukogu peasekretariaadi julgeolekuasutuseks on peasekretär. Seoses sellega täidab peasekretär järgmisi kohustusi:

a) viib ellu nõukogu julgeolekupoliitikat ja vaatab seda regulaarselt läbi;

b) koordineerib liikmesriikide riiklike julgeolekuasutustega kõiki julgeolekuküsimusi, mis puudutavad nõukogu tegevusega seotud salastatud teabe kaitset;

c) annab vastavalt artikli 7 lõikele 3 nõukogu peasekretariaadi ametnikele, muudele teenistujatele ja riikide lähetatud ekspertidele loa juurdepääsuks CONFIDENTIEL UE/EU CONFIDENTIAL või kõrgemal tasemel salastatud teabele;

d) annab vajaduse korral korralduse uurida kõiki nõukogu valduses oleva või nõukogust pärit salastatud teabe tegeliku või kahtlustatava ohtu sattumise või kadumise juhtumeid ning taotleb, et asjaomased julgeolekuasutused osutaksid selliste uurimiste läbiviimisel abi;

e) kontrollib regulaarselt nõukogu peasekretariaadi tööruumides salastatud teabe kaitseks võetud turvameetmeid;

f) korraldab korrapäraseid külastusi, et hinnata ELi salastatud teabe kaitseks võetud turvameetmeid käesolevat otsust või selle põhimõtteid kohaldavates liidu organites, asutustes ja üksustes;

g) hindab koostöös ja kokkuleppel asjaomase riikliku julgeolekuasutusega regulaarselt liikmesriikide teenistustes ja tööruumides ELi salastatud teabe kaitseks võetud turvameetmeid;

h) tagab vajaduse korral turvameetmete koordineerimise salastatud teabe kaitse eest vastutavate liikmesriikide pädevate asutustega ning vajaduse korral kolmandate riikide või rahvusvaheliste organisatsioonidega, sealhulgas selles osas, mis puudutab ELi salastatud teabe julgeolekut ähvardavate ohtude olemust ja seda, milliste vahenditega end nende ohtude eest kaitsta, ning

i) sõlmib artikli 13 lõike 2 punktis b osutatud halduskokkuleppeid.

Nõukogu peasekretariaadi julgeolekubüroo abistab peasekretäri nimetatud kohustuste täitmisel.

3. Liikmesriigid peaksid artikli 15 lõike 3 rakendamiseks tegema järgmist:

a) määrama riikliku julgeolekuasutuse, kes tuuakse ära C liites ja kes vastutab ELi salastatud teabe kaitseks võetavate turvameetmete eest, et:

   i) mis tahes avalik-õigusliku või eraõigusliku riigisisese talituse, organi või asutuse valduses olevat ELi salastatud teavet kaitstaks nii kodu- kui välismaal käesoleva otsuse kohaselt;

   ii) ELi salastatud teabe kaitseks võetud turvameetmeid hinnataks või vaadataks regulaarselt läbi;

▼B

iii) kõik valitsusasutustes või lepinglaste juures töötavad isikud, kellele võidakse anda juurdepääs CONFIDENTIEL UE/EU CONFIDENTIAL või kõrgemal tasemel salastatud teabele, oleks läbinud nõuetekohase julgeolekukontrolli või omaks oma tööülesannete tõttu selleks muid nõuetekohaseid volitusi vastavalt riigisisestele õigusaktidele;

iv) vajaduse korral töötataks välja julgeolekukavad, et vähendada miinimumini ELi salastatud teabe ohtu sattumise või kadumise riski;

v) ELi salastatud teabe kaitsmisega seotud julgeolekuküsimusi koordineeritaks teiste pädevate riiklike asutustega, sealhulgas käesolevas otsuses nimetatud asutustega, ning

vi) vastataks asjakohastele, eelkõige kõigi käesolevat otsust või selle põhimõtteid kohaldavate ELi lepingu V jaotise 2. peatüki alusel loodud liidu organite, asutuste, üksuste, operatsioonide ning ELi eriesindajate ja nende isikkoosseisu liikmete poolt esitatud julgeolekukontrolli läbiviimise taotlustele;

b) tagama, et nende pädevad asutused annavad riigi valitsusele ja tema kaudu nõukogule teavet ja nõu ELi salastatud teabe julgeolekut ähvardavate ohtude olemuse kohta ja selle kohta, milliste vahenditega salastatud teavet nende ohtude eest kaitsta.

Artikkel 17

Julgeolekukomitee

1. Moodustatakse julgeolekukomitee. Julgeolekukomitee vaatab läbi ja annab hinnangu käesoleva otsuse reguleerimisalasse kuuluvatele julgeolekuküsimustele ning esitab nõukogule vajaduse korral oma soovitused.

2. Julgeolekukomitee koosneb liikmesriikide riiklike julgeolekuasutuste esindajatest ning komitee koosolekutel osalevad ka komisjoni ja Euroopa välisteenistuse esindajad. Komitee eesistuja on peasekretär või tema määratud esindaja. Julgeolekukomitee tuleb kokku nõukogu korraldusel või peasekretäri või riikliku julgeolekuasutuse taotlusel.

Kui arutatakse käesolevat otsust või selle põhimõtteid kohaldavate liidu organite, asutuste või üksustega seotud küsimusi, võib komitee koosolekutele kutsuda ka asjaomaste organite, asutuste ja üksuste esindajad.

3. Julgeolekukomitee korraldab oma töö nii, et ta suudab esitada soovitusi konkreetsete julgeolekuvaldkondade kohta. Komitee moodustab infokindluse küsimustega tegeleva ekspertkoosseisu ning vajaduse korral muid ekspertidest koosnevaid koosseise. Komitee koostab selliste ekspertkoosseisude volitused ja saab neilt nende tegevuse kohta aruandeid, sealhulgas vajaduse korral soovitusi nõukogule.

▼B

Artikkel 18

Varasemate otsuste asendamine

1. Käesoleva otsusega tunnistatakse kehtetuks ja asendatakse nõukogu otsus 2011/292/EL ([1]).

2. Kõik nõukogu otsuste 2001/264/EÜ ([2]) ja 2011/292/EL kohaselt ELi salastatud teavet sisaldavad dokumendid on jätkuvalt kaitstud vastavalt käesoleva otsuse asjakohastele sätetele.

Artikkel 19

Jõustumine

Käesolev otsus jõustub *Euroopa Liidu Teatajas* avaldamise päeval.

([1]) Nõukogu 31. märtsi 2011. aasta otsus 2011/292/EL ELi salastatud teabe kaitseks vajalike julgeolekueeskirjade kohta (ELT L 141, 27.5.2011, lk 17).

([2]) Nõukogu 19. märtsi 2001. aasta otsus 2001/264/EÜ, millega võetakse vastu nõukogu julgeolekueeskirjad (EÜT L 101, 11.4.2001, lk 1).

▼B

LISAD

I LISA

Töötajatega seotud julgeolek

II LISA

Füüsiline julgeolek

III LISA

Salastatud teabe haldamine

IV LISA

Side- ja infosüsteemides töödeldava ELi salastatud teabe kaitse

V LISA

Tööstusjulgeolek

VI LISA

Salastatud teabe vahetamine kolmandate riikide ja rahvusvaheliste organisatsioonidega

▼B

I LISA

TÖÖTAJATEGA SEOTUD JULGEOLEK

I. SISSEJUHATUS

1. Käesolev lisa sisaldab sätteid artikli 7 rakendamise kohta. Lisas sätestatakse kriteeriumid, mille alusel on võimalik kindlaks teha, kas isikule võib tema lojaalsust ja usaldusväärsust arvesse võttes anda loa juurdepääsuks ELi salastatud teabele, ning uurimis- ja haldusmenetlused, mida tuleb sellisel juhul järgida.

II. JUURDEPÄÄSU ANDMINE ELi SALASTATUD TEABELE

2. Isikule antakse juurdepääs salastatud teabele pärast seda, kui:

a) tema teadmisvajadus on kindlaks tehtud,

b) teda on teavitatud ELi salastatud teabe kaitseks vajalikest julgeolekueeskirjadest ja -menetlustest ning ta on kinnitanud oma vastutust seoses kõnealuse teabe kaitsmisega, ning

c) CONFIDENTIEL UE/EU CONFIDENTIAL või kõrgemal tasemel salastatud teabe puhul pärast seda, kui:

— talle on antud asjakohase tasemega juurdepääsuluba või tal on ametiülesannetest tulenev juurdepääsuõigus vastavalt riigisisestele õigusaktidele või

— nõukogu peasekretariaadi ametnike, muude teenistujate ja riiklike lähetatud ekspertide puhul, kui nõukogu peasekretariaadi ametisse nimetav asutus on andnud talle kuni teatava kuupäevani juurdepääsu teatud tasemel ELi salastatud teabele kooskõlas punktidega 16–25.

3. Kõik liikmesriigid ja nõukogu peasekretariaat määravad oma struktuurides kindlaks need ametikohad, mis eeldavad juurdepääsu CONFIDENTIEL UE/EU CONFIDENTIAL või kõrgemal tasemel salastatud teabele ja seetõttu nõuavad asjakohase tasemega julgeolekukontrolli läbimist.

III. JUURDEPÄÄSULOA ANDMISE NÕUDED

4. Pärast nõuetekohase taotluse saamist vastutavad riiklikud julgeolekuasutused või muud pädevad riiklikud asutused julgeolekukontrolli läbiviimise tagamise eest oma riigi kodanike suhtes, kes vajavad juurdepääsu CONFIDENTIEL UE/EU CONFIDENTIAL või kõrgemal tasemel salastatud teabele. Kontrolli standardid peavad vastama riigisisestele õigusaktidele, et oleks võimalik anda juurdepääsuluba või kinnitus selle kohta, et isikule võib vajaduse korral anda loa juurdepääsuks ELi salastatud teabele.

5. Kui asjaomane isik elab teise liikmesriigi või kolmanda riigi territooriumil, taotlevad pädevad riiklikud asutused abi elukohariigi pädevalt asutuselt vastavalt riigisisestele õigusaktidele. Liikmesriigid abistavad üksteist julgeolekukontrolli läbiviimisel vastavalt riigisisestele õigusaktidele.

6. Kui see on riigisiseste õigusaktide kohaselt lubatud, siis võivad riiklikud julgeolekuasutused või muud pädevad riiklikud asutused läbi viia julgeolekukontrolli mittekodanike suhtes, kes vajavad juurdepääsu CONFIDENTIEL UE/EU CONFIDENTIAL või kõrgemal tasemel salastatud teabele. Kontrolli standardid peavad vastama riigisisestele õigusaktidele.

▼B

Julgeolekukontrolli kriteeriumid

7. Isiku lojaalsus ja usaldusväärsus seoses tema julgeolekukontrolli läbimisega juurdepääsuks CONFIDENTIEL UE/EU CONFIDENTIAL või kõrgemal tasemel salastatud teabele tehakse kindlaks julgeolekukontrolli abil. Pädev riiklik asutus annab sellise julgeolekukontrolli tulemuste põhjal üldise hinnangu. Julgeolekukontrolli põhikriteeriumid hõlmavad riigisiseste õigusaktidega lubatud ulatuses teavet selle kohta, kas isik:

a) on toime pannud või üritanud toime panna mis tahes spionaaži-, terrorismi-, sabotaaži- või riigireetmisakti või õhutanud mässule, on olnud nende ettevalmistamise kaasosaliseks või aidanud kaasa nende toimepanekule;

b) on või on olnud seotud spioonide, terroristide, saboteerijate või isikutega, keda on põhjendatult eelnimetatuteks peetud, või selliste organisatsioonide või välisriikide esindajatega, kaasa arvatud välisriikide luureteenistuste esindajatega, kes võiks ohustada liidu ja/või liikmesriikide julgeolekut, välja arvatud juhul, kui ametikohustuste täitmise käigus on antud luba selliste sidemete pidamiseks;

c) on või on olnud liikmeks organisatsioonis, mis püüab vägivalla, õõnestus- või muu seadusvastase tegevuse abil muu hulgas kukutada liikmesriigi valitsust, muuta liikmesriigi põhiseaduslikku korda või muuta liikmesriigi valitsuse koosseisu või poliitikat;

d) on või on olnud alapunktis c nimetatud organisatsiooni toetaja, või on või on olnud tihedalt seotud selliste organisatsioonide liikmetega;

e) on tahtlikult varjanud, moonutanud või võltsinud olulist, eelkõige julgeolekualast teavet, või on tahtlikult valetanud julgeolekuankeeti täites või julgeolekukontrolli juurde kuuluva küsitluse käigus;

f) on süüdi mõistetud kriminaalkuriteos või õigusrikkumistes;

g) on alkoholisõltlane, tarvitab ebaseaduslikke uimasteid ja/või kuritarvitab seadusega lubatud uimasteid;

h) peab või on pidanud end ülal viisil, millega võib kaasneda oht muutuda väljapressimise või surveavalduse objektiks;

i) on tegudes või sõnades üles näidanud ebaausust, ebalojaalsust või ebausaldusväärsust;

j) on tõsiselt või korduvalt rikkunud julgeolekueeskirju; või on toime pannud või üritanud toime panna side- ja infosüsteemidega seotud keelatud tegevust; ning

k) võib sattuda surve alla (nt isikul on ühe või mitme ELi mittekuuluva riigi kodakondsus või sugulased või lähedased tuttavad, kes võivad olla sunnitud kuuletuma välisriikide luureteenistustele, terroristlikele rühmitistele või muudele kehtiva korra vastu suunatud organisatsioonidele või isikutele, kelle eesmärgid võivad ohustada liidu ja/või liikmesriikide julgeolekuhuvisid).

▼B

8. Julgeolekukontrolli käigus võidakse vajaduse korral ja kooskõlas riigisiseste õigusaktidega oluliseks pidada ka asjaomase isiku majanduslikku olukorda ja tervise seisundit.

9. Julgeolekukontrolli käigus võidakse vajaduse korral ja kooskõlas riigisiseste õigusaktidega oluliseks pidada ka abikaasa, elukaaslase või lähedase pereliikme käitumist ja nendega seotud asjaolusid.

Kontrollinõuded, mida peab järgima juurdepääsu lubamisel ELi salastatud teabele

Esmakordne juurdepääsuloa andmine

10. Esmakordsel CONFIDENTIEL UE/EU CONFIDENTIAL või SECRET UE/EU SECRET tasemel salastatud teabele juurdepääsuloa andmisel lähtutakse julgeolekukontrolli tulemustest vähemalt viimase viie aasta või isiku 18-aastaseks saamisest möödunud aja kohta, olenevalt sellest, kumb periood on lühem, ning kontroll hõlmab järgmist:

a) sellisele ELi salastatud teabe tasemele vastava julgeolekuankeedi täitmine, millele asjaomane isik võib juurdepääsu vajada; pärast täitmist edastatakse nimetatud ankeet pädevale julgeolekuasutusele;

b) isikusamasuse ja kodakondsuse tuvastamine – kontrollida tuleb isiku sünniaega ja -kohta ning tuvastada tema isikusamasus. Tehakse kindlaks isiku varasem ja praegune kodakondsus; sealjuures tuleb hinnata, kas isik võib sattuda välisriikidest lähtuva mis tahes surve alla, näiteks tingituna eelnevatest elukohtadest või varasematest sidemetest, ning

c) üleriigiliste ja kohalike registrite kontrollimine – tuleb kontrollida riiklikke julgeoleku- ja karistusregistreid, kui viimased on olemas, ja/või teisi võrreldavaid riiklikke ja politseiregistreid. Tuleb kontrollida selliste õiguskaitseasutuste registreid, kelle halduspiirkonnas isik on elanud või töötanud.

11. Esmakordsel TRÈS SECRET UE/EU TOP SECRET tasemel salastatud teabele juurdepääsuloa andmisel lähtutakse julgeolekukontrolli tulemustest vähemalt viimase kümne aasta või isiku 18-aastaseks saamisest möödunud aja kohta, olenevalt sellest, kumb periood on lühem. Alapunktis e sätestatud vestluste läbiviimisel hõlmab kontroll vähemalt viimast seitset aastat või siis isiku 18-aastaseks saamisest möödunud aega, olenevalt sellest, kumb periood on lühem. Lisaks punktis 7 nimetatud kriteeriumitele kontrollitakse TRÈS SECRET UE/EU TOP SECRET taseme juurdepääsulubade andmisel riigisiseste õigusaktidega lubatud ulatuses järgmisi aspekte (neid võib kontrollida ka enne CONFIDENTIEL UE/EU CONFIDENTIAL ja SECRET UE/EU SECRET taseme juurdepääsulubade andmist, kui see on riigisiseste õigusaktidega ette nähtud):

a) majanduslik olukord – hangitakse teavet isiku majandusliku olukorra kohta, et hinnata, kas ta võiks tingituna tõsistest rahalistest raskustest sattuda välis- või kodumaalt lähtuva surve alla, või avastada tema seletamatut jõukust;

▼B

b) haridus – isiku haridusliku tausta kontrollimiseks hangitakse teavet isiku õppimise kohta koolides, kõrgkoolides ja teistes õppeasutustes alates kaheksateistkümnendast eluaastast või uurimist läbi viiva asutuse äranägemisel sobivaks peetud perioodi jooksul;

c) töökohad – hangitakse teavet praeguse ja varasema töö kohta, kusjuures allikatena kasutatakse personaliosakondades säilitatavaid dokumente, tööalaseid iseloomustusi ja aruandeid ning tööandjaid ja ülemusi;

d) sõjaväeteenistus – vajaduse korral kontrollitakse isiku teenistuskäiku relvajõududes ja teenistusest lahkumise asjaolusid ning

e) vestlused – kui riigisisesed õigusaktid seda ette näevad ja võimaldavad, viiakse läbi vestlus või vestlused asjaomase isikuga. Vestlused viiakse samuti läbi teiste isikutega, kes võivad anda erapooletu hinnangu isiku tausta, tegevuse, lojaalsuse ja usaldusväärsuse kohta. Kui asjaomases riigis on tavaks lasta kontrollitaval isikul endal kedagi soovitada, siis tuleb soovitatud isikutega vestelda, välja arvatud juhul, kui sellest loobumiseks on kaalukaid põhjuseid.

12. Täieliku ülevaate saamiseks isiku kohta olemasolevast asjassepuutuvast teabest ning isiku usaldusväärsust kahjustava teabe kinnitamiseks või kummutamiseks võib vajaduse korral ja kooskõlas riigisiseste õigusaktidega läbi viia lisakontrolle.

Juurdepääsuloa kehtivuse pikendamine

13. Pärast juurdepääsuloa esmakordset andmist ja tingimusel, et isik on vaheaegadeta olnud liikmesriigi valitsusasutuse või nõukogu peasekretariaadi teenistuses ja vajab endiselt juurdepääsu ELi salastatud teabele, tuleb juurdepääsuluba kehtivuse pikendamiseks läbi vaadata TRÈS SECRET UE/EU TOP SECRET taseme loa puhul vähemalt iga viie aasta järel ning SECRET UE/EU SECRET ja CONFIDENTIEL UE/EU CONFIDENTIAL taseme lubade puhul vähemalt iga kümne aasta järel alates asjaomaste lubade andmise aluseks olnud viimase julgeolekukontrolli tulemustest teavitamise kuupäevast. Juurdepääsuloa kehtivuse pikendamiseks läbiviidav julgeolekukontroll hõlmab eelmise julgeolekukontrolli läbiviimisest möödunud perioodi.

14. Juurdepääsulubade kehtivuse pikendamisel kontrollitakse punktides 10 ja 11 nimetatud aspekte.

15. Kehtivuse pikendamise taotlused tuleb esitada õigeaegselt, võttes arvesse seda, kui palju aega kulub julgeolekukontrolli läbiviimiseks. Kui asjaomane riiklik julgeolekuasutus või muu pädev riiklik asutus saab asjaomase kehtivuse pikendamise taotluse ja vastava julgeolekuankeedi enne juurdepääsuloa kehtivuse lõppemist ja vajalik julgeolekukontroll ei ole veel lõpule viidud, võib pädev riiklik asutus siiski pikendada olemasoleva juurdepääsuloa kehtivust kuni 12 kuuks, kui see on riigisiseste õigusaktidega lubatud. Kui selle 12-kuulise perioodi lõppedes ei ole julgeolekukontroll ikka veel lõpule viidud, antakse asjaomasele isikule selliseid tööülesandeid, mille täitmine ei nõua juurdepääsuluba.

Lubade andmise kord nõukogu peasekretariaadis

16. Nõukogu peasekretariaadi ametnike ja muude teenistujate puhul edastab nõukogu peasekretariaadi julgeolekuasutus täidetud julgeolekuankeedi selle liikmesriigi riiklikule julgeolekuasutusele, mille kodanik asjaomane isik on, taotledes sellele ELi salastatud teabe tasemele vastava julgeolekukontrolli läbiviimist, millele asjaomane isik juurdepääsu vajab.

▼B

17. Kui nõukogu peasekretariaadile saab teatavaks ELi salajasele teabele juurdepääsuluba taotlevat isikut puudutav julgeolekukontrolli seisukohast oluline teave, teatab nõukogu peasekretariaat asjaomaste õigusaktide kohaselt toimides sellest asjaomasele riiklikule julgeolekuasutusele.

18. Pärast julgeolekukontrolli läbiviimist teatab asjaomane riiklik julgeolekuasutus nõukogu peasekretariaadi julgeolekuasutusele kõnealuse kontrolli tulemusest, kasutades selleks julgeolekukomitee poolt kirjavahetuseks ette nähtud standardvormi.

a) Juhul kui julgeolekukontrolli tulemus kinnitab, et ei ole ilmnenud asjaolusid, mis võiksid isiku lojaalsuse ja usaldusväärsuse kahtluse alla seada, võib nõukogu peasekretariaadi ametisse nimetav asutus anda asjaomasele isikule loa juurdepääsuks vastaval salastatuse tasemel ELi salastatud teabele kuni kindlaksmääratud kuupäevani.

b) Juhul kui julgeolekukontrolli tulemus sellist kinnitust ei anna, teavitab nõukogu peasekretariaadi ametisse nimetav asutus sellest asjaomast isikut, kes võib taotleda, et ametisse nimetav asutus kuulaks ära tema selgitused. Ametisse nimetav asutus võib küsida pädevalt riiklikult julgeolekuasutuselt täiendavaid selgitusi, mille andmine on riigisiseste õigusaktide kohaselt võimalik. Kui tulemus leiab kinnitust, siis ELi salajasele teabele juurdepääsuks luba ei anta.

19. Julgeolekukontrolli, sealhulgas selle tulemuste suhtes kohaldatakse kõnealuses liikmesriigis kehtivaid asjaomaseid õigusakte, sealhulgas edasikaebamise kohta. Nõukogu peasekretariaadi ametisse nimetava asutuse otsuseid võib edasi kaevata vastavalt nõukogu määrusega (EMÜ, Euratom, ESTÜ) nr 259/68 ([1]) kehtestatud Euroopa Liidu ametnike personalieeskirjadele ja Euroopa Liidu muude teenistujate teenistustingimustele („personalieeskirjad ja teenistustingimused”).

20. Riiklikud eksperdid, kes on lähetatud nõukogu peasekretariaati CONFIDENTIEL UE/EU CONFIDENTIAL või sellest kõrgemal tasemel ELi salastatud teabele juurdepääsu nõudvale ametikohale, esitavad enne tööle asumist nõukogu peasekretariaadi julgeolekuasutusele kehtiva juurdepääsutõendi juurdepääsuks ELi salastatud teabele, mille alusel ametisse nimetav asutus annab loa juurdepääsuks ELi salastatud teabele.

21. Nõukogu peasekretariaat tunnustab kõigi muude liidu institutsioonide, organite ja asutuste antud luba juurdepääsuks ELi salastatud teabele, eeldusel et see on kehtiv. Luba hõlmab kõiki tööülesandeid, mida asjaomane isik nõukogu peasekretariaadis täidab. Liidu institutsioon, organ või asutus, kus isik tööle asub, teatab asjaomasele riiklikule julgeolekuasutusele tööandja muutumisest.

22. Kui isiku teenistusperiood ei alga 12 kuu jooksul julgeolekukontrolli tulemuse teatamisest nõukogu peasekretariaadi ametisse nimetavale asutusele või kui isiku teenistus katkeb 12 kuuks, mille jooksul ta ei tööta nõukogu peasekretariaadis või liikmesriigi valitsusasutuse ametikohal, siis pöördutakse kõnealuse tulemuse kehtivuse ja nõuetekohasuse kohta kinnituse saamiseks asjaomase riikliku julgeolekuasutuse poole.

23. Kui nõukogu peasekretariaadile saab teatavaks ELi salastatud teabele juurdepääsuks luba omava isikuga seotud turvariski puudutav teave, teatab nõukogu peasekretariaat asjakohaste õigusaktide kohaselt toimides sellest asjaomasele riiklikule julgeolekuasutusele ning võib peatada juurdepääsu ELi salastatud teabele või sellele juurdepääsuks antud loa tühistada.

([1]) Nõukogu 29. veebruari 1968. aasta määrus (EMÜ, Euratom, ESTÜ) nr 259/68, millega kehtestatakse Euroopa ühenduste ametnike personalieeskirjad ja muude teenistujate teenistustingimused ning komisjoni ametnike suhtes ajutiselt kohaldatavad erimeetmed (EÜT L 56, 4.3.1968, lk 1).

▼B

24. Kui riiklik julgeolekuasutus teatab nõukogu peasekretariaadile ELi salastatud teabele juurdepääsuks luba omava isiku kohta punkti 18 alapunkti a kohaselt antud kinnituse tühistamisest, võib nõukogu peasekretariaadi ametisse nimetav asutus küsida riiklikult julgeolekuasutuselt selgitust, mille andmine on riigisiseste õigusaktide kohaselt võimalik. Kui isiku usaldusväärsust kahjustav teave leiab kinnitust, tühistatakse luba ning isikule keelatakse juurdepääs ELi salastatud teabele ja ametikohtadele, mille puhul selline juurdepääs on võimalik või mille puhul isik võiks ohustada julgeolekut.

25. Nõukogu peasekretariaadi ametnikule või muule teenistujale antud ELi salastatud teabele juurdepääsu loa tühistamise või kehtivuse peatamise otsusest ja vajaduse korral selle põhjustest teavitatakse asjaomast isikut, kes võib taotleda, et ametisse nimetav asutus kuulaks ära tema selgitused. Riikliku julgeolekuasutuse esitatud teabe suhtes kohaldatakse kõnealuses liikmesriigis kehtivaid asjaomaseid õigusakte, sealhulgas edasikaebamise kohta. Nõukogu peasekretariaadi ametisse nimetava asutuse otsuseid võib edasi kaevata vastavalt personalieeskirjadele ja teenistustingimustele.

Juurdepääsulubade ja lubade registrid

26. Liikmesriigid ja nõukogu peasekretariaat peavad salastatuse tasemel CONFIDENTIEL UE/EU CONFIDENTIAL või kõrgemal tasemel teabele juurdepääsuks antud juurdepääsulubade ja lubade vastavaid registreid. Kõnealused registrid sisaldavad vähemalt andmeid selle kohta, millisel salastatuse tasemel ELi salastatud teabele võib asjaomasele isikule juurdepääsu lubada, juurdepääsuloa andmise kuupäeva ja kehtivusaja kohta.

27. Pädev julgeolekuasutus võib väljastada juurdepääsutõendi, millel on kirjas, millisel salastatuse tasemel ELi salastatud teabele võib asjaomasele isikule juurdepääsu lubada (CONFIDENTIEL UE/EU CONFIDENTIAL või kõrgem), vastava ELi salastatud teabele juurdepääsu võimaldava juurdepääsuloa või ELi salastatud teabele juurdepääsu loa kehtivuse lõppemise kuupäev ja tõendi enda kehtivuse lõppemise kuupäev.

Erandid juurdepääsuloa andmise nõudest

28. Nende isikute juurdepääs ELi salastatud teabele, kellel on liikmesriikides oma tööülesannete tõttu selleks nõuetekohased volitused, määratakse kindlaks kooskõlas riigisiseste õigusaktidega; selliseid isikuid teavitatakse nende julgeolekualastest kohustustest seoses ELi salastatud teabe kaitsmisega.

IV. JULGEOLEKUALANE ÕPE JA JULGEOLEKUALASE TEADLIKKUSE SUURENDAMINE

29. Kõik juurdepääsuloa saanud isikud kinnitavad kirjalikult, et nad mõistavad oma kohustusi seoses ELi salastatud teabe kaitsmisega ning on teadlikud tagajärgedest, mis kaasnevad ELi salastatud teabe ohtu sattumisega. Nimetatud kirjalike kinnituste registreid peavad vastavalt liikmesriigid ja nõukogu peasekretariaat.

30. Kõigile isikutele, kellel on luba juurdepääsuks ELi salastatud teabele või kes peavad töötlema ELi salastatud teavet, selgitatakse alguses ning tutvustatakse regulaarselt julgeolekuohte ning nad peavad viivitamata teatama asjaomasele julgeolekuasutusele kõigist lähenemiskatsetest, mida nad peavad kahtlustäratavateks või ebatavalisteks.

31. Kõiki isikuid, kelle töökohustused ei eelda enam juurdepääsu ELi salastatud teabele, teavitatakse nende kohustusest jätkuvalt kaitsta ELi salastatud teavet ning vajaduse korral kinnitavad nad seda kirjalikult.

V. ERANDLIKUD ASJAOLUD

32. Kui see on riigisiseste õigusaktide kohaselt lubatud, võib liikmesriigi pädeva riikliku asutuse väljastatud juurdepääsuloaga, millega antakse juurdepääs riigi salastatud teabele, võimaldada liikmesriigi ametnikele ajutiselt kuni ELi salastatud teabele juurdepääsuloa andmiseni juurdepääsu samaväärse

▼B

salastatuse tasemega ELi salastatud teabele vastavalt B liites esitatud vastavustabelile, kui selline ajutine juurdepääs on liidu huvides nõutav. Riiklikud julgeolekuasutused teavitavad julgeolekukomiteed, kui sellise ajutise juurdepääsu võimaldamine ELi salastatud teabele ei ole riigisiseste õigusaktide kohaselt lubatud.

33. Olukorra kiireloomulisusest tulenevalt ja juhul, kui see on teenistuse huvide tõttu nõuetekohaselt põhjendatud, võib nõukogu peasekretariaadi ametisse nimetav asutus pärast selle liikmesriigi riikliku julgeolekuasutusega konsulteerimist, mille kodanik asjaomane isik on, ning isiku usaldusväärsust kahjustavate asjaolude puudumise kinnitamiseks läbiviidud eelkontrollide tulemusest olenevalt anda enne täieliku julgeolekukontrolli lõpulejõudmist nõukogu peasekretariaadi ametnikele ja muudele teenistujatele konkreetse ülesande täitmiseks ajutise loa juurdepääsuks ELi salastatud teabele. Nimetatud ajutisi lube antakse kuni kuueks kuuks ja need ei võimalda juurdepääsu TRÈS SECRET UE/EU TOP SECRET tasemel salastatud teabele. Kõik ajutise loa saanud isikud kinnitavad kirjalikult, et nad mõistavad oma kohustusi seoses ELi salastatud teabe kaitsmisega ning on teadlikud tagajärgedest, mis kaasnevad ELi salastatud teabe ohtu sattumisega. Nimetatud kirjalike kinnituste registrit peab nõukogu peasekretariaat.

34. Kui isik kavatsetakse määrata ametikohale, mis nõuab kõrgema tasemega juurdepääsuluba, kui isik hetkel omab, võib isiku ajutiselt ametisse määrata tingimusel, et:

a) isiku ülemus põhjendab kirjalikult möödapääsmatut vajadust juurdepääsuks kõrgemal salastatuse tasemel ELi salastatud teabele;

b) juurdepääs piirdub ELi salastatud teabe konkreetsete elementidega, mis on vajalikud tööülesande täitmiseks;

c) isikul on kehtiv juurdepääsuluba või luba juurdepääsuks ELi salastatud teabele;

d) on astutud samme ametikoha jaoks nõutava tasemega juurdepääsuloa saamiseks;

e) pädeva asutuse poolt on piisavalt kontrollitud, et isik ei ole tõsiselt ega korduvalt rikkunud julgeolekueeskirju;

f) isiku ametisse määramine on pädeva asutuse poolt heaks kiidetud ning

g) erandi tegemisega seotud dokumente, kaasa arvatud kirjeldust teabe kohta, millele juurdepääs võimaldati, säilitatakse asjakohases registris või allregistris.

35. Eespool kirjeldatud korda kasutatakse ühekordse juurdepääsu andmiseks ELi salastatud teabele, mille salastatuse tase on ühe astme võrra kõrgem sellest, mille suhtes asjaomane isik on läbinud julgeolekukontrolli. Kõnealust korda ei rakendata korduvalt.

36. Väga erandlike asjaolude korral, näiteks vaenulikus keskkonnas läbiviidavate missioonide või kasvavate rahvusvaheliste pingete ajal, kui erakorralised meetmed seda nõuavad ja eelkõige inimelude päästmise eesmärgil, võivad liikmesriigid ja peasekretär anda võimaluse korral kirjalikult loa juurdepääsuks CONFIDENTIEL UE/EU CONFIDENTIAL või SECRET UE/EU SECRET tasemel salastatud teabele nõutavat juurdepääsuluba mitteomavatele isikutele, tingimusel et selline luba on hädavajalik ning puudub põhjendatud kahtlus asjaomase isiku lojaalsuse ja usaldusväärsuse suhtes. Kõnealuse loa andmisega seotud dokumente, kaasa arvatud kirjeldust teabe kohta, millele juurdepääs võimaldati, säilitatakse registris.

▼B

37. TRÈS SECRET UE/EU TOP SECRET tasemel salastatud teabe puhul antakse kõnealune erakorraline juurdepääs üksnes liidu kodanikele, kellele on lubatud juurdepääs TRÈS SECRET UE/EU TOP SECRET tasemel salastatud teabega samaväärsel tasemel riigisiseselt salastatud teabele või SECRET UE/EU SECRET tasemel salastatud teabele.

38. Punktides 36 ja 37 sätestatud korra kasutamise juhtudest teavitatakse julgeolekukomiteed.

39. Kui liikmesriigi õigusaktidega on ajutiste lubade, ajutise ametissemääramise ning isikutele salastatud teabele ühekordse või erakorralise juurdepääsu andmise suhtes kehtestatud rangemad eeskirjad, siis rakendatakse käesolevas jaos ette nähtud menetlusi vaid asjaomastes riigisisestes õigusaktides sätestatud piirides.

40. Julgeolekukomiteele esitatakse aastaaruanne käesolevas jaos sätestatud menetluste kasutamise kohta.

VI. NÕUKOGUS TOIMUVATEL KOOSOLEKUTEL OSALEMINE

41. Kui punktist 28 ei tulene teisiti, võivad isikud, kellele on tehtud ülesandeks osaleda nõukogu istungitel või nõukogu ettevalmistavate organite koosolekutel, kus käsitletakse CONFIDENTIEL UE/EU CONFIDENTIAL või kõrgemal tasemel salastatud teavet, teha seda alles pärast nende juurdepääsuloa olemasolu kontrollimist. Liikmesriikide esindajate puhul edastavad pädevad asutused juurdepääsutõendi või muud juurdepääsuloa olemasolu kinnitavad tõendid nõukogu peasekretariaadi julgeolekubüroole või erandjuhul esitab selle asjaomane esindaja isiklikult. Vajaduse korral võib kasutada koondnimekirja, milles on esitatud asjaomased juurdepääsuloa olemasolu tõendid.

42. Kui julgeolekuga seotud põhjustel on tühistatud sellise isiku juurdepääsuluba ELi salastatud teabele, kelle tööülesanded nõuavad osalemist nõukogu istungitel või nõukogu ettevalmistavate organite koosolekutel, siis teavitab pädev asutus sellest nõukogu peasekretariaati.

VII. VÕIMALIK JUURDEPÄÄS ELi SALASTATUD TEABELE

43. Kullerid, valvetöötajad ja saatjad peavad läbima nõuetekohase taseme julgeolekukontrolli või riigisiseste õigusaktidega ette nähtud muu asjakohase kontrolli, neid teavitatakse ELi salastatud teabe kaitseks vajalikest julgeolekumenetlustest ning neile antakse juhtnöörid nende hoolde usaldatud ELi salastatud teabe kaitsmiseks.

▼B

II LISA

FÜÜSILINE JULGEOLEK

I. SISSEJUHATUS

1. Käesolev lisa sisaldab sätteid artikli 8 rakendamise kohta. Lisas sätestatakse miinimumnõuded objektide, hoonete, ametiruumide ja muude alade, kus toimub ELi salastatud teabe töötlemine ja säilitamine, sealhulgas side- ja infosüsteeme sisaldavate alade füüsiliseks kaitsmiseks.

2. ELi salastatud teabele volitamata juurdepääsu vältimiseks töötatakse välja füüsilise julgeoleku meetmed, mille eesmärk on:

a) tagada, et ELi salastatud teabe töötlemine ja säilitamine toimub nõuetekohaselt;

b) võimaldada töötajate eristamist seoses juurdepääsuga ELi salastatud teabele nende teadmisvajaduse ja vajaduse korral julgeolekukontrolli läbimise alusel;

c) hoida ära, takistada ja avastada lubamatuid toiminguid ning

d) välistada salajane või jõuga sissetung või tekitada sissetungijatele viivitusi.

II. FÜÜSILISE JULGEOLEKU NÕUDED JA MEETMED

3. Füüsilise julgeoleku meetmed valitakse välja pädevate asutuste poolt läbiviidava ohtude hinnangu alusel. Nõukogu peasekretariaat ja liikmesriigid kohaldavad ELi salastatud teabe kaitseks oma objektidel riskijuhtimisprotsessi, et tagada sellise tasemega füüsiline kaitse, mis on vastavuses hinnatud riskiga. Riskijuhtimisprotsessis võetakse arvesse kõiki asjakohaseid tegureid, eelkõige:

a) ELi salastatud teabe salastatuse taset;

b) ELi salastatud teabe vormi ja hulka, pidades meeles asjaolu, et suurte ELi salastatud teabe koguste või tervikkogumite puhul võib osutuda vajalikuks kohaldada rangemaid kaitsemeetmeid;

c) ELi salastatud teavet sisaldavate hoonete või alade ülesehitust ning neid ümbritsevat keskkonda ning

d) hinnangut ohule, mida kujutavad endast luureteenistused, kelle tegevus on suunatud liidu või liikmesriikide vastu, ning sabotaažist, terrorismist ja õõnestavast või muust kriminaalsest tegevusest tulenevale ohule.

4. Süvakaitse põhimõttele tuginedes määrab pädev julgeolekuasutus kindlaks, milliseid asjakohaseid füüsilise julgeoleku meetmeid rakendada. Need võivad hõlmata üht või mitut järgmistest meetmetest:

a) piirdebarjäär – füüsiline barjäär, mis kaitseb kaitsmist vajava ala piire;

b) sissetungi avastamise süsteemid – sissetungi avastamise süsteemi võib kasutada piirdebarjääri turvalisuse suurendamiseks või ruumides ja hoonetes turvateenistuse asendamiseks või abistamiseks;

▼B

c) juurdepääsu kontroll – juurdepääsu kontrolli võidakse teostada objekti, objektil asuva hoone või hoonete või hoones asuvate alade või ruumide suhtes. Kontrolli võib teostada elektrooniliste või elektromehaaniliste vahendite abil, seda võivad teostada turvateenistujad ja/või administraator või seda võib teostada muude füüsiliste vahendite abil;

d) turvateenistujad – tööle võib võtta vastava väljaõppe ja juhendamisega ning asjakohase julgeolekukontrolli läbinud turvateenistujaid, muu hulgas salajase sissetungi takistamiseks;

e) sisetelevisioonisüsteem – turvateenistujad võivad kasutada sisetelevisioonisüsteemi intsidentide tuvastamiseks ja sissetungi avastamise süsteemi häirete kontrollimiseks suurtel aladel või perimeetril;

f) turvavalgustus – turvavalgustust võidakse kasutada potentsiaalsete sissetungijate eemalhoidmiseks, aga ka pakkumaks turvateenistujale vajalikku valgustust tõhusa järelevalve tegemiseks kas otseselt või kaudselt sisetelevisioonisüsteemi abil, ning

g) muud asjakohased füüsilise julgeoleku meetmed, mille eesmärk on hoida ära või avastada volitamata juurdepääsu või ELi salastatud teabe kahjustamist või kadumist.

5. Pädeval asutusel võib lubada korraldada sisse- ja väljapääsudes läbiotsimisi, et takistada loata esemete toomist objektidele või hoonetesse või sealt ELi salastatud teabe loata väljaviimist.

6. Kui on oht, et ELi salastatud teavet võidakse jälgida, isegi kui see toimub juhuslikult, võetakse selle takistamiseks asjakohaseid meetmeid.

7. Uute rajatiste puhul määratletakse füüsilise julgeoleku nõuded ja nende funktsionaalne kirjeldus osana rajatiste planeerimise ja projekteerimise protsessist. Olemasolevate rajatiste puhul rakendatakse füüsilise julgeoleku nõudeid võimalikult suures ulatuses.

III. ELi SALASTATUD TEABE FÜÜSILISE KAITSMISE SEADMED

8. Pädev julgeolekuasutus tagab ELi salastatud teabe füüsiliseks kaitseks vajalike seadmete (nt seifid, paberipurustajad, ukselukud, elektroonilised juurdepääsu kontrollimise süsteemid, sissetungi avastamise süsteemid, häiresüsteemid) hankimisel, et nimetatud seadmed vastavad heakskiidetud tehnilistele standarditele ja miinimumnõuetele.

9. ELi salastatud teabe füüsiliseks kaitsmiseks kasutatavate seadmete tehnilised kirjeldused sätestatakse julgeolekusuunistes, mille kiidab heaks julgeolekukomitee.

10. Turvasüsteemide tööd kontrollitakse korrapäraste ajavahemike järel ja seadmeid hooldatakse regulaarselt. Hooldustööde tegemisel võetakse arvesse kontrollide tulemusi, et tagada seadmete jätkuv töötamine optimaalsel režiimil.

11. Iga kontrolli käigus vaadatakse konkreetsete turvameetmete ja kogu julgeolekusüsteemi tõhusus uuesti läbi.

IV. FÜÜSILISELT KAITSTUD ALAD

12. ELi salastatud teabe füüsiliseks kaitsmiseks luuakse kaht tüüpi füüsiliselt kaitstud alad või riigisisese süsteemi kohaselt samaväärsed alad:

▼B

a) haldustegevuse alad ning

b) turvaalad (sealhulgas tehniliselt kaitstud turvaalad).

Käesolevas otsuses käsitatakse viiteid haldustegevuse aladele ja turvaaladele (sealhulgas tehniliselt kaitstud turvaaladele) ühtlasi ka viidetena riigisisese süsteemi kohaselt samaväärsetele aladele.

13. Pädev julgeolekuasutus tõendab, et ala vastab nõuetele, mille alusel võib selle tunnistada haldustegevuse alaks, turvaalaks või tehniliselt kaitstud turvaalaks.

14. Haldustegevuse alade puhul:

a) kehtestatakse selgelt määratletud välispiir, mis võimaldab kontrollida isikuid ja võimaluse korral sõidukeid;

b) võimaldatakse alale siseneda ilma saatjata ainult isikutel, keda pädev asutus on selleks nõuetekohaselt volitanud, ning

c) viibivad kõik muud isikud alal alati koos saatjaga või läbivad samaväärse kontrolli.

15. Turvaalade puhul:

a) kehtestatakse selgelt määratletud ja kaitstud välispiir, millesse sisenemist ja millest väljumist kontrollitakse läbipääsulubade või isikutuvastussüsteemi abil;

b) võimaldatakse alale siseneda ilma saatjata ainult isikutel, kes on läbinud julgeolekukontrolli ja kellel on nende teadmisvajadusest tulenevalt sisenemiseks eriluba; ning

c) viibivad kõik muud isikud alal alati koos saatjaga või läbivad samaväärse kontrolli.

16. Juhul kui turvaalale sisenemine tähendab praktiliselt otsest juurdepääsu alas asuvale salastatud teabele, kohaldatakse järgmisi täiendavaid nõudeid:

a) peab olema selgelt märgitud, milline on kõnealusel alal tavaliselt hoitava teabe kõrgeim salastatuse tase;

b) kõigil külastajatel peab olema alale sisenemiseks eriluba, nad viibivad alal alati koos saatjaga ning nad peavad olema läbinud nõuetekohase julgeolekukontrolli, välja arvatud juhul, kui rakendatud on meetmeid, mis muudavad juurdepääsu ELi salastatud teabele võimatuks.

17. Pealtkuulamise vastu kaitstud turvaalad määratakse tehniliselt kaitstud turvaaladena. Kohaldatakse järgmisi täiendavaid nõudeid:

a) alad varustatakse sissetungi avastamise süsteemiga; kui alad ei ole kasutuses, need lukustatakse, ja kui alad on kasutusel, neid valvatakse. Kõiki võtmeid kontrollitakse vastavalt VI jaole;

b) kõiki sellistele aladele sisenevaid isikuid ja esemeid kontrollitakse;

▼B

c) selliseid alasid tuleb vastavalt pädeva julgeolekuasutuse nõudmistele regulaarselt füüsiliselt ja/või tehniliselt kontrollida. Sellised kontrollid viiakse läbi ka iga loata sisenemise või sellise sisenemise kahtluse korral ning

d) sellistele aladele ei paigaldata loata sideliine, telefone ega muid sidevahendeid, elektri- või elektroonilisi seadmeid.

18. Olenemata punkti 17 alapunktist d vaatab pädev julgeolekuasutus enne SECRET UE/EU SECRET ja kõrgemal tasemel salastatud teabega seonduvate koosolekute toimumiseks või töö tegemiseks ette nähtud alade kasutamist, ning kui ohtu ELi salastatud teabele hinnatakse suureks, üle kõik sidevahendid ja elektri- või elektroonikaseadmed, tagamaks et selliste seadmetega ei saa edastada teavet tahtmatult ega varjatult arusaadaval kujul väljapoole turvaala piire.

19. Turvaalasid, kus töötajad ei viibi ööpäevaringselt, kontrollitakse vajaduse korral tavapärase tööaja lõppedes ja pisteliselt väljaspool tavapärast tööaega, välja arvatud juhul, kui alale on paigaldatud sissetungi avastamise süsteem.

20. Haldustegevuse ala piires võib ajutiselt luua turvaalasid või tehniliselt kaitstud turvaalasid salastatud teavet käsitlevate koosolekute pidamiseks või muul samalaadsel eesmärgil.

21. Iga turvaala jaoks töötatakse välja turvanõuete rakendamise kord, milles määratakse kindlaks järgmised asjaolud:

a) millise tasemega ELi salastatud teavet võib kõnealusel alal töödelda ja säilitada;

b) alal kohaldatavad järelevalve- ja kaitsemeetmed;

c) isikud, kellel on nende teadmisvajadusest ja vastava juurdepääsuloa olemasolust tulenevalt lubatud alale siseneda saatjata;

d) vajaduse korral saatjatega või ELi salastatud teabe kaitsega seotud kord muudele isikutele alale juurdepääsu võimaldamisel ning

e) muud asjakohased meetmed ja toimingud.

22. Turvaaladele ehitatakse turvakambrid. Turvakambrite seinad, põrandad, laed, aknad ja lukustatavad uksed peavad olema pädeva julgeolekuasutuse poolt heaks kiidetud ja pakkuma samaväärset kaitset kui samal tasemel ELi salastatud teabe säilitamiseks heakskiidetud seifid.

V. FÜÜSILISED KAITSEMEETMED ELi SALASTATUD TEABE TÖÖTLEMISEKS JA SÄILITAMISEKS

23. RESTREINT UE/EU RESTRICTED tasemel ELi salastatud teavet võib töödelda:

a) turvaalal;

b) haldustegevuse alal, tingimusel et ELi salastatud teave on kaitstud volitamata isikute juurdepääsu eest, või

▼B

c) väljaspool turvaala või haldustegevuse ala, tingimusel et valdaja veab ELi salastatud teavet vastavalt III lisa punktidele 28–41 ja kohustub järgima pädeva julgeolekuasutuse kehtestatud julgeolekujuhistes sätestatud kompenseerivaid meetmeid, mis tagavad ELi salastatud teabe kaitse volitamata isikute juurdepääsu eest.

24. RESTREINT UE/EU RESTRICTED tasemel ELi salastatud teavet säilitatakse sobivas lukustatud kontorimööblis haldustegevuse alal või turvaalal. Seda võib ajutiselt säilitada väljaspool turvaala või haldustegevuse ala, tingimusel et valdaja kohustub järgima pädeva julgeolekuasutuse kehtestatud julgeolekujuhistes sätestatud kompenseerivaid meetmeid.

25. CONFIDENTIEL UE/EU CONFIDENTIAL või SECRET UE/EU SECRET tasemel ELi salastatud teavet võib töödelda:

a) turvaalal;

b) haldustegevuse alal, tingimusel et ELi salastatud teave on kaitstud volitamata isikute juurdepääsu eest, või

c) väljaspool turvaala või haldustegevuse ala, tingimusel et valdaja:

i) veab ELi salastatud teavet vastavalt III lisa punktidele 28–41;

ii) kohustub järgima pädeva julgeolekuasutuse kehtestatud julgeolekujuhistes sätestatud kompenseerivaid meetmeid, mis tagavad ELi salastatud teabe kaitse volitamata isikute juurdepääsu eest;

iii) hoiab ELi salastatud teavet kogu aeg isikliku järelevalve all ning

iv) on paberkujul dokumentide puhul teavitanud sellest asjakohast registrit.

26. CONFIDENTIEL UE/EU CONFIDENTIAL või SECRET UE/EU SECRET tasemel ELi salastatud teavet säilitatakse turvaalal kas seifis või turvakambris.

27. TRÈS SECRET UE/EU TOP SECRET tasemel ELi salastatud teavet töödeldakse turvaalal.

28. TRÈS SECRET UE/EU TOP SECRET tasemel ELi salastatud teavet säilitatakse turvaalal ühel järgmistest tingimustest:

a) seifis vastavalt punktile 8, kasutades ühte või mitut järgmistest täiendavatest kontrollimeetmetest:

i) pidev kaitse või kontrollimine julgeolekukontrolli läbinud turvateenistujate või valvetöötajate poolt;

ii) heakskiidetud sissetungi avastamise süsteem koos turvateenistuse reageerimisüksusega;

b) sissetungi avastamise süsteemiga varustatud turvakambris, mille juurde kuulub turvateenistuse reageerimisüksus.

▼B

29. Eeskirjad ELi salastatud teabe veo kohta väljaspool füüsiliselt kaitstud alasid on esitatud III lisas.

VI. ELi SALASTATUD TEABE KAITSEKS KASUTATAVATE VÕTMETE JA KOODIDE JÄRELEVALVE

30. Pädev julgeolekuasutus määrab kindlaks ametiruumide, muude ruumide, turvakambrite ja seifide võtmete ja koodide haldamise korra. Selline kord peab kaitsma volitamata juurdepääsu eest.

31. Koodid tuleb pähe õppida ja koode teadvate isikute arv peab olema võimalikult väike. ELi salastatud teabe säilitamiseks kasutatavate seifide ja turvakambrite koode muudetakse:

a) uue konteineri saabumisel;

b) kõnealust koodi teadva personali koosseisu muutumise korral;

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

d) kui lukku on hooldatud või parandatud ning

e) vähemalt iga 12 kuu järel.

▼B

III LISA

SALASTATUD TEABE HALDAMINE

I. SISSEJUHATUS

1. Käesolev lisa sisaldab sätteid artikli 9 rakendamise kohta. Selles sätestatakse haldusmeetmed ELi salastatud teabe kontrollimiseks kogu selle kasutusaja jooksul, et aidata ära hoida ja avastada sellise teabe teadlik või juhuslik ohtu sattumine või kadumine.

II. SALASTATUSE TASEMETE HALDAMINE

Salastatuse tasemed ja märked

2. Teave peab olema salastatud, kui see vajab kaitset seoses oma salajasusega.

3. ELi salastatud teabe koostaja vastutab selle salastatuse taseme määramise eest vastavalt asjaomastele salastamise suunistele ning teabe esialgse levitamise eest.

4. ELi salastatud teabe salastatuse tase määratakse kindlaks artikli 2 lõike 2 kohaselt ja lähtudes artikli 3 lõike 3 kohaselt heaks kiidetud julgeolekupoliitikast.

5. Salastatuse tase peab olema selgelt ja täpselt märgitud, olenemata sellest, kas ELi salastatud teave on paberkandjal, suuline või elektroonilises või muus vormis.

6. Ühe dokumendi eri osad (st leheküljed, lõigud, jaotised, lisad, liited, manused ja täiendused) võivad vajada erineval tasemel salastamist ning need tähistatakse vastavalt, sealhulgas nende säilitamisel elektroonilises vormis.

7. Dokumendi või faili üldine salastatuse tase on vähemalt sama kõrge kui selle kõige kõrgema salastatuse tasemega osal. Erinevatest allikatest pärineva teabe koondamisel vaadatakse lõpptulemus üle, et määrata kindlaks üldine salastatuse tase, sest vajalikuks võib osutuda dokumendi üksikosadele määratust kõrgem salastatuse tase.

8. Võimaluse korral liigendatakse erinevatel tasemetel salastatud osi sisaldav dokument selliselt, et selle erinevatel tasemetel salastatud osad on kergesti tuvastatavad ja vajaduse korral eraldatavad ülejäänud dokumendist.

9. Kui dokumentidele on lisatud kiri või teade, määratakse sellele kõige kõrgema salastatuse tasemega dokumendi salastatuse tase. Kirja või teate koostaja märgib täpselt, milline on selle salastatuse tase ilma lisatud dokumentideta, kasutades selleks asjakohast märget, näiteks:

CONFIDENTIEL UE/EU CONFIDENTIAL

Manus(t)eta RESTREINT UE/EU RESTRICTED

Märked

10. Lisaks ühele artikli 2 lõikes 2 nimetatud salastusmärkele võib ELi salastatud teave kanda täiendavat märget, nagu:

a) teabe koostajale viitav tunnus;

b) piirangud, koodsõnad või lühendid, millega täpsustatakse dokumendiga seotud tegevusvaldkonda, dokumendi levitamist üksnes teadmisvajaduse põhjal või kasutuspiiranguid;

c) avaldatavuse märked või

▼B

d) vajaduse korral kuupäev või konkreetne sündmus, pärast mida võib salastatuse taset alandada või salastatuse kustutada.

Salastusmärgete lühendid

11. Teksti üksikute lõikude salastatuse taseme märkimiseks võib kasutada salastatuse taseme standardlühendeid. Sellised lühendid ei asenda salastusmärke täielikku varianti.

12. ELi salastatud dokumentides võib lühemate kui ühe lehekülje pikkuste tekstilõikude salastatuse taseme märkimisel kasutada järgmisi standardlühendeid:

TRÈS SECRET UE/EU TOP SECRET	TS-UE/EU-TS
SECRET UE/EU SECRET	S-UE/EU-S
CONFIDENTIEL UE/EU CONFIDENTIAL	C-UE/EU-C
RESTREINT UE/EU RESTRICTED	R-UE/EU-R

ELi salastatud dokumentide koostamine

13. ELi salastatud dokumendi koostamisel:

a) märgitakse igale leheküljele selgelt salastatuse tase;

b) nummerdatakse iga lehekülg;

c) peab dokumendil olema kirjas viitenumber ja teema, mis ei ole salastatud teave, välja arvatud kui see on sellisena tähistatud;

d) märgitakse dokumendile koostamise kuupäev ning

e) SECRET UE/EU SECRET ja kõrgemal tasemel salastatud dokumentidele kantakse koopia number igale leheküljele, kui antakse välja mitu koopiat.

14. Kui punkti 13 ei ole võimalik ELi salastatud teabe suhtes kohaldada, võetakse vastavalt artikli 6 lõikele 2 koostatavatele julgeolekusuunistele muid sobivaid meetmeid.

ELi salastatud teabe salastatuse taseme alandamine ja salastatuse kustutamine

15. Teabe koostamise ajal märgib koostaja võimaluse korral ning eelkõige RESTREINT UE/EU RESTRICTED tasemel salastatud teabe puhul, kas ELi salastatud teabe salastatuse taset võib teataval kuupäeval või konkreetse sündmuse järel alandada või selle kustutada.

16. Nõukogu peasekretariaat vaatab korrapäraselt läbi tema valduses oleva ELi salastatud teabe, et teha kindlaks, kas salastatuse tase on jätkuvalt kehtiv. Nõukogu peasekretariaat kehtestab süsteemi, mille abil vaadatakse mitte harvem kui iga viie aasta järel läbi sellise ELi salastatud teabe salastatuse tase, mille on koostanud nõukogu peasekretariaat. Selline läbivaatamine ei ole vajalik, kui teabe koostaja on juba alguses osutanud, et teabe salastatuse taset alandatakse või salastatus kustutatakse automaatselt, ning teave on vastavalt tähistatud.

III. ELi SALASTATUD TEABE REGISTREERIMINE JULGEOLEKUKAALUTLUSTEL

17. Iga ELi salastatud teavet töötleva nõukogu peasekretariaadi ja liikmesriikide valitsusasutuste struktuuriüksuse jaoks määratakse kindlaks vastutav register, et tagada ELi salastatud teabe töötlemine käesoleva otsuse kohaselt. Registrid luuakse II lisas määratletud turvaaladena.

▼B

18. Käesolevas otsuses tähendab julgeolekukaalutlustel registreerimine („registreerimine”) menetluste kohaldamist, mille abil talletatakse andmed materjali kogu kasutusaja iga etapi, sealhulgas selle levitamise ja hävitamise kohta.

19. Kogu CONFIDENTIEL UE/EU CONFIDENTIAL ja sellest kõrgemal tasemel salastatud materjal registreeritakse selleks määratud registrites, kui see saabub asutuse struktuuriüksusesse või kui see sealt välja saadetakse.

20. Nõukogu peasekretariaadi keskregistris peetakse arvet kogu salastatud teabe üle, mida nõukogu ja nõukogu peasekretariaat edastavad kolmandatele riikidele ja rahvusvahelistele organisatsioonidele, ja kogu salastatud teabe üle, mis neilt saadakse.

21. Side- ja infosüsteemi puhul võib registreerimiseks kasutada side- ja infosüsteemis sisalduvaid protsesse.

22. Nõukogu kiidab heaks julgeolekupoliitika ELi salastatud teabe julgeolekukaalutlustel registreerimise kohta.

TRÈS SECRET UE/EU TOP SECRET TASEMEL SALASTATUD DOKUMENTIDE REGISTRID

23. Liikmesriikides ja nõukogu peasekretariaadis määratakse üks register toimima TRÈS SECRET UE/EU TOP SECRET tasemel salastatud teabe keskse vastuvõtva ja edastava asutusena. Vajaduse korral võib määrata allregistreid kõnealust teavet registreerimise eesmärgil töötlema.

24. Sellised allregistrid ei tohi edastada TRÈS SECRET UE/EU TOP SECRET tasemel salastatud dokumente otse teistele sama TRÈS SECRET UE/EU TOP SECRET keskregistri allregistritele või väljapoole ilma nimetatud keskregistri sõnaselge nõusolekuta.

IV. ELi SALASTATUD DOKUMENTIDE KOPEERIMINE JA TÕLKIMINE

25. TRÈS SECRET UE/EU TOP SECRET tasemel salastatud dokumente ei tohi kopeerida ega tõlkida ilma selle koostaja eelneva kirjaliku nõusolekuta.

26. Kui SECRET UE/EU SECRET ja sellest madalamal tasemel salastatud dokumentide koostaja ei ole seadnud piiranguid nende kopeerimise või tõlkimise suhtes, siis võib dokumendi valdaja ülesandel neid kopeerida või tõlkida.

27. Originaaldokumendi suhtes kohaldatavaid turvameetmeid rakendatakse ka selle dokumendi koopiate ja tõlgete suhtes.

V. ELi SALASTATUD TEABE VEDU

28. ELi salastatud teabe vedamise suhtes kohaldatakse punktides 30–41 ette nähtud kaitsemeetmeid. Kui ELi salastatud teavet veetakse elektroonilisel andmekandjal, ja olenemata artikli 9 lõikest 4, võib allpool esitatud kaitsemeetmeid täiendada asjakohaste tehniliste vastumeetmetega, mis nähakse ette pädeva julgeolekuasutuse poolt, et minimeerida teabe ohtu sattumise või kadumise riski.

29. Pädevad julgeolekuasutused nõukogu peasekretariaadis ja liikmesriikides väljastavad juhised ELi salastatud teabe vedamiseks käesoleva otsuse kohaselt.

Hoones või hoonete kompleksis

30. Hoones või hoone tekompleksis veetav ELi salastatud teave tuleb kinni katta, et vältida selle sisu märkamise võimalust.

▼B

31. Hoones või hoonete kompleksis veetakse TRÈS SECRET UE/EU TOP SECRET tasemel salastatud teavet turvaümbrikus, millele on märgitud üksnes adressaadi nimi.

Liidu piires

32. Liidu piires hoonete või valduste vahel veetav ELi salastatud teave pakendatakse selliselt, et see on kaitstud teabe loata avaldamise eest.

33. CONFIDENTIEL UE/EU CONFIDENTIAL ja SECRET UE/EU SECRET tasemel salastatud teabe vedu liidus toimub ühel järgmistest viisidest:

a) vastavalt vajadusele kas sõjalise, valitsuse või diplomaatilise kulleriga;

b) käsipostiga, tingimusel et:

i) ELi salastatud teave on kogu aeg vedaja valduses, välja arvatud kui seda hoitakse vastavalt II lisas sätestatud nõuetele;

ii) ELi salastatud teavet ei avata teeloleku ajal ega loeta avalikes kohtades;

iii) isikuid teavitatakse nende vastutusest seoses julgeolekuga ning

iv) isikutele antakse vajaduse korral kulleri sertifikaat;

c) postiteenuste või kommertskullerteenuste kaudu, tingimusel et:

i) need on asjaomase riikliku julgeolekuasutuse poolt vastavalt riigisisestele õigusaktidele heaks kiidetud ning

ii) nad kohaldavad asjakohaseid kaitsemeetmeid, mis vastavad artikli 6 lõike 2 kohaselt koostatavates julgeolekusuunistes kehtestatud miinimumnõuetele.

Kui vedu toimub ühest liikmesriigist teise, piirdub alapunkti c sätete kohaldamine kuni CONFIDENTIEL UE/EU CONFIDENTIAL tasemeni salastatud teabega.

34. RESTREINT UE/EU RESTRICTED tasemel salastatud teavet võib vedada ka postiteenuste või kommertskullerteenuste kaudu. Sellise teabe vedamiseks kullerisertifikaati ei nõuta.

35. CONFIDENTIEL UE/EU CONFIDENTIAL või SECRET UE/EU SECRET tasemel salastatud materjali (nt seadet või masinat), mida ei saa vedada punktis 33 nimetatud viisidel, tuleb V lisa kohaselt vedada kaubana transpordiettevõtjate poolt.

36. TRÈS SECRET UE/EU TOP SECRET tasemel salastatud teabe vedu liidu piires hoonete või valduste vahel toimub vastavalt vajadusele sõjalise, valitsuse või diplomaatilise kulleriga.

Vedu liidust kolmanda riigi territooriumile

37. Liidust kolmanda riigi territooriumile veetav ELi salastatud teave pakendatakse selliselt, et see on kaitstud teabe loata avaldamise eest.

▼B

38. CONFIDENTIEL UE/EU CONFIDENTIAL või SECRET UE/EU SECRET tasemel salastatud teabe vedu liidust kolmanda riigi territooriumile toimub ühel järgmistest viisidest:

a) sõjalise või diplomaatilise kulleriga;

b) käsipostiga, tingimusel et:

i) pakil on ametlik pitser või on pakendil märge, mis näitab, et tegemist on ametliku saadetisega, ja see ei läbi tolli- või turvakontrolli;

ii) isikutel on vastava paki kohta antud kullerisertifikaat, mis annab neile loa seda pakki vedada;

iii) ELi salastatud teave on kogu aeg vedaja valduses, välja arvatud kui seda hoitakse vastavalt II lisas sätestatud nõuetele;

iv) ELi salastatud teavet ei avata teeloleku ajal ega loeta avalikes kohtades ning

v) isikuid teavitatakse nende vastutusest seoses julgeolekuga.

39. Liidu poolt kolmandale riigile või rahvusvahelisele organisatsioonile edastatud CONFIDENTIEL UE/EU CONFIDENTIAL või SECRET UE/EU SECRET tasemel salastatud teabe vedu peab vastama artikli 13 lõike 2 punkti a või b kohaselt sõlmitud salastatud teabe kaitse lepingu või halduskokkuleppe asjaomastele sätetele.

40. RESTREINT UE/EU RESTRICTED tasemel salastatud teavet võib vedada ka postiteenuste või kommertskullerteenuste kaudu.

41. TRÈS SECRET UE/EU TOP SECRET tasemel salastatud teabe vedu liidust kolmanda riigi territooriumile toimub sõjalise või diplomaatilise kulleriga.

VI. ELi SALASTATUD TEABE HÄVITAMINE

42. ELi salastatud dokumendid, mida ei ole enam vaja, võib hävitada, ilma et see piiraks arhiveerimist puudutavaid asjaomaseid õigusnorme.

43. Artikli 9 lõike 2 kohaselt registreerimisele kuuluvad dokumendid hävitab vastutav register dokumendi valdaja või pädeva asutuse ülesandel. Registreerimisraamatud ja muu registreerimisteave ajakohastatakse vastavalt.

44. SECRET UE/EU SECRET või TRÈS SECRET UE/EU TOP SECRET tasemel salastatud dokumentide hävitamise juures viibib tunnistaja, kes on läbinud vähemalt hävitatava dokumendi salastatuse tasemele vastava julgeolekukontrolli.

45. Registripidaja ja tunnistaja, kui viimase kohalolek on nõutav, kirjutavad alla dokumendi hävitamisaktile, mis antakse hoiule registrisse. Registris säilitatakse TRÈS SECRET UE/EU TOP SECRET tasemel salastatud dokumentide hävitamisakte vähemalt kümme aastat ja CONFIDENTIEL UE/EU CONFIDENTIAL ning SECRET UE/EU SECRET tasemel salastatud dokumentide hävitamisakte vähemalt viis aastat.

46. Salastatud, sealhulgas RESTREINT UE/EU RESTRICTED tasemel salastatud dokumendid hävitatakse viisil, mis vastab asjakohastele liidu

▼B

või samaväärsetele standarditele, või mis on liikmesriikide poolt heaks kiidetud vastavalt riigisisestele tehnilistele standarditele, et takistada nende täielikku või osalist taastamist.

47. ELi salastatud teabe salvestamiseks kasutatud elektrooniliste salvestusvahendite hävitamine toimub vastavalt IV lisa punktile 37.

48. Hädaolukorras, kus esineb ELi salastatud teabe otsene loata avalikustamise oht, hävitab teabe valdaja selle viisil, mis teeb võimatuks ELi salastatud teabe tervikliku või osalise taastamise. Koostajat ja päritoluregistrit teavitatakse registreeritud ELi salajase teabe hävitamisest hädaolukorra tõttu.

VII. HINDAMISKÜLASTUSED

49. Mõistet „hindamiskülastus” kasutatakse, et tähistada:

a) artikli 9 lõike 3 ning artikli 16 lõike 2 punktide e, f ja g kohaseid kontrolle või hindamiskülastusi või

b) artikli 13 lõike 5 kohast hindamiskülastust,

mille eesmärk on hinnata ELi salastatud teabe kaitsmiseks rakendatavate meetmete tõhusust.

50. Hindamiskülastustel on muu hulgas järgmised eesmärgid:

a) tagada, et järgitakse käesolevas otsuses ELi salastatud teabe kaitseks kehtestatud nõutavaid miinimumstandardeid;

b) rõhutada julgeoleku ja tõhusa riskijuhtimise olulisust kontrollitavates asutustes;

c) soovitada vastumeetmeid salastatud teabe salajasuse, tervikluse või käideldavuse kadumisest tuleneva konkreetse mõju leevendamiseks ning

d) tõhustada julgeolekuasutustes käimasolevaid julgeolekualase väljaõppe ning teadlikkuse parandamise programme.

51. Enne iga kalendriaasta lõppu võtab nõukogu vastu artikli 16 lõike 1 punktis c ette nähtud hindamiskülastuste kava järgmiseks aastaks. Iga hindamiskülastuse konkreetne kuupäev määratakse kindlaks kokkuleppel asjaomase liidu organi või asutuse, liikmesriigi, kolmanda riigi või rahvusvahelise organisatsiooniga.

Hindamiskülastuste korraldamine

52. Hindamiskülastusi korraldatakse selleks, et kontrollida hinnatava üksuse asjakohaste eeskirjade ja menetluste ning ka üksuse töötavade vastavust käesolevas otsuses sätestatud aluspõhimõtetele ja miinimumstandarditele ning kõnealuse üksusega toimuva salastatud teabe vahetamist reguleerivatele sätetele.

53. Hindamiskülastusi korraldatakse kahes osas. Enne tegelikku külastust peetakse vajaduse korral ettevalmistav koosolek asjaomase üksusega. Pärast kõnealust ettevalmistavat koosolekut koostab hindamisrühm kokkuleppel asjaomase üksusega üksikasjaliku hindamiskülastuse kava, mis hõlmab kõiki julgeolekuvaldkondi. Hindamiskülastuse rühmal peaks olema juurdepääs mis tahes kohale, kus töödeldakse ELi salastatud teavet, eelkõige registritele ning side- ja infosüsteemide paiknemise kohtadele.

54. Hindamiskülastused liikmesriikide valitsusasutustesse, kolmandatesse riikidesse ja rahvusvahelistesse organisatsioonidesse toimuvad täielikus koostöös külastatava üksuse, kolmanda riigi või rahvusvahelise organisatsiooni ametnikega.

▼B

55. Hindamiskülastusi liidu organitesse, asutustesse ja üksustesse, kus kohaldatakse käesolevat otsust või selle põhimõtteid, viiakse läbi selle liikmesriigi julgeolekuasutuse ekspertide abiga, kelle territooriumil organ või asutus asub.

56. Hindamiskülastuste läbiviimisel liidu organitesse, asutustesse ja üksustesse, kus kohaldatakse käesolevat otsust või selle põhimõtteid, ning kolmandatesse riikidesse ja rahvusvahelistesse organisatsioonidesse võidakse taotleda liikmesriigi julgeolekuasutuste ekspertide abi ja panustamist vastavalt julgeolekukomitee poolt heaks kiidetud üksikasjalikule korrale.

Aruanded

57. Hindamiskülastuse lõpus esitatakse külastatud üksusele peamised järeldused ja soovitused. Seejärel koostatakse aruanne hindamiskülastuse kohta. Juhul kui on tehtud ettepanekuid parandusmeetmeteks või esitatud soovitusi, lisatakse aruandesse piisavalt üksikasjalikku teavet tehtud järelduste toetamiseks. Aruanne edastatakse külastatud üksuse asjaomasele asutusele.

58. Liikmesriikide valitsusasutustes teostatavate hindamiskülastuste puhul:

a) edastatakse hindamisaruande kavand asjaomasele riiklikule julgeolekuasutusele, et kontrollida faktide õigsust ja seda, et aruanne ei sisaldaks RESTREINT UE/EU RESTRICTED tasemest kõrgemal tasemel salastatud teavet, ning

b) saadetakse hindamisaruanded nõukogu julgeolekukomiteele, kui asjaomane liikmesriigi julgeolekuasutus ei taotle aruande üldise levitamise keelamist; aruanne salastatakse RESTREINT UE/EU RESTRICTED tasemel.

Nõukogu peasekretariaadi julgeolekuasutuse (julgeolekubüroo) vastutusel koostatakse korrapärane aruanne, milles tuuakse esile liikmesriikides kindlaksmääratud ajavahemiku jooksul teostatud hindamiskülastuste käigus saadud õppetunnid, ning julgeolekukomitee vaatab selle läbi.

59. Kolmandatesse riikidesse ja rahvusvahelistesse organisatsioonidesse tehtud hindamiskülastuste puhul saadetakse aruanne julgeolekukomiteele. Aruanne salastatakse vähemalt RESTREINT UE/EU RESTRICTED tasemel. Parandusmeetmeid kontrollitakse järelkülastuse ajal ning nendest teavitatakse julgeolekukomiteed.

60. Käesolevat otsust või selle põhimõtteid kohaldavatesse liidu organitesse, asutustesse ja üksustesse tehtud hindamiskülastuste puhul saadetakse aruanded julgeolekukomiteele. Hindamiskülastuse aruande kavand edastatakse asjaomasele organile või asutusele, et kontrollida faktide õigsust ja seda, et aruanne ei sisaldaks RESTREINT UE/EU RESTRICTED tasemest kõrgemal tasemel salastatud teavet. Parandusmeetmeid kontrollitakse järelkülastuse ajal ning nendest teavitatakse julgeolekukomiteed.

61. Nõukogu peasekretariaadi julgeolekuasutus kontrollib punktis 50 sätestatud eesmärkidel korrapäraselt nõukogu peasekretariaadi struktuuriüksusi.

Kontroll-loend

62. Hindamiskülastuse käigus kontrollitavate objektide loendi koostab ja seda ajakohastab nõukogu peasekretariaadi julgeolekuasutus (julgeolekubüroo). Kõnealune kontroll-loend edastatakse julgeolekukomiteele.

63. Kontroll-loendi koostamiseks vajalik teave saadakse eelkõige külastuse ajal kontrollitava üksuse julgeolekutöötajatelt. Pärast kontroll-loendi täitmist üksikasjalike vastustega salastatakse see vastavalt kontrollitud üksusega kokku lepitule. Kontroll-loend ei ole kontrolliaruande osa.

▼B

IV LISA

SIDE- JA INFOSÜSTEEMIDES TÖÖDELDAVA ELi SALASTATUD TEABE KAITSE

I. SISSEJUHATUS

1. Käesolev lisa sisaldab sätteid artikli 10 rakendamise kohta.

2. Toimingute julgeoleku tagamiseks ja nõuetekohaseks läbiviimiseks side- ja infosüsteemis on olulised järgmised infokindluse omadused ja mõisted:

autentsus:	tagatis, et teave on ehtne ja pärineb heausksest allikast;
käideldavus:	teave on volitatud isiku taotluse korral kättesaadav ja kasutatav;
salajasus:	teavet ei avalikustata volitamata isikutele, üksustele või töötlemiseks;
terviklus:	teabe ja süsteemi osade täpsuse ja terviklikkuse kaitse;
salgamise vääramine:	võime tõestada tegevuse või sündmuse toimumist selliselt, et kõnealuse sündmuse või tegevuse toimumist ei saa hiljem eitada.

II. INFOKINDLUSE PÕHIMÕTTED

3. Allpool esitatavad sätted on iga side- ja infosüsteemi, milles töödeldakse ELi salastatud teavet, turvalisuse aluseks. Kõnealuste sätete rakendamise üksikasjalikud nõuded määratakse kindlaks infokindluse julgeolekupoliitikates ja julgeolekusuunistes.

Turvariski juhtimine

4. Turvariski juhtimine on side- ja infosüsteemi määratlemise, arendamise, kasutamise ja haldamise lahutamatu osa. Riskijuhtimist (hindamine, käsitlemine, aktsepteerimine ja teavitamine) viiakse läbi süsteemiomanike, projekteerimisasutuste, töötlejate ja julgeolekualase heakskiidu andmise asutuste esindajate poolt ühiselt järkjärgulise protsessina, kasutades tõestatud, läbipaistvat ja täielikult arusaadavat riskihindamise protsessi. Side- ja infosüsteemi ulatus ja selle osad määratakse selgelt kindlaks riskijuhtimisprotsessi alguses.

5. Pädevad asutused käsitlevad side- ja infosüsteeme ähvardavaid võimalikke ohtusid ning koostavad ajakohased ja täpsed riskihinnangud, mis kajastavad olemasolevat töökeskkonda. Nad ajakohastavad pidevalt oma teadmisi süsteemi haavatavuse küsimustes ning vaatavad regulaarselt läbi haavatavust käsitlevad hinnangud, et ajakohastada neid vastavalt muutustele infotehnoloogia valdkonnas.

6. Turvariski käsitlemise eesmärk on kohaldada kindlat hulka turvameetmeid, mis tagavad rahuldava tasakaalu kasutajate nõudmiste, kulude ja turvalisuse jääkriski vahel.

7. Konkreetsed nõuded, nende ulatus ja üksikasjalikkuse aste, mille määrab kindlaks side- ja infosüsteemi akrediteerimise eest vastutav asjaomane turvalisuse akrediteerimise asutus, peavad olema vastavuses hinnatud ohuga, mille puhul on arvesse võetud kõiki olulisi tegureid, sealhulgas side- ja infosüsteemis töödeldava ELi salastatud teabe salastatuse taset. Akrediteerimine hõlmab jääkriski käsitleva ametliku dokumendi koostamist ja jääkriski aktsepteerimist vastutava asutuse poolt.

▼B

Julgeolek side- ja infosüsteemi kogu kasutusaja jooksul

8. Julgeoleku tagamine on nõutav side- ja infosüsteemi kogu kasutusaja jooksul alates selle kasutusele võtmisest kuni kasutusest kõrvaldamiseni.

9. Side- ja infosüsteemi kogu kasutusaja iga etapi puhul tehakse kindlaks iga sellega seotud osaleja roll ja tegevus seoses nimetatud süsteemi julgeolekuga.

10. Kõigi side- ja infosüsteemide, sealhulgas nende tehniliste ja mittetehniliste turvameetmete suhtes viiakse akrediteerimisprotsessi käigus läbi turvatestid, et tagada, et on saavutatud sobiv kindluse tase, ning teha kindlaks, et need süsteemid on nõuetekohaselt rakendatud, integreeritud ja konfigureeritud.

11. Turvalisuse hindamine, kontrollimine ja läbivaatamine toimub regulaarselt side- ja infosüsteemi kasutamise ja hooldamise ajal ning samuti erakorraliste asjaolude tekkimisel.

12. Side- ja infosüsteemi julgeolekualane dokumentatsioon kujuneb süsteemi kasutusaja jooksul muudatuste ja konfiguratsiooni haldamise protsessi lahutamatu osana.

Parim tava

13. Nõukogu peasekretariaat ja liikmesriigid teevad koostööd, et töötada välja parim tava side- ja infosüsteemis töödeldava ELi salastatud teabe kaitseks. Parimat tava käsitlevates suunistes kirjeldatakse side- ja infosüsteemi tehnilisi, füüsilisi, organisatsioonilisi ja menetluslikke turvameetmeid, mille tõhusus teadaolevate ohtude tõrjumisel ja haavatavuse kõrvaldamisel on tõendatud.

14. Side- ja infosüsteemides töödeldava ELi salastatud teabe kaitsel tuginetakse nii liidus kui ka väljaspool liitu asuvate infokindlusega tegelevate asutuste kogemustele.

15. Parima tava levitamine ja edasine rakendamine aitab saavutada ühtse infokindluse taseme nõukogu peasekretariaadi ja liikmesriikide poolt kasutatavate erinevate side- ja infosüsteemide puhul, milles töödeldakse ELi salastatud teavet.

Süvakaitse

16. Side- ja infosüsteemidega seotud riskide maandamiseks rakendatakse erinevaid tehnilisi ja mittetehnilisi mitme kaitseliinina võetavaid turvameetmeid. Need kaitseliinid on muu hulgas järgmised:

    a) *tõrje:* turvameetmed mõjutamaks side- ja infosüsteemi vastast rünnakut kavandavaid isikuid kavatsusest loobuma;

    b) *ennetamine:* side- ja infosüsteemi vastase rünnaku takistamiseks või blokeerimiseks mõeldud turvameetmed;

    c) *avastamine:* side- ja infosüsteemi vastu toimuva rünnaku avastamiseks mõeldud turvameetmed;

    d) *vastupidavus:* turvameetmed, mille eesmärk on tagada rünnaku minimaalne mõju teabele või side- ja infosüsteemi osadele ja vältida edasise kahju tekitamist, ning

    e) *taastamine:* side- ja infosüsteemi kasutamiseks turvalise olukorra taastamiseks mõeldud turvameetmed.

    Selliste turvameetmete tugevusaste määratakse kindlaks vastavalt riskihinnangule.

17. Riiklik julgeolekuasutus või muu pädev asutus tagab järgmise:

    a) küberkaitsevõime rakendamine, et reageerida ohtudele, mis võivad ületada organisatsiooni ja riigi piire, ning

▼B

b) reageeringute kooskõlastamine ja kõnealuste ohtude, intsidentide ja nendega seotud riskide jagamine (arvuti turvarikkele reageerimise võime).

Minimaalsuse ja privileegide piiratuse põhimõte

18. Toimimiseks vajalike nõuete täitmiseks rakendatakse üksnes hädavajalikke funktsioone, seadmeid ja teenuseid, et vältida asjatut riski.

19. Õnnetusjuhtumitest, vigadest või side- ja infosüsteemi loata kasutamisest tuleneva kahju piiramiseks antakse side- ja infosüsteemi kasutajatele ja automatiseeritud protsessidele vaid selline juurdepääs, õigused ja volitused, mis on neile vajalik oma ülesannete täitmiseks.

20. Side- ja infosüsteemi poolt teostatavat logimist kontrollitakse vajaduse korral akrediteerimisprotsessi käigus.

Infokindluse alane teadlikkus

21. Side- ja infosüsteemide julgeoleku esimeseks kaitseliiniks on riskide teadvustamine ja turvameetmete olemasolu. Eelkõige peavad kõik side- ja infosüsteemiga selle kasutusaja jooksul kokku puutuvad töötajad, sealhulgas kasutajad, mõistma järgmist:

a) turvanõuete rikkumine võib oluliselt kahjustada side- ja infosüsteeme;

b) omavahelise ühendatuse ja sõltuvuse tõttu võivad kahjustada muud süsteemid ning

c) isikud omavad vastavalt oma rollile süsteemides ja protsessides isiklikku vastutust ja kohustusi seoses side- ja infosüsteemi turvalisusega.

22. Turvalisusega seotud vastutuse mõistmise tagamiseks on infokindluse alane koolitus ja teadlikkust parandav koolitus kohustuslik kõigile asjaomastele töötajatele, sealhulgas kõrgema astme juhtkonnale ning side- ja infosüsteemi kasutajatele.

Infotehnoloogia turvatoodete hindamine ja heakskiitmine

23. Turvameetmete usaldatavus, mida väljendatakse infokindluse taseme kaudu, määratakse kindlaks riskijuhtimisprotsessi tulemuste põhjal ning kooskõlas asjaomaste julgeolekupoliitikate ja julgeolekusuunistega.

24. Infokindluse taset kontrollitakse rahvusvaheliselt tunnustatud või riiklikult heakskiidetud protsesside ja meetodite abil. See hõlmab esmast hindamist, kontrolli ja auditeerimist.

25. ELi salastatud teabe kaitsmiseks kasutatavaid krüptovahendeid hindab ja annab neile heakskiidu liikmesriigi krüptovahendite heakskiitmise asutus.

26. Enne krüptovahenditele artikli 10 lõike 6 kohase nõukogu või peasekretäri heakskiidu soovitamist on kõnealused krüptovahendid läbinud edukalt sellise liikmesriigi nõuetekohase pädevusega asutuse poolt teostatud teise poole hindamise, kes ei ole seotud seadme väljatöötamise ega tootmisega. Teise poole teostatava hindamise nõutav põhjalikkuse aste sõltub asjaomaste toodete abil kaitstava ELi salastatud teabe maksimaalsest salastatuse tasemest. Nõukogu kiidab heaks julgeolekupoliitika krüptovahendite hindamise ja heakskiitmise kohta.

27. Kui see on õigustatud konkreetsetel operatiivsetel põhjustel, võib vastavalt vajadusele kas nõukogu või peasekretär loobuda julgeolekukomitee soovitusel käesoleva lisa punktis 25 või 26 sätestatud nõuetest ja anda artikli 10 lõikes 6 sätestatud korras konkreetseks tähtajaks ajutise heakskiidu.

▼B

28. Nõukogu, kes tegutseb julgeolekukomitee soovitusel, võib aktsepteerida kolmanda riigi või rahvusvahelise organisatsiooni krüptovahendite hindamis-, valiku- ja heakskiitmismenetlust ning lugeda seega sellised krüptovahendid sobivaks kaitsma kõnealusele riigile või rahvusvahelisele organisatsioonile edastatavat ELi salastatud teavet.

29. Nõuetekohase pädevusega asutus on liikmesriigi krüptovahendite heakskiitmise asutus, kes on nõukogu poolt kehtestatud kriteeriumite alusel akrediteeritud teostama teise poolena nende krüptovahendite hindamist, mis on mõeldud ELi salastatud teabe kaitsmiseks.

30. Nõukogu kiidab heaks julgeolekupoliitika mittekrüpteerivate infotehnoloogia turvatoodete kvalifitseerimise ja heakskiitmise kohta.

Edastamine turvaaladel ja haldustegevuse aladel

31. Olenemata käesoleva otsuse sätetest võib ELi salastatud teabe edastamisel turvaalade või haldustegevuse alade piires kasutada siiski riskijuhtimisprotsessi tulemuste alusel ja turvalisuse akrediteerimise asutuse loal teabe krüpteerimata edastamist või madalamal tasemel krüpteerimist.

Side- ja infosüsteemide turvaline ühendamine

32. Käesolevas otsuses tähendab omavaheline ühendus kahe või enama infotehnoloogia süsteemi vahelist otseühendust, mille eesmärgiks on andmete ja muude teaberessursside (nt side) ühesuunaline või mitmesuunaline jagamine.

33. Side- ja infosüsteem käsitab igat temaga ühendatud infotehnoloogia süsteemi esialgu ebausaldusväärsena ja rakendab salastatud teabe vahetuse kontrollimiseks kaitsemeetmeid.

34. Kõigi side- ja infosüsteemi mõne teise infotehnoloogia süsteemiga ühendamiste puhul tuleb täita järgmised põhinõuded:

a) selliste ühenduste töö- või kasutamisnõuded kehtestavad ja kinnitavad pädevad asutused;

b) ühendus peab läbima riskijuhtimis- ja akrediteerimisprotsessi ja on nõutav pädeva turvalisuse akrediteerimise asutuste heakskiit ning

c) kõigi side- ja infosüsteemide ühenduspunktides rakendatakse kaitseteenuseid (Boundary Protection Services).

35. Akrediteeritud side- ja infosüsteemi ei ühendata kaitsmata või avaliku võrguga, välja arvatud juhul, kui side- ja infosüsteem on kiitnud heaks kaitseteenuse, mida rakendatakse sellel eesmärgil side- ja infosüsteemi ning kaitsmata või avaliku võrgu vahel. Selliste omavaheliste ühendustega seotud turvameetmed vaatab läbi pädev infokindluse asutus ja kiidab heaks pädev turvalisuse akrediteerimise asutus.

Kui kaitsmata või avalikku võrku kasutatakse üksnes ülekandeks ja andmed on krüpteeritud sellise krüptovahendiga, mis on heaks kiidetud artikli 10 kohaselt, ei loeta sellist ühendust omavaheliseks ühenduseks.

36. TRÈS SECRET UE/EU TOP SECRET tasemel salastatud teabe töötlemiseks akrediteeritud side- ja infosüsteemi vahetu või astmeline ühendamine kaitsmata või avaliku võrguga on keelatud.

Elektroonilised salvestuskandjad

37. Elektroonilised salvestuskandjad tuleb hävitada pädeva julgeolekuasutuse poolt heaks kiidetud korra kohaselt.

▼B

38. Elektrooniliste salvestuskandjate taaskasutamine, nende salastatuse taseme alandamine või salastatuse kustutamine toimub vastavalt artikli 6 lõikele 2 koostatavatele julgeolekusuunistele.

Erakorralised asjaolud

39. Olenemata käesoleva otsuse sätetest võib erakorraliste asjaolude, nagu ähvardava või reaalse kriisi, konflikti, sõjaolukorra või operatiivsete erakorraliste asjaolude korral rakendada allpool kirjeldatud konkreetseid protseduure.

40. ELi salastatud teavet võib pädeva asutuse nõusolekul edastada, kasutades madalama salastatuse taseme jaoks heakskiidetud krüptovahendeid või krüpteerimata, kui mis tahes viivitus põhjustaks selgelt suuremat kahju kui salastatud teabe avalikuks saamisega kaasnev kahju ja kui:

a) teabe saatja ja saaja käsutuses ei ole kas nõutavat või ühtegi krüptoseadet ning

b) salastatud materjali õigeaegne edastamine muude vahendite abil ei ole võimalik.

41. Punktis 39 kirjeldatud asjaolude korral edastatud salastatud teavet ei tähistata märgete või tunnustega, mis eristavad seda salastamata teabest või teabest, mida on võimalik kaitsta olemasoleva krüptovahendiga. Teabe saajaid teavitatakse salastatuse tasemest viivitamatult muude vahendite abil.

42. Kui kohaldatakse punkti 39, esitatakse vastav aruanne pädevale asutusele ja julgeolekukomiteele.

III. INFOKINDLUSE TAGAMISE TOIMINGUD JA ASUTUSED

43. Liikmesriikides ja nõukogu peasekretariaadis kehtestatakse järgmised allpool kirjeldatud infokindluse tagamise toimingud. Kõnealused toimingud ei nõua eraldi struktuuriüksuste moodustamist. Neil on eraldi volitused. Siiski võib kõnealuseid toiminguid ja nendega kaasnevaid vastutusi ühendada või integreerida samasse struktuuriüksusesse või jagada erinevatesse struktuuriüksustesse, tingimusel et välditakse sisemist huvide või ülesannete konflikti.

Infokindluse asutus

44. Infokindluse asutuse ülesanded on järgmised:

a) töötada välja infokindluse julgeolekupoliitikad ja julgeolekusuunised ning jälgida nende tõhusust ja asjakohasust;

b) kaitsta ja hallata krüptovahenditega seotud tehnilist teavet;

c) tagada ELi salastatud teabe kaitsmiseks valitud infokindluse meetmete vastavus nende kõlblikkust ja valikut reguleerivale asjakohasele poliitikale;

d) tagada, et krüptovahendid valitakse vastavalt nende kõlblikkuse ja valiku alasele poliitikale;

e) infokindluse alase koolituse ja teadlikkuse koordineerimine;

f) konsulteerida infokindluse julgeolekupoliitikate ja julgeolekusuuniste osas süsteemi tarnija, turvalisuse eest vastutajate ning kasutajate esindajatega ning

g) tagada, et julgeolekukomitee ekspertkoosseisul, mis tegeleb infokindluse küsimustega, on juurdepääs asjakohastele infokindluse alastele eriteadmistele.

▼B

TEMPEST-asutus

45. TEMPEST-asutus vastutab selle eest, et side- ja infosüsteemid oleksid kooskõlas TEMPESTi poliitika ja suunistega. Asutus kiidab heaks TEMPESTi vastumeetmed selliste seadmete ja toodete jaoks, mis on mõeldud kindlaksmääratud salastatuse tasemel ELi salastatud teabe kaitsmiseks nende töökeskkonnas.

Krüptovahendite heakskiitmise asutus

46. Krüptovahendite heakskiitmise asutuse kohustus on tagada, et krüptovahendid oleksid kooskõlas vastavalt liikmesriikide või nõukogu krüpteerimispoliitikaga. Asutus annab ELi salastatud teabe kaitsmiseks mõeldud krüptovahenditele heakskiidu kindlaksmääratud salastatuse tasemel ELi salastatud teabe töötlemiseks nimetatud toote töökeskkonnas. Liikmesriikide puhul vastutab krüptovahendite heakskiitmise asutus lisaks ka krüptovahendite hindamise eest.

Krüptomaterjalide jaotamise asutus

47. Krüptomaterjalide jaotamise asutuse ülesanded on järgmised:

a) ELi krüptomaterjali haldamine ja arvepidamine selle üle;

b) asjakohaste protseduuride täitmise ja kanalite loomise tagamine ELi krüptomaterjali üle arvepidamise, turvalise töötlemise, säilitamise ja levitamise tagamiseks ning

c) ELi krüptomaterjalide neid kasutavatele isikutele või talitustele edastamise või selliste materjalide neid kasutavatelt isikutelt või talitustelt vastuvõtmise tagamine.

Turvalisuse akrediteerimise asutus

48. Süsteemi turvalisuse akrediteerimise asutuse ülesanded on järgmised:

a) tagada, et side- ja infosüsteem vastab asjaomastele julgeolekupoliitikatele ja julgeolekusuunistele; anda side- ja infosüsteemile heakskiitmise teatis kinnitamaks, et süsteemi töökeskkonnas võib töödelda kindlaksmääratud salastatuse tasemel ELi salastatud teavet; määrata kindlaks akrediteerimise tingimused ning kriteeriumid, mille alusel nõutakse uue heakskiidu andmist;

b) kehtestada vastavalt asjaomastele poliitikatele turvalisuse akrediteerimise protsess, milles on selgelt esitatud turvalisuse akrediteerimise asutuse pädevusalasse kuuluvate side- ja infosüsteemide heakskiitmise tingimused;

c) määratleda turvalisuse akrediteerimise strateegia, milles on esitatud akrediteerimisprotsessi põhjalikkuse aste, mis on vastavuses nõutava kindluse tasemega;

d) vaadata läbi ja kinnitada turvadokumentatsioon, sealhulgas riskijuhtimise ja jääkriski teatised, süsteemispetsiifiliste turvanõuete teatised, turvanõuete rakendamise kontrollimise dokumentatsioon ja turvanõuete rakendamise kord, ning tagada dokumentatsiooni vastavus nõukogu julgeolekueeskirjadele ja -poliitikatele;

e) kontrollida turvameetmete rakendamist seoses side- ja infosüsteemidega, teostades või rahastades turvaanalüüse, kontrolli või ülevaateid;

f) kindlaks määrata julgeolekualased nõuded (nt juurdepääsu lubade tasemed) side- ja infosüsteemi suhtes tundlike ametikohtade jaoks;

g) kinnitada side- ja infosüsteemis turvalisuse tagamiseks kasutatavate heakskiidetud krüptovahendite ja TEMPEST-toodete valik;

▼B

h) kiita heaks side- ja infosüsteemi ühendamine muude side- ja infosüsteemidega või vajaduse korral osaleda ühises heakskiitmises ning

i) konsulteerida süsteemi tarnija, turvalisuse eest vastutajate ning kasutajate esindajatega turvariski juhtimise küsimustes, eelkõige jääkriski ning heakskiitmise teatise tingimuste osas.

49. Nõukogu peasekretariaadi turvalisuse akrediteerimise asutus vastutab kõigi nõukogu peasekretariaadi pädevusse kuuluvates valdkondades kasutatavate side- ja infosüsteemide akrediteerimise eest.

50. Liikmesriigi asjaomane turvalisuse akrediteerimise asutus vastutab liikmesriigi pädevusse kuuluvates valdkondades kasutatavate side- ja infosüsteemide ning nende osade akrediteerimise eest.

51. Nii nõukogu peasekretariaadi kui ka liikmesriikide turvalisuse akrediteerimise asutuste pädevusse kuuluvatesse valdkondadesse kuuluvate side- ja infosüsteemide puhul vastutab akrediteerimise eest ühine turvalisuse akrediteerimise amet. Sellesse kuulub iga liikmesriigi turvalisuse akrediteerimise asutuse esindaja ja selle tegevustest võtab osa komisjoni turvalisuse akrediteerimise asutuse esindaja. Kõnealuse süsteemi aruteludele kutsutakse osalema muid üksusi, kelle sõlmpunktid on side- ja infosüsteemis.

Ühist turvalisuse akrediteerimise ametit juhib nõukogu peasekretariaadi turvalisuse akrediteerimise asutuse esindaja. Ühine turvalisuse akrediteerimise amet teeb otsuseid side- ja infosüsteemis sõlmpunkte omavate institutsioonide, liikmesriikide ja muude üksuste turvalisuse akrediteerimise asutuste esindajate vahelise konsensuse alusel. Ühine turvalisuse akrediteerimise amet esitab oma tegevuse kohta julgeolekukomiteele korrapäraselt aruandeid ja teavitab julgeolekukomiteed kõigist akrediteerimisteatistest.

Infokindluse rakendusasutus

52. Süsteemi infokindluse rakendusasutuse ülesanded on järgmised:

a) töötada välja turvadokumentatsioon kooskõlas turvapoliitika ja julgeolekusuunistega, eelkõige jääkriski käsitlevat avaldust sisaldav süsteemispetsiifiliste turvanõuete teatis, turvanõuete rakendamise kord ning side- ja infosüsteemi akrediteerimise protsessi raames koostatav krüptoplaan;

b) osaleda süsteemispetsiifiliste tehnilise turvalisuse meetmete, seadmete ja tarkvara valimises ja katsetamises, teostada järelevalvet nende rakendamise üle ja tagada nende turvaline paigaldamine, konfigureerimine ja haldamine kooskõlas asjakohase turvadokumentatsiooniga;

c) osaleda TEMPESTi turvameetmete ja seadmete valimises, kui see on süsteemispetsiifiliste turvanõuete teatises nõutud, ja tagada koostöös TEMPEST-asutusega nende turvaline paigaldamine ja hooldus;

d) teostada järelevalvet turvalisusega seotud töökorra rakendamise ja kohaldamise üle ning vajaduse korral delegeerida turvalisusega seotud töökohustusi süsteemi omanikule;

e) hallata ja töödelda krüptovahendeid, tagades krüpto- ja kontrollitavate vahendite säilitamine, ning vajaduse korral tagada krüpteerimisvariantide genereerimine;

f) teostada turvaanalüüsi läbivaatamist ja katsetamist, eelkõige koostada turvalisuse akrediteerimise asutuse nõudel asjakohaseid riskiaruandeid;

g) pakkuda side- ja infosüsteemispetsiifilist infokindluse alast koolitust ning

h) rakendada ja kasutada side- ja infosüsteemispetsiifilisi turvameetmeid.

▼B

V LISA

TÖÖSTUSJULGEOLEK

I. SISSEJUHATUS

1. Käesolev lisa sisaldab sätteid artikli 11 rakendamise kohta. Selles sätestatakse üldised julgeolekunõuded, mida kohaldatakse tööstus- ja muudele ettevõtetele lepingueelsetel läbirääkimistel ja nõukogu peasekretariaadi poolt sõlmitud salastatud lepingute kogu kehtivusaja jooksul.

2. Nõukogu kiidab heaks tööstusjulgeolekut puudutavad suunised, milles visandatakse eelkõige üksikasjalikud nõuded seoses töötlemislubadega, julgeolekuaspekte käsitlevate dokumentidega, külastustega ning ELi salastatud teabe edastamise ja vedamisega.

II. SALASTATUD LEPINGUTE TURVAELEMENDID

Salastatuse taseme määramise juhend

3. Enne salastatud lepingu sõlmimist või sellise lepingu sõlmimise pakkumismenetluse algatamist määrab nõukogu peasekretariaat kui lepingu sõlmija kindlaks pakkujatele ja lepinglastele edastatava teabe salastatuse taseme ning samuti lepinglaste poolt loodava teabe salastatuse taseme. Selleks koostab nõukogu peasekretariaat lepingu täitmiseks kasutatava salastatuse taseme määramise juhendi.

4. Salastatud lepingu eri osade salastatuse taseme määramisel kohaldatakse järgmisi põhimõtteid:

a) salastatuse taseme määramise juhendi koostamisel võtab nõukogu peasekretariaat arvesse kõiki asjaomaseid julgeolekuaspekte, sealhulgas salastatuse taset, mille teabe koostaja on määranud lepingus kasutatavale ja heakskiidetud teabele;

b) lepingu üldine salastatuse tase ei või olla madalam kui selle mis tahes osa kõrgeim salastatuse tase ning

c) lepingu täitmise käigus lepinglaste loodud või neile esitatud teabe salastatuse taseme muutumise korral ning kui hiljem muudetakse salastatuse taseme määramise juhendit, võtab nõukogu peasekretariaat vajaduse korral ühendust liikmesriikide riikliku julgeolekuasutuse / määratud julgeolekuasutuse või muu asjaomase pädeva julgeolekuasutusega.

Julgeolekuaspekte käsitlev dokument

5. Lepinguga seotud konkreetseid julgeolekunõudeid kirjeldatakse julgeolekuaspekte käsitlevas dokumendis. Julgeolekuaspekte käsitlev dokument sisaldab vajaduse korral salastatuse taseme määramise juhendit ning see on salastatud lepingu või all-lepingu lahutamatu osa.

6. Julgeolekuaspekte käsitlev dokument sisaldab sätteid, milles nõutakse, et lepinglane ja/või all-lepinglane järgiks käesolevas otsuses sätestatud miinimumstandardeid. Kõnealuste miinimumstandardite eiramine võib olla piisav alus lepingu lõpetamiseks.

Programmi/projekti julgeolekujuhised (julgeolekujuhised)

7. Sõltuvalt ELi salastatud teabele juurdepääsu või selle töötlemist või säilitamist hõlmavate programmide või projektide ulatusest võib programmi või projekti juhtimiseks määratud lepingu sõlmija koostada konkreetsed

▼B

programmi/projekti julgeolekujuhised. Programmi/projekti julgeolekujuhised peab heaks kiitma liikmesriigi riiklik julgeolekuasutus / määratud julgeolekuasutus või muu programmis/projektis osalev pädev julgeolekuasutus ning need võivad sisaldada täiendavaid julgeolekunõudeid.

III. TÖÖTLEMISLUBA

8. Töötlemisloa väljastab riiklik julgeolekuasutus / määratud julgeolekuasutus või liikmesriigi muu pädev julgeolekuasutus tõendamaks vastavalt riigisisestele õigusaktidele, et tööstus- või muu üksus suudab oma valdustes kaitsta asjaomasel salastatuse tasemel (CONFIDENTIEL UE/EU CONFIDENTIAL või SECRET UE/EU SECRET) ELi salastatud teavet. See esitatakse nõukogu peasekretariaadile kui lepingu sõlmijale enne, kui lepinglasele või all-lepinglasele või potentsiaalsele lepinglasele või all-lepinglasele tohib edastada ELi salastatud teavet või võimaldada sellele juurdepääsu.

9. Töötlemisloa väljastamisel peab asjaomane riiklik julgeolekuasutus või määratud julgeolekuasutus vähemalt:

a) hindama tööstus- või muu üksuse terviklikkust;

b) hindama omandiõigust, kontrolli või lubamatu mõju võimalikkust, mida saaks turvariskiks pidada;

c) kontrollima, et tööstus- või muu üksus on kehtestanud julgeolekusüsteemi, mis hõlmab kõiki asjakohaseid turvameetmeid, mis on vajalikud CONFIDENTIEL UE/EU CONFIDENTIAL või SECRET UE/EU SECRET tasemel salastatud teabe või materjali kaitsmiseks vastavalt käesolevas otsuses esitatud nõuetele;

d) kontrollima, et CONFIDENTIEL UE/EU CONFIDENTIAL või SECRET UE/EU SECRET tasemel salastatud teabele juurdepääsu vajavate juhtkonna liikmete, omanike ja töötajate julgeolekustaatus on kindlaks määratud käesolevas otsuses sätestatud nõuete kohaselt, ning

e) kontrollima, et tööstus- või muu üksus on määranud ametisse julgeolekuametniku, kes vastutab juhtkonna ees julgeolekuga seotud kohustuste täitmise eest kõnealuses üksuses.

10. Kui see on asjakohane, teavitab nõukogu peasekretariaat lepingu sõlmijana asjakohast riiklikku julgeolekuasutust või määratud julgeolekuasutust või muud pädevat julgeolekuasutust sellest, et lepingueelses etapis või lepingu täitmiseks on vaja töötlemisluba. Töötlemis- või juurdepääsuluba on lepingueelses etapis nõutav, kui pakkumismenetluse käigus on vaja väljastada CONFIDENTIEL UE/EU CONFIDENTIAL või SECRET UE/EU SECRET tasemel ELi salastatud teavet.

11. Kui nõutakse töötlemisluba, ei anna lepingu sõlmija eelistatud pakkujale täitmiseks salastatud lepingut enne, kui on saadud kinnitus selle liikmesriigi riiklikult julgeolekuasutuselt, määratud julgeolekuasutuselt või muult pädevalt julgeolekuasutuselt, kus on asjaomase lepinglase või all-lepinglase asukoht, et on väljastatud nõuetekohane töötlemisluba.

12. Töötlemisloa väljastanud riiklik julgeolekuasutus / määratud julgeolekuasutus või muu pädev julgeolekuasutus teavitab nõukogu peasekretariaati

▼B

kui lepingu sõlmijat kõigist töötlemisloaga seotud muudatustest. All-lepingust teavitatakse julgeolekuasutust / määratud julgeolekuasutust või muud pädevat julgeolekuasutust.

13. Töötlemisloa tühistamine asjaomase riikliku julgeolekuasutuse / määratud julgeolekuasutuse või muu pädeva julgeolekuasutuse poolt on nõukogu peasekretariaadile piisav alus lepingu sõlmijana salastatud lepingu lõpetamiseks või pakkuja hankekonkursilt kõrvaldamiseks.

IV. ELi SALASTATUD LEPINGUD JA ALL-LEPINGUD

14. Pakkujale lepingueelses etapis ELi salastatud teabe edastamise korral sisaldab pakkumiskutse sätet, millega kohustatakse osalejat, kes pakkumist ei esita või kes ei osutu väljavalituks, tagastama kindlaksmääratud tähtaja jooksul kõik salastatud dokumendid.

15. Salastatud lepingu või all-lepingu sõlmimise järel teavitab nõukogu peasekretariaat lepingu sõlmijana lepinglase või all-lepinglase riiklikku julgeolekuasutust / määratud julgeolekuasutust või muud pädevat julgeolekuasutust salastatud lepinguga seotud julgeolekusätetest.

16. Salastatud lepingute lõpetamisel teatab nõukogu peasekretariaat lepingu sõlmijana (ja all-lepingu puhul vajaduse korral kas riiklik julgeolekuasutus / määratud julgeolekuasutus või muu pädev julgeolekuasutus) sellest viivitamata selle liikmesriigi riiklikule julgeolekuasutusele / määratud julgeolekuasutusele või muule pädevale julgeolekuasutusele, kus lepinglane või all-lepinglane on registreeritud.

17. Üldiselt nõutakse, et lepinglane või all-lepinglane tagastab salastatud lepingu või all-lepingu lõpetamisel tema valduses oleva ELi salastatud teabe lepingu sõlmijale.

18. Erisätteid ELi salastatud teabe hävitamiseks lepingu täitmise jooksul või lõpetamisel sätestatakse julgeolekuaspekte käsitlevas dokumendis.

19. Kui lepinglasel või all-lepinglasel lubatakse ELi salastatud teavet säilitada pärast lepingu lõppemist, järgib kõnealune lepinglane või all-lepinglane jätkuvalt käesolevas otsuses sisalduvaid miinimumstandardeid ning kaitseb ELi salastatud teabe salajasust.

20. Tingimused, mille alusel lepinglane võib sõlmida all-lepinguid, on määratletud nii pakkumismenetluses kui ka lepingus.

21. Lepinglane taotleb nõukogu peasekretariaadilt kui lepingu sõlmijalt luba enne all-lepingu sõlmimist salastatud lepingu mis tahes osa täitmiseks. All-lepinguid ei tohi sõlmida tööstus- või muude üksustega, mis on registreeritud sellistes Euroopa Liitu mittekuuluvates riikides, mis ei ole sõlminud liiduga salastatud teabe kaitse lepingut.

22. Lepinglane vastutab selle eest, et oleks tagatud kõigi all-lepinguga seotud tegevuste teostamine kooskõlas käesolevas otsuses sätestatud miinimumnõuetega, ning ei anna ELi salastatud teavet all-lepinglasele ilma lepingu sõlmija eelneva kirjaliku nõusolekuta.

23. Lepinglase või all-lepinglase loodud või töödeldava ELi salastatud teabe suhtes teostab teabe koostaja õigusi lepingu sõlmija.

▼B

V. SALASTATUD LEPINGUTEGA SEOTUD KÜLASTUSED

24. Kui nõukogu peasekretariaadi, lepinglase või all-lepinglase töötajatel on salastatud lepingu täitmiseks vaja juurdepääsu CONFIDENTIEL UE/EU CONFIDENTIAL või SECRET UE/EU SECRET tasemel salastatud teabele üksteise ruumides, tuleb külastusi korraldada koostöös riiklike julgeolekuasutuste / määratud julgeolekuasutuste või muude pädevate julgeolekuasutusega. Riiklikud julgeolekuasutused / määratud julgeolekuasutused võivad siiski seoses konkreetsete projektidega kokku leppida korra, mille kohaselt selliseid külastusi võib korraldada otse.

25. Kõigil külastajatel peab olema juurdepääsuluba nõukogu peasekretariaadi lepinguga seotud ELi salastatud teabele ja teadmisvajadus sellise teabe suhtes.

26. Külastajatele võimaldatakse juurdepääs vaid külaskäigu eesmärgiga seotud ELi salastatud teabele.

VI. ELi SALASTATUD TEABE EDASTAMINE JA VEDU

27. ELi salastatud teabe elektroonilise edastamise suhtes kohaldatakse artikli 10 ja IV lisa asjakohaseid sätteid.

28. ELi salastatud teabe veo suhtes kohaldatakse III lisa asjakohaseid sätteid kooskõlas riigisiseste õigusaktidega.

29. Salastatud materjali vedamisel kaubana kohaldatakse julgeolekukorra kindlaksmääramisel järgmisi põhimõtteid:

a) julgeolek kindlustatakse lähtekohast lõppsihtkohta transportimise kõigil etappidel;

b) saadetisele kohaldatava kaitse tase määratakse selles sisalduva materjali kõrgeima salastatuse taseme põhjal;

c) veoteenuseid pakkuvatele äriühingutele tuleb hankida nõuetekohasel tasemel töötlemisluba. Sellisel juhul viiakse saadetist töötlevate töötajate suhtes läbi I lisa kohane julgeolekukontroll;

d) enne CONFIDENTIEL UE/EU CONFIDENTIAL või SECRET UE/EU SECRET tasemel salastatud materjali piiriülest vedu koostab saatja veoplaani ning selle kinnitab asjaomane riiklik julgeolekuasutus / määratud julgeolekuasutus või muu asjakohane pädev julgeolekuasutus;

e) veod toimuvad võimalikult täpselt punktist punkti ja need lõpetatakse nii kiiresti kui asjaolud seda võimaldavad ning

f) võimaluse korral peaks teekond kulgema üksnes läbi liikmesriikide. Teekond läbi Euroopa Liitu mittekuuluvate riikide tuleks ette võtta üksnes siis, kui selleks on andnud loa nii lähteriigi kui ka vastuvõtjariigi riiklik julgeolekuasutus / määratud julgeolekuasutus või muu pädev julgeolekuasutus.

VII. ELi SALASTATUD TEABE EDASTAMINE KOLMANDATES RIIKIDES PAIKNEVATELE LEPINGLASTELE

30. ELi salastatud teave edastatakse kolmandates riikides paiknevatele lepinglastele ja all-lepinglastele vastavalt turvameetmetele, mis on kokku lepitud nõukogu peasekretariaadi kui lepingu sõlmija ning selle asjaomase kolmanda riigi riikliku julgeolekuasutuse / määratud julgeolekuasutuse vahel, kus lepinglane on registreeritud.

▼B

VIII. RESTREINT UE/EU RESTRICTED TASEMEL SALASTATUD TEAVE

31. Nõukogu peasekretariaadil kui lepingu sõlmijal on vastavalt vajadusele kooskõlas liikmesriigi riikliku julgeolekuasutuse / määratud julgeolekuasutusega lepingu tingimuste alusel õigus korraldada kontrolle lepinglaste/all-lepinglaste valdustesse, et kontrollida, kas lepingus nõutud asjakohased turvameetmed RESTREINT UE/EU RESTRICTED tasemel ELi salastatud teabe kaitsmiseks on kasutusele võetud.

32. Nõukogu peasekretariaat teavitab lepingu sõlmijana riiklikke julgeolekuasutusi / määratud julgeolekuasutusi või muid pädevaid julgeolekuasutusi RESTREINT UE/EU RESTRICTED tasemel salastatud teavet sisaldavatest lepingutest niivõrd, kuivõrd seda nõutakse riigisiseste õigusaktide kohaselt.

33. Lepinglastelt või all-lepinglastelt ja nende töötajatelt ei nõuta töötlemis- või juurdepääsuluba nõukogu peasekretariaadi poolt sõlmitud lepingute puhul, mis sisaldavad RESTREINT UE/EU RESTRICTED tasemel salastatud teavet.

34. Lepingu sõlmijana vaatab nõukogu peasekretariaat läbi RESTREINT UE/EU RESTRICTED tasemel salastatud teabele juurdepääsu eeldavate lepingute pakkumiskutsetele laekunud vastused, ilma et see piiraks töötlemis- või juurdepääsulubade suhtes riigisiseste õigusaktide kohaselt kehtestatud võimalike nõuete kohaldamist.

35. Tingimused, mille alusel lepinglane võib all-lepinguid sõlmida, peavad olema kooskõlas punktiga 21.

36. Kui leping hõlmab RESTREINT UE/EU RESTRICTED tasemel salastatud teabe töötlemist lepinglase side- ja infosüsteemis, tagab nõukogu peasekretariaat lepingu sõlmijana, et lepingus või mis tahes all-lepingus täpsustatakse side- ja infosüsteemi akrediteerimiseks vajalikud tehnilised ja haldusnõuded, mis on vastavuses hinnatud riskiga ja milles on arvesse võetud kõik olulised tegurid. Sellise side- ja infosüsteemi akrediteerimise ulatus lepitakse kokku lepingu sõlmija ja asjaomase julgeolekuasutuse / määratud julgeolekuasutuse vahel.

▼B

VI LISA

SALASTATUD TEABE VAHETAMINE KOLMANDATE RIIKIDE JA RAHVUSVAHELISTE ORGANISATSIOONIDEGA

I. SISSEJUHATUS

1. Käesolev lisa sisaldab sätteid artikli 13 rakendamise kohta.

II. SALASTATUD TEABE VAHETAMIST REGULEERIVAD RAAMISTIKUD

2. Kui nõukogu otsustab, et on pikaajaline vajadus vahetada salastatud teavet:

— sõlmitakse salastatud teabe kaitse leping või

— sõlmitakse halduskokkulepe

vastavalt artikli 13 lõikele 2 ning III ja IV jaole ning julgeolekukomitee soovituse alusel.

3. Kui ÜJKP operatsiooni eesmärgil loodud ELi salastatud teavet tuleb esitada kõnealusel operatsioonil osalevatele kolmandatele riikidele või rahvusvahelistele organisatsioonidele ning kui ei ole kumbagi punktis 2 osutatud raamistikku, reguleeritakse ELi salastatud teabe vahetamist osaleva kolmanda riigi või rahvusvahelise organisatsiooniga V jao kohaselt vastavalt järgnevale:

— osalemise raamleping;

— ajutine osalemisleping või

— kui pole kumbagi eespool nimetatud lepingut, siis ajutine halduskokkulepe.

4. Punktides 2 ja 3 osutatud raamistiku puudumisel, ja kui on otsustatud edastada ELi salastatud teavet kolmandale riigile või rahvusvahelisele organisatsioonile erakorralistel ja ajutistel alustel VI jao kohaselt, palutakse asjaomasel kolmandal riigil või rahvusvahelisel organisatsioonil esitada kirjalik kinnitus, et nad kaitsevad neile edastatud ELi salastatud teavet käesolevas otsuses sätestatud aluspõhimõtete ja miinimumstandardite kohaselt.

III. SALASTATUD TEABE KAITSE LEPINGUD

5. Salastatud teabe kaitse lepingutega kehtestatakse ELi ja kolmanda riigi või rahvusvahelise organisatsiooni vahelist salastatud teabe vahetamist reguleerivad aluspõhimõtted ja miinimumstandardid.

6. Salastatud teabe kaitse lepingutega nähakse ette asjaomaste liidu institutsioonide ja organite pädevate julgeolekuasutuste ning asjaomase kolmanda riigi või rahvusvahelise organisatsiooni pädeva julgeolekuasutuse vaheline tehniline rakenduskord. Sellises rakenduskorras võetakse arvesse asjaomases kolmandas riigis või rahvusvahelises organisatsioonis kehtivate julgeolekueeskirjade, -struktuuride ja -menetlustega tagatud kaitsetaset. Rakenduskorra kiidab heaks julgeolekukomitee.

7. ELi salastatud teavet vahetatakse salastatud teabe kaitse lepingu alusel elektrooniliselt vaid juhul, kui see on lepinguga või vastava tehnilise rakenduskorraga sõnaselgelt ette nähtud.

8. Kui nõukogu sõlmib salastatud teabe kaitse lepingu, määratakse iga lepinguosalise juures kindlaks register, millest saab teabevahetuse jaoks peamine salastatud teabe vastuvõtmise ja väljastamise koht.

▼B

9. Selleks et hinnata julgeolekueeskirjade, -struktuuride ja -menetluste tõhusust asjaomases kolmandas riigis või rahvusvahelises organisatsioonis, korraldatakse vastastikusel kokkuleppel asjaomase kolmanda riigi või rahvusvahelise organisatsiooniga hindamiskülastusi. Sellised hindamiskülastused toimuvad vastavalt III lisa asjakohastele sätetele ja nende käigus hinnatakse järgmisi aspekte:

a) salastatud teabe kaitsmise suhtes kohaldatav õiguslik raamistik;

b) kolmanda riigi või rahvusvahelise organisatsiooni julgeolekupoliitika erijooned ja julgeolekukorralduse viis, mis võib mõjutada vahetamiseks lubatud teabe salastatuse taset;

c) tegelikult kohaldatavad turvameetmed ja -kord ning

d) edastatava ELi salastatud teabe tasemele vastavad julgeolekukontrolli menetlused.

10. Liidu nimel hindamiskülastust teostav töörühm hindab seda, kas asjaomase kolmanda riigi või rahvusvahelise organisatsiooni julgeolekualased õigusaktid ja menetlused on piisavad asjaomasel salastatuse tasemel ELi salastatud teabe kaitsmiseks.

11. Selliste külastuste tulemused esitatakse aruandes, mille alusel julgeolekukomitee määrab kindlaks, kui kõrgel tasemel ELi salastatud teavet võib asjaomase kolmanda poolega vahetada paberkandjal ja vajaduse korral elektrooniliselt, ning samuti mis tahes eritingimused, mis puudutavad teabevahetust kõnealuse poolega.

12. Enne kui julgeolekukomitee rakenduskorra heaks kiidab, püütakse igal juhul korraldada täielik julgeoleku hindamiskülastus asjaomasesse kolmandasse riiki või rahvusvahelisse organisatsiooni, et teha kindlaks seal kasutatava julgeolekusüsteemi laad ja tõhusus. Kui seda korraldada ei ole siiski võimalik, esitab nõukogu peasekretariaadi julgeolekubüroo julgeolekukomiteele talle kättesaadavale teabele tuginedes võimalikult põhjaliku aruande, milles teavitatakse julgeolekukomiteed kolmandas riigis või rahvusvahelises organisatsioonis kohaldatavatest julgeolekueeskirjadest ja julgeoleku korraldusest.

13. Enne ELi salastatud teabe tegelikku edastamist asjaomasele kolmandale riigile või rahvusvahelisele organisatsioonile edastatakse hindamiskülastuse aruanne või sellise aruande puudumisel punktis 12 osutatud aruanne julgeolekukomiteele, kes selle rahuldavaks tunnistab.

14. Liidu institutsioonide ja organite pädevad julgeolekuasutused teatavad kolmandale riigile või rahvusvahelisele organisatsioonile kuupäeva, millest alates on liidul võimalik lepingu alusel ELi salastatud teavet edastada, ning samuti ELi salastatud teabe kõrgeima salastatuse taseme, millesse kuuluvat teavet võib paberkandjal elektroonilisel teel vahetada.

15. Järelhindamiskülastusi korraldatakse vastavalt vajadusele, eelkõige juhul, kui:

a) tekib vajadus tõsta edastatava ELi salastatud teabe salastatuse taset;

b) liitu on teavitatud kolmanda riigi või rahvusvahelise organisatsiooni julgeolekukorra põhjalikust muutmisest, mis võib avaldada mõju sellele, kuidas ta kaitseb ELi salastatud teavet, või

c) on toimunud tõsine intsident, millega kaasnes ELi salastatud teabe loata avalikustamine.

▼B

16. Pärast salastatud teabe kaitse lepingu jõustumist ja salastatud teabe vahetamist asjaomase kolmanda riigi või rahvusvahelise organisatsiooniga võib julgeolekukomitee otsustada muuta kõrgeimat salastatuse taset, millesse kuuluvat teavet võib paberkandjal või elektrooniliselt vahetada, võttes eelkõige arvesse võimalike järelkülastuste tulemusi.

IV. HALDUSKOKKULEPPED

17. Kui esineb pikaajaline vajadus vahetada kolmanda riigi või rahvusvahelise organisatsiooniga teavet, mille salastatuse tase ei ületa üldjuhul taset RESTREINT UE/EU RESTRICTED ja kui julgeolekukomitee on teinud kindlaks, et kõnealuse poole julgeolekusüsteem ei ole salastatud teabe kaitse lepingu sõlmimiseks nõuetekohasel tasemel, võib peasekretär nõukogu heakskiidul sõlmida nõukogu peasekretariaadi nimel halduskokkuleppe kõnealuse kolmanda riigi või rahvusvahelise organisatsiooni asjaomase asutusega.

18. Kui kiireloomulistel operatiivpõhjustel on vaja kiiresti kehtestada salastatud teabe vahetamise raamistik, võib nõukogu erakorraliselt otsustada, et sõlmitavat halduskokkulepet kasutatakse kõrgemal tasemel salastatud teabe vahetamiseks.

19. Halduskokkulepped sõlmitakse üldjuhul kirjavahetuse vormis.

20. Enne ELi salastatud teabe tegelikku edastamist kõnealusele kolmandale riigile või rahvusvahelisele organisatsioonile korraldatakse punktis 9 kirjeldatud hindamiskülastus ning edastatakse külastuse aruanne või sellise aruande puudumisel punktis 12 osutatud aruanne julgeolekukomiteele, kes selle rahuldavaks tunnistab.

21. Halduskokkuleppe alusel ei vahetata ELi salastatud teavet elektrooniliselt, välja arvatud juhul, kui see on kokkuleppes sõnaselgelt ette nähtud.

V. SALASTATUD TEABE VAHETAMINE ÜJKP OPERATSIOONIDE RAAMES

22. Kolmandate riikide või rahvusvaheliste organisatsioonide osalemist ÜJKP operatsioonidel reguleerivad kriisiohjamisoperatsioonides osalemise raamlepingud. Sellised lepingud sisaldavad sätteid ÜJKP operatsioonide eesmärgil loodud ELi salastatud teabe edastamise kohta osalevatele kolmandatele riikidele või rahvusvahelistele organisatsioonidele. Kõrgeim salastatuse tase, millesse kuuluvat ELi salastatud teavet võib vahetada, on RESTREINT UE/EU RESTRICTED ÜJKP tsiviiloperatsioonide jaoks ja CONFIDENTIEL UE/EU CONFIDENTIAL ÜJKP sõjaliste operatsioonide jaoks, kui konkreetse ÜJKP operatsiooni loomist käsitlevas otsuses ei ole sätestatud teisiti.

23. Konkreetse ÜJKP operatsiooni jaoks sõlmitud ajutised osalemislepingud sisaldavad sätteid kõnealuse operatsiooni eesmärgil loodud ELi salastatud teabe edastamise kohta osalevale kolmandale riigile või rahvusvahelisele organisatsioonile. Kõrgeim salastatuse tase, millesse kuuluvat ELi salastatud teavet võib vahetada, on RESTREINT UE/EU RESTRICTED ÜJKP tsiviiloperatsioonide jaoks ja CONFIDENTIEL UE/EU CONFIDENTIAL ÜJKP sõjaliste operatsioonide jaoks, kui konkreetse ÜJKP operatsiooni loomist käsitlevas otsuses ei ole sätestatud teisiti.

▼B

24. Salastatud teabe kaitse lepingu puudumise korral ja kuni osalemislepingu sõlmimiseni edastatakse operatsiooni eesmärgil loodud ELi salastatud teavet operatsioonis osalevale kolmandale riigile või rahvusvahelisele organisatsioonile kõrge esindaja poolt sõlmitud halduskokkuleppe või VI jao kohaselt teabe edastamise ajutise otsuse alusel. ELi salastatud teavet võib sellise korra alusel vahetada üksnes kolmanda riigi või rahvusvahelise organisatsiooni operatsioonis osalemiseks kavandatud aja lõpuni. Kõrgeim salastatuse tase, millesse kuuluvat ELi salastatud teavet võib vahetada, on RESTREINT UE/EU RESTRICTED ÜJKP tsiviiloperatsioonide jaoks ja CONFIDENTIEL UE/EU CONFIDENTIAL ÜJKP sõjaliste operatsioonide jaoks, kui konkreetse ÜJKP operatsiooni loomist käsitlevas otsuses ei ole sätestatud teisiti.

25. Punktides 22–24 osutatud osalemise raamlepingutes, ajutistes osalemislepingutes ja ajutistes halduskokkulepetes sisalduvates salastatud teavet käsitlevates sätetes nähakse ette, et asjaomane kolmas riik või rahvusvaheline organisatsioon tagab selle, et tema poolt operatsioonile lähetatud isikkoosseisu liikmed kaitsevad ELi salastatud teavet vastavalt nõukogu julgeolekueeskirjadele ja täiendavatele juhenditele, mis väljastatakse pädevate asutuste poolt, sealhulgas operatsiooni käsuliinis.

26. Kui liidu ja osaleva kolmanda riigi või rahvusvahelise organisatsiooni vahel sõlmitakse hiljem salastatud teabe kaitse leping, asendab salastatud teabe kaitse leping ELi salastatud teabe vahetamise ja töötlemise puhul osalemise raamlepingus, ajutises osalemiselepingus või ajutises halduskokkuleppes sisalduvad salastatud teabe vahetamist käsitlevad sätted.

27. ELi salastatud teabe elektrooniline vahetamine kolmanda riigi või rahvusvahelise organisatsiooniga sõlmitud osalemise raamlepingu, ajutise osalemiselepingu või ajutise halduskokkuleppe alusel ei ole lubatud, välja arvatud juhul, kui see on asjaomases lepingus või kokkuleppes selgesõnaliselt ette nähtud.

28. ÜJKP operatsiooni eesmärgil loodud ELi salastatud teavet võib avalikustada kõnealusele operatsioonile lähetatud kolmandate riikide või rahvusvaheliste organisatsioonide personalile vastavalt punktidele 22–27. Kui kõnealusele personalile antakse juurdepääs ELi salastatud teabele ÜJKP operatsiooni tööruumides või side- ja infosüsteemis, tuleb kohaldada meetmeid (sealhulgas avalikustatud ELi salastatud teabe registreerimine), et vähendada teabekao või teabe ohtu sattumise riski. Sellised meetmed määratakse kindlaks asjaomastes planeerimis- ja missioonidokumentides.

29. Salastatud teabe kaitse lepingu puudumisel võib ELi salastatud teabe edastamine ÜJKP operatsiooni toimumiskoha riigile konkreetse ja vahetu operatiivvajaduse korral toimuda kõrge esindaja sõlmitud halduskokkuleppe alusel. Selline võimalus nähakse ette ÜJKP operatsiooni käsitlevas otsuses. Sellistel asjaoludel edastatud ELi salastatud teave on piiratud ÜJKP operatsiooni eesmärkidel koostatud teabega ja selle salastatuse tase ei ole kõrgem kui RESTREINT UE/EU RESTRICTED, välja arvatud juhul, kui ÜJKP operatsiooni loomist käsitlevas otsuses ei ole ette nähtud kõrgemat salastatuse taset. Sellise halduskokkuleppe kohaselt peab operatsiooni toimumiskoha riik kohustuma kaitsma ELi salastatud teavet miinimumstandardite kohaselt, mis on vähemalt sama ranged kui käesolevas otsuses sätestatud miinimumstandardid.

▼B

30. Salastatud teabe kaitse lepingu puudumise korral võib ELi salastatud teavet edastada kolmandatele riikidele ja rahvusvahelistele organisatsioonidele, kes ÜJKP operatsioonis ei osale, kõrge esindaja sõlmitud halduskokkuleppe alusel. Vajaduse korral nähakse selline võimalus ja sellega seonduvad tingimused ette ÜVJP operatsiooni loomist käsitlevas otsuses. Sellistel asjaoludel edastatud ELi salastatud teave on piiratud ÜJKP operatsiooni eesmärkidel koostatud teabega ja selle salastatuse tase ei ole kõrgem kui RESTREINT UE/EU RESTRICTED, välja arvatud juhul, kui ÜJKP operatsiooni loomist käsitlevas otsuses ei ole ette nähtud kõrgemat salastatuse taset. Kõnealuse halduskokkuleppe kohaselt peab asjaomane kolmas riik või rahvusvaheline organisatsioon kohustuma kaitsma ELi salastatud teavet miinimumstandardite kohaselt, mis on vähemalt sama ranged kui käesolevas otsuses sätestatud miinimumstandardid.

31. Enne punktide 22, 23 ja 24 kohast ELi salastatud teabe edastamist käsitlevate sätete rakendamist ei ole vaja sätestada rakenduskorda või teha hindamiskülastusi.

VI. ELi SALASTATUD TEABE ERAKORRALINE AJUTINE EDASTAMINE

32. Kui puudub III–V jao kohane raamistik ja kui nõukogu või mõni nõukogu ettevalmistavatest organitest määrab kindlaks, et esineb erakorraline vajadus edastada ELi salastatud teavet kolmandale riigile või rahvusvahelisele organisatsioonile, toimib nõukogu peasekretariaat järgmiselt:

a) kontrollib niivõrd, kui see on võimalik, kolmanda riigi või rahvusvahelise organisatsiooni julgeolekuasutuselt, kas selle julgeolekueeskirjad, -struktuurid ja menetlused tagavad talle edastatava ELi salastatud teabe kaitse vastavalt standarditele, mis on vähemalt sama ranged kui käesolevas otsuses sätestatud standardid, ning

b) palub julgeolekukomiteel väljastada olemasoleva teabe põhjal soovituse selle kolmanda riigi või rahvusvahelise organisatsiooni julgeolekueeskirjade, -struktuuride ja -menetluste usaldusväärsuse kohta, kellele ELi salastatud teavet kavatsetakse edastada.

33. Kui julgeolekukomitee esitab ELi salastatud teabe edastamist toetava soovituse, edastatakse küsimus arutamiseks alaliste esindajate komiteele (Coreper), kes langetab otsuse teabe edastamise kohta.

34. Kui julgeolekukomitee soovituses ei toetata ELi salastatud teabe edastamist:

a) arutab ÜVJP/ÜJKP valdkonnaga seotud küsimusi poliitika- ja julgeolekukomitee, kes sõnastab soovituse, mille alusel Coreper teeb otsuse;

b) kõigi muude valdkondade puhul arutab küsimust ja teeb otsuse Coreper.

35. Vajaduse korral, ja kui selleks on teabe koostaja eelnev kirjalik nõusolek, võib Coreper otsustada, et salastatud teavet võib edastada vaid osaliselt või juhul, kui selle salastatuse taset eelnevalt alandatakse või salastatus kustutatakse, või et edastatav teave koostatakse viiteta allikale või algsele ELi salastatuse tasemele.

36. ELi salastatud teabe edastamise otsuse järel edastab nõukogu peasekretariaat asjaomase dokumendi, mis varustatakse avaldatavuse märkega kolmanda riigi või rahvusvahelise organisatsiooni kohta, kellele see on edastatud. Enne teabe tegelikku edastamist võtab asjaomane kolmas pool endale kirjalikult kohustuse kaitsta saadavat ELi salastatud teavet vastavalt käesolevas otsuses sätestatud aluspõhimõtetele ja miinimumstandarditele.

▼B

VII. VOLITUSE ANDMINE ELi SALASTATUD TEABE EDASTAMISEKS KOLMANDATELE RIIKIDELE VÕI RAHVUSVAHELISTELE ORGANISATSIOONIDELE

37. Kui salastatud teabe vahetamiseks kolmanda riigi või rahvusvahelise organisatsiooniga on olemas punkti 2 kohane raamistik, võtab nõukogu vastu otsuse anda peasekretärile volitused edastada asjaomasele kolmandale riigile või rahvusvahelisele organisatsioonile ELi salastatud teavet, järgides koostaja nõusoleku põhimõtet. Peasekretär võib delegeerida sellised volitused nõukogu peasekretariaadi kõrgematele ametnikele.

38. Kui punkti 2 esimese taande kohane salastatud teabe kaitse leping on olemas, võib nõukogu teha otsuse anda kõrgele esindajale volitused nõukogust pärit ühise välis- ja julgeolekupoliitika alase ELi salastatud teabe edastamiseks asjaomasele kolmandale riigile või rahvusvahelisele organisatsioonile, kui selles teabes sisalduva mis tahes allikmaterjali koostaja on andnud selleks oma nõusoleku. Kõrge esindaja võib delegeerida sellised volitused Euroopa välisteenistuse kõrgetele ametnikele või ELi eriesindajatele.

39. Kui salastatud teabe vahetamiseks kolmanda riigi või rahvusvahelise organisatsiooniga on olemas punkti 2 või 3 kohane raamistik, antakse kõrgele esindajale volitused edastada ELi salastatud teavet vastavalt ÜJKP operatsiooni loomist käsitlevale otsusele ja järgides koostaja nõusoleku põhimõtet. Kõrge esindaja võib delegeerida sellised volitused Euroopa välisteenistuse kõrgetele ametnikele, ELi operatsioonide, relvajõudude või missioonide ülematele või ELi missioonide juhtidele.

▼B

Liited

A liide

Mõisted

B liide

Salastatuse tasemete vastavus

C liide

Riiklike julgeolekuasutuste loetelu

D liide

Lühendite loetelu

▼B

A liide

MÕISTED

Käesolevas otsuses kasutatakse järgmisi mõisteid:

„akrediteerimine” – menetlus, mille tulemusena väljastatakse ametlik turvalisuse akrediteerimise asutuse avaldus selle kohta, et süsteem on saanud heakskiidu töötamiseks kindlaksmääratud salastatuse tasemel, käitamiskeskkonna konkreetses turvarežiimis ja vastuvõetaval riskitasemel, tuginedes eeldusele, et on rakendatud heakskiidetud tehnilisi, füüsilisi, korralduslikke ja menetluslikke turvameetmeid;

„varad” – kõik, mis on organisatsiooni, selle töötoimingute ja nende jätkumise jaoks väärtuslik, sealhulgas organisatsiooni missiooni toetavad teaberessursid;

„luba juurdepääsuks ELi salastatud teabele” – nõukogu peasekretariaadi ametisse nimetava asutuse otsus, mis on tehtud liikmesriigi pädeva asutuse kinnituse põhjal, et nõukogu peasekretariaadi ametnikule, muule teenistujale või riiklikule lähetatud eksperdile võib eeldusel, et tema teadmisvajadus on kindlaks määratud ja talle on nõuetekohaselt selgitatud tema kohustusi, lubada kindlaksmääratud kuupäevani juurdepääsu kindla salastatuse tasemega (CONFIDENTIEL UE/EU CONFIDENTIAL või kõrgem) ELi salastatud teabele;

„side- ja infosüsteemi kasutusaeg” – kogu side- ja infosüsteemi eksisteerimise kestus, mis hõlmab algatamist, kontseptsiooni loomist, kavandamist, vajaduste analüüsi, projekteerimist, arendamist, katsetamist, rakendamist, käitamist, hooldust ning tegevuse lõpetamist;

„salastatud leping” – leping, mille nõukogu peasekretariaat on sõlminud lepinglasega kaupade tarnimise, tööde teostamise või teenuste osutamise eesmärgil, mille täitmise eelduseks on või mille täitmisega kaasneb juurdepääs ELi salastatud teabele või sellise teabe loomine;

„salastatud all-leping” – leping, mille nõukogu peasekretariaadi lepinglane on sõlminud teise lepinglasega (st all-lepinglasega) kaupade tarnimise, tööde teostamise või teenuste osutamise eesmärgil, mille täitmise eelduseks on või mille täitmisega kaasneb juurdepääs ELi salastatud teabele või sellise teabe loomine;

„side- ja infosüsteem” – vt artikli 10 lõiget 2;

„lepinglane” – üksikisik või juriidiline isik, kellel on lepinguliste kohustuste võtmiseks õigus- ja teovõime;

„krüptomaterjal” – krüptoalgorütmid, krüptoriistvara- ja tarkvaramoodulid ning -tooted, sealhulgas rakendamise üksikasjad ja seotud dokumentatsioon ning kodeerimisandmed;

„krüptovahend” – vahend, mille esmane ja peamine funktsioon on turvateenuste (konfidentsiaalsus, andmeterviklus, kättesaadavus, autentsus, salgamise väärамine) pakkumine ühe või enama krüpteerimismehhanismi kaudu;

▼B

„ÜJKP operatsioon” – ELi lepingu V jaotise 2. peatüki kohane kriisiohjamise sõjaline või tsiviiloperatsioon;

„salastatuse kustutamine” – salastatuse tühistamine;

„süvakaitse” – erinevate mitme kaitseliinina võetavate turvameetmete kohaldamine;

„määratud julgeolekuasutus” – asutus, mis vastutab liikmesriigi julgeolekuasutuse ees tööstus- või muudele üksustele riigi kõigi tööstusjulgeolekuga seotud poliitikaküsimuste edastamise eest ning kõnealuse poliitika suunamise ja selle rakendamisel abi andmise eest. Määratud julgeolekuasutuse ülesandeid võib täita riiklik julgeolekuasutus või muu pädev asutus;

„dokument” – talletud teave selle füüsilisest kujust ja omadustest olenemata;

„taseme alandamine” – salastatuse taseme alandamine;

„ELi salastatud teave” – vt artikli 2 lõiget 1;

„töötlemisluba” – riikliku julgeolekuasutuse või määratud julgeolekuasutuse haldusotsus selle kohta, et lähtudes julgeoleku seisukohast, võib ettevõte pakkuda piisaval tasemel kaitset teataval salastatuse tasemel ELi salastatud teabele;

„töötlemine” – kõik võimalikud toimingud, mida ELi salastatud teabega võidakse teha selle kasutusaja jooksul. See hõlmab teabe koostamist, töötlemist, vedu, salastatuse taseme alandamist ja salastatuse kustutamist ning teabe hävitamist. Side- ja infosüsteemi puhul hõlmab see ka teabe kogumist, kuvamist, edastamist ja säilitamist;

„valdaja” – kontrollitud teadmisvajadusega nõuetekohaselt volitatud isik, kelle valduses on ELi salastatud teave ja kes seetõttu vastutab selle kaitsmise eest;

„tööstus- või muu üksus” – üksus, mis on kaasatud kaupade tarnimisse, tööde teostamisse või teenuste osutamisse; selleks võib olla tööstus-, kaubandus-, teenindus-, teadus-, uurimis-, haridus- või arendusüksus või füüsilisest isikust ettevõtja;

„tööstusjulgeolek” – vt artikli 11 lõiget 1;

„infokindlus” – vt artikli 10 lõiget 1;

„omavaheline ühendus” – vt IV lisa punkti 32;

„salastatud teabe haldamine” – vt artikli 9 lõiget 1;

▼B

„materjal” – dokument, andmekandja või valmistatud või valmistamisel olev masin või seade;

„teabe koostaja” – liidu institutsioon, organ või asutus, liikmesriik, kolmas riik või rahvusvaheline organisatsioon, kelle volitusel on salastatud teave loodud ja/või liidu struktuuridesse sisestatud;

„töötajatega seotud julgeolek” – vt artikli 7 lõiget 1;

„juurdepääsuluba” – liikmesriigi pädeva asutuse avaldus, mis tehakse pärast julgeolekukontrolli lõpuleviimist liikmesriigi pädevate asutuste poolt ja mis kinnitab, et isikule võib lubada kindlaksmääratud kuupäevani juurdepääsu teatud salastatuse tasemel ELi salastatud teabele (salastatuse tase CONFIDENTIEL UE/EU CONFIDENTIAL või kõrgem);

„juurdepääsutõend” – pädeva asutuse väljastatud tõend, mis kinnitab, et isik on läbinud julgeolekukontrolli ja tal on kehtiv juurdepääsutõend või ametisse nimetava asutuse luba juurdepääsuks ELi salastatud teabele, millel on kirjas, millisel salastatuse tasemel ELi salastatud teabele võib asjaomasele isikule juurdepääsu lubada (CONFIDENTIEL UE/EU CONFIDENTIAL või kõrgem), vastava juurdepääsuloa kehtivuse lõppemise kuupäev ja tõendi enda kehtivuse lõppemise kuupäev;

„füüsiline julgeolek” – vt artikli 8 lõiget 1;

„programmi/projekti julgeolekujuhised” („julgeolekujuhised”) – loetelu julgeolekumenetlustest, mida kohaldatakse konkreetse programmi/projekti suhtes julgeolekumenetluste standardimiseks. Seda võib programmi/projekti kestel muuta;

„registreerimine” – vt III lisa punkti 18;

„jääkrisk” – risk, mis jääb püsima pärast turvameetmete rakendamist, eeldusel et kõik ohud ei ole tõrjutud ning kõiki haavatavusi ei saa kõrvaldada;

„risk” – võimalus, et antud oht kasutab ära organisatsiooni või selle poolt kasutatava süsteemi sisemisi või väliseid haavatavusi ja kahjustab seeläbi organisatsiooni ja selle materiaalset ja mittemateriaalset vara. Riski mõõdetakse olemasolevate ohtude tõenäosuse ja nende mõju kombinatsioonina;

— „riski aktsepteerimine” – otsus leppida jääkriski edasise olemasoluga pärast riski käsitlemist;

— „riski hindamine” – ohtude ja haavatavuse kindlakstegemine ning sellega seotud riskianalüüsi, st riski tõenäosuse ja mõju analüüsi teostamine;

— „riskiteavitus” – side- ja infosüsteemide kasutajaskonna riskiteadlikkuse suurendamine, heakskiitvate asutuste teavitamine sellistest riskidest ja riskide alane aruandlus töötlejatele;

▼B

— „riski käsitlemine” – riski leevendamine, kõrvaldamine, vähendamine (tehniliste, füüsiliste, korralduslike või menetluslike meetmete asjakohase kombineerimise abil), riski ülekandmine või seire;

„julgeolekuaspekte käsitlev dokument” – lepingu sõlmija poolt esitatud konkreetsete lepinguliste tingimuste kogum, mis moodustab sellise salastatud lepingu lahutamatu osa, millega kaasneb juurdepääs ELi salastatud teabele või millega kaasneb sellise teabe loomine, ning millega määratakse kindlaks lepingu julgeolekunõuded või need lepingu osad, millele on tarvis tagada julgeolekukaitse;

„salastatuse taseme määramise juhend” – dokument, milles kirjeldatakse programmi või lepingu salastatud osi, määrates kindlaks neile kohaldatavad salastatuse tasemed. Salastatuse taseme määramise juhendit võib kogu programmi või lepingu kehtivusaja jooksul täiendada ja nende teabeelementide salastatuse taset võib muuta või alandada; kui salastatuse taseme määramise juhend on olemas, on see julgeolekuaspekte käsitleva dokumendi osa;

„julgeolekukontroll” – kontroll, mille viib läbi liikmesriigi pädev asutus kõnealuses liikmesriigis kehtivate õigusnormide kohaselt, et saada kinnitust selle kohta, et ei ole teada midagi kahtlust äratavat, mis takistaks andmast isikule juurdepääsuluba või luba juurdepääsuks teatud tasemel (CONFIDENTIEL UE/EU CONFIDENTIAL või kõrgem) ELi salastatud teabele;

„turvarežiim” – side- ja infosüsteemi toimimise aluseks olevate tingimuste määratlemine, mis põhineb töödeldava teabe salastatuse tasemel ja selle kasutajate juurdepääsutasemetel, ametlikul juurdepääsu heakskiidul ja teadmisvajadustel. Salastatud teabe töötlemiseks või edastamiseks on neli režiimi: ühtlase ülaturbe režiim, diferentsiaalse ülaturbe režiim, lahterdatud kasutajarežiim ja mitmetasemelise turbe režiim;

— „ühtlase ülaturbe režiim” – süsteemi turvarežiim, mille puhul kõik isikud, kellel on side- ja infosüsteemile juurdepääs, peavad läbima side- ja infosüsteemis töödeldava teabe kõrgeimale salastatuse tasemele vastava julgeolekukontrolli ja neil on ühine teadmisvajadus kogu side- ja infosüsteemis töödeldava teabe järele;

— „diferentsiaalse ülaturbe režiim” – süsteemi turvarežiim, mille puhul kõik isikud, kellel on juurdepääs side- ja infosüsteemile, peavad läbima süsteemis töödeldava teabe kõrgeimale salastatuse tasemele vastava julgeolekukontrolli, kuid kõigil isikutel, kellel on juurdepääs side- ja infosüsteemile, ei ole ühist teadmisvajadust kogu side- ja infosüsteemis töödeldava teabe järele; teabele juurdepääsu heakskiidu võib anda isik;

— „lahterdatud kasutajarežiim” – süsteemi turvarežiim, mille puhul kõik isikud, kellel on juurdepääs side- ja infosüsteemile, peavad läbima süsteemis töödeldava teabe kõrgeimale salastatuse tasemele vastava julgeolekukontrolli, kuid kõigil isikutel, kellel on juurdepääs side- ja infosüsteemile, ei ole ametlikku luba juurdepääsuks kogu side- ja infosüsteemis töödeldavale teabele; ametlik luba nõuab juurdepääsu kontrolli ametlikku keskset haldamist erinevalt ühe isiku äranägemisest juurdepääsu andmisel;

▼B

— „mitmetasemelise turbe režiim” – süsteemi turvarežiim, mille puhul kõik isikud, kellel on juurdepääs side- ja infosüsteemile, ei pea läbima süsteemis töödeldava teabe kõrgeimale salastatuse tasemele vastavat julgeolekukontrolli ning kõigil isikutel ei ole ühist teadmisvajadust kogu side- ja infosüsteemis töödeldava teabe järele;

„turvariski juhtimise protsess” – organisatsiooni või selle poolt kasutatava süsteemi julgeolekut mõjutada võivate ebakindlate sündmuste kindlaksmääramise, kontrollimise ja minimeerimise kogu protsess. See hõlmab kõiki riskidega seotud tegevusi, sealhulgas hindamist, käsitlemist, aktsepteerimist ja teavitust;

„TEMPEST” – paljastavate elektromagnetkiirguste uurimine ja kontrollimine ning nende tõkestamise meetmed;

„oht” – soovimatu intsidendi võimalik põhjus, mis võib kahjustada organisatsiooni või selle poolt kasutatavat süsteemi; selline oht võib olla juhuslik või tahtlik (kuritahtlik) ning seda iseloomustavad ohtlikud elemendid, võimalikud sihtmärgid ja ründemeetodid;

„haavatavus” – mis tahes laadi puudus, mida üks või mitu ohtu võivad ära kasutada. Haavatavus võib tähendada tegematajätmist või olla seotud kontrolli nõrkusega tulenevalt selle ranguse, täielikkuse või järjepidevuse puudumisest ning see võib olla tehnilist, menetluslikku, füüsilist, korralduslikku või operatsioonilist laadi.

▼M1

B liide

SALASTATUSE TASEMETE VASTAVUS

EU	TRÈS SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Belgia	Très Secret (Loi 11.12.1998) Zeer Geheim (Wet 11.12.1998)	Secret (Loi 11.12.1998) Geheim (Wet 11.12.1998)	Confidentiel (Loi 11.12.1998) Vertrouwelijk (Wet 11.12.1998)	vt allpool märkus ([1])
Bulgaaria	Строго секретно	Секретно	Поверително	За служебно ползване
Tšehhi Vabariik	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Taani	YDERST HEMMELIGT	HEMMELIGT	FORTROLIGT	TIL TJENESTEBRUG
Saksamaa	STRENG GEHEIM	GEHEIM	VS (([2]))- VERTRAULICH	VS — NUR FÜR DEN DIENSTGEBRAUCH
Eesti	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Iirimaa	Top Secret	Secret	Confidential	Restricted
Kreeka	Άκρως Απόρρητο Abr: ΑΑΠ	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Hispaania	SECRETO	RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
Prantsusmaa	Très Secret Défense	Secret Défense	Confidentiel Défense	vt allpool märkus (([3]))
Horvaatia	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Itaalia	Segretissimo	Segreto	Riservatissimo	Riservato
Küpros	Άκρως Απόρρητο Abr: (ΑΑΠ)	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Läti	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Leedu	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo

([1]) Belgias ei ole salastatuse taset „Diffusion Restreinte/Beperkte Verspreiding”. Belgia töötleb ja kaitseb „RESTREINT UE/EU RESTRICTED” tasemel salastatud teavet viisil, mis ei ole leebem Euroopa Liidu Nõukogu julgeolekueeskirjades kirjeldatud standarditest ja menetlustest.

([2]) Saksamaa: VS = Verschlusssache.

([3]) Prantsusmaa ei kasuta oma siseriiklikus süsteemis salastatuse taset „RESTREINT”. Prantsusmaa töötleb ja kaitseb „RESTREINT UE/EU RESTRICTED” tasemel salastatud teavet viisil, mis ei ole leebem Euroopa Liidu Nõukogu julgeolekueeskirjades kirjeldatud standarditest ja menetlustest.

▼M1

Luksemburg | Très Secret Lux | Secret Lux | Confidentiel Lux | Restreint Lux |

Ungari | Szigorúan titkos! | Titkos! | Bizalmas! | Korlátozott terjesztésű! |

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

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

Madalmaad | Stg. ZEER GEHEIM | Stg. GEHEIM | Stg. CONFIDENTIEEL | Dep. VERTROUWELIJK |

Austria | Streng Geheim | Geheim | Vertraulich | Eingeschränkt |

Poola | Ściśle tajne | Tajne | Poufne | Zastrzeżone |

Portugal | Muito Secreto | Secreto | Confidencial | Reservado |

Rumeenia | Strict secret de importanță deosebită | Strict secret | Secret | Secret de serviciu |

Sloveenia | STROGO TAJNO | TAJNO | ZAUPNO | INTERNO

Slovakkia | Prísne tajné | Tajné | Dôverné | Vyhradené |

Soome | ERITTÄIN SALAINEN YTTERST HEMLIG | SALAINEN HEMLIG | LUOTTAMUKSELLINEN KONFIDENTIELL | KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG |

Rootsi ([2]) | HEMLIG/TOP SECRET HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET | HEMLIG/SECRET HEMLIG | HEMLIG/CONFIDENTIAL HEMLIG | HEMLIG/RESTRICTED HEMLIG |

Ühendkuningriik | UK TOP SECRET | UK SECRET | vt allpool märkus ([3]) | UK OFFICIAL-SENSITIVE

([1]) Malta puhul võib kasutada nii malta- kui ingliskeelset märgistust.

([2]) Rootsi: ülemises reas esitatud märget kasutavad sõjaväeasutused ja alumises reas esitatud märget kasutavad muud asutused.

([3]) Ühendkuningriik ei kasuta oma siseriiklikus süsteemis enam salastatuse taset „UK CONFIDENTIAL”. Ühendkuningriik töötleb ja kaitseb „CONFIDENTIEL UE/EU CONFIDENTIAL” tasemel salastatud teavet vastavalt salastatuse taseme „UK SECRET” suhtes kohaldatavatele julgeolekualase kaitse nõuetele.

▼B

C liide

RIIKLIKE JULGEOLEKUASUTUSTE LOETELU

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

Sekretariaadi tel: +32 25014542
Faks: +32 25014596
E-post: nvo-ans@diplobel.fed.be

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

Tel: +372 7170019, +372 7170117
Faks: +372 7170213
E-post: nsa@mod.gov.ee

BULGAARIA
State Commission on Information Security
90 Cherkovna Str.
1505 Sofia

Tel: +359 29333600
Faks: +359 29873750
E-post: dksi@government.bg
Veebisait: www.dksi.bg

IIRIMAA
National Security Authority
Department of Foreign Affairs
76 - 78 Harcourt Street
Dublin 2

Tel: +353 14780822
Faks: +353 14082959

TŠEHHI VABARIIK
Národní bezpečnostní úřad
(National Security Authority)
Na Popelce 2/16
150 06 Praha 56

Tel: +420 257283335
Faks: +420 257283110
E-post: czech.nsa@nbu.cz
Veebisait: www.nbu.cz

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

Τηλ.: +30 2106572045 (ώρες γραφείου)
+30 2106572009 (ώρες γραφείου)
Φαξ: +30 2106536279
+30 2106577612

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

Tel: +30 2106572045
+30 2106572009
Faks: +30 2106536279
+30 2106577612

TAANI
Politiets Efterretningstjeneste
(Danish Security Intelligence Service)
Klausdalsbrovej 1
2860 Søborg

Tel: +45 33148888
Faks: +45 33430190

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

Tel: +45 33325566
Faks: +45 33931320

HISPAANIA
Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
28023 Madrid

Tel: +34 913725000
Faks: +34 913725808
E-post: nsa-sp@areatec.com

▼B

GERMANY Bundesministerium des Innern Referat ÖS III 3 Alt-Moabit 101 D D-11014 Berlin Tel: +49 30186810 Faks: +49 30186811441 E-post: oesIII3@bmi.bund.de	**PRANTSUSMAA** Secrétariat général de la défense et de la sécurité nationale Sous-direction Protection du secret (SGDSN/PSD) 51 Boulevard de la Tour-Maubourg 75700 Paris 07 SP Tel: +33 171758177 Faks: +33 171758200
HORVAATIA Ured Vijeća za nacionalnu sigurnost Croatian NSA Jurjevska 34 10000 Zagreb Croatia Tel: +385 14681222 Faks: +385 14686049 www.uvns.hr	**LUKSEMBURG** Autorité nationale de Sécurité Boîte postale 2379 1023 Luxembourg Tel: +352 24782210 üldtelefon +352 24782253 otseliin Faks: +352 24782243
ITAALIA Presidenza del Consiglio dei Ministri D.I.S. - U.C.Se. Via di Santa Susanna, 15 00187 Roma Tel: +39 0661174266 Faks: +39 064885273	**UNGARI** Nemzeti Biztonsági Felügyelet (National Security Authority of Hungary) H-1024 Budapest, Szilágyi Erzsébet fasor 11/B Tel: +36 (1) 7952303 Faks: +36 (1) 7950344 Postiaadress: H-1357 Budapest, PO Box 2 E-post: nbf@nbf.hu Veebisait: www.nbf.hu
KÜPROS ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ Εθνική Αρχή Ασφάλειας (ΕΑΑ) Υπουργείο Άμυνας Λεωφόρος Εμμανουήλ Ροΐδη 4 1432 Λευκωσία, Κύπρος Τηλέφωνα: +357 22807569, +357 22807643, +357 22807764 Τηλεομοιότυπο: +357 22302351 Ministry of Defence Minister's Military Staff National Security Authority (NSA) 4 Emanuel Roidi street 1432 Nicosia Tel: +357 22807569, +357 22807643, +357 22807764 Faks: +357 22302351 E-post: cynsa@mod.gov.cy	**MALTA** Ministry for Home Affairs and National Security P.O. Box 146 MT-Valletta Tel: +356 21249844 Faks: +356 25695321
LÄTI National Security Authority Constitution Protection Bureau of the Republic of Latvia P.O.Box 286 LV-1001 Riga Tel: +371 67025418 Faks: +371 67025454 E-post: ndi@sab.gov.lv	**MADALMAAD** Ministerie van Binnenlandse Zaken en Koninkrijksrelaties Postbus 20010 2500 EA Den Haag Tel: +31 703204400 Faks: +31 703200733 Ministerie van Defensie Beveiligingsautoriteit Postbus 20701 2500 ES Den Haag Tel: +31 703187060 Faks: +31 703187522

▼B

LEEDU Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija (The Commission for Secrets Protection Coordination of the Republic of Lithuania National Security Authority) Gedimino 40/1 LT-01110 Vilnius Tel: +370 70666701, +370 70666702 Faks: +370 70666700 E-post: nsa@vsd.lt	**AUSTRIA** Informationssicherheitskommission Bundeskanzleramt Ballhausplatz 2 1014 Wien Tel: +43 1531152594 Faks: +43 1531152615 E-post: ISK@bka.gv.at
POOLA Agencja Bezpieczeństwa Wewnętrznego – ABW (Internal Security Agency) 2 A Rakowiecka St. 00–993 Warszawa Tel: +48 225857360 Faks: +48 225858509 E-post: nsa@abw.gov.pl Veebisait: www.abw.gov.pl	**SLOVAKKIA** Národný bezpečnostný úrad (National Security Authority) Budatínska 30 P.O. Box 16 850 07 Bratislava Tel: +421 268692314 Faks: +421 263824005 Veebisait: www.nbusr.sk
PORTUGAL Presidência do Conselho de Ministros Autoridade Nacional de Segurança Rua da Junqueira, 69 1300-342 Lisboa Tel: +351 213031710 Faks: +351 213031711	**SOOME** National Security Authority Ministry for Foreign Affairs P.O. Box 453 FI-00023 Government Tel: +358 16055890 Faks: +358 916055140 E-post: NSA@formin.fi
RUMEENIA Oficiul Registrului Național al Informațiilor Secrete de Stat (Romanian NSA – ORNISS National Registry Office for Classified Information) Str. Mureş nr. 4, sector 1 012275 Bucureşti Tel: +40 212245830 Faks: +40 212240714 E-post: nsa.romania@nsa.ro Veebisait: www.orniss.ro	**ROOTSI** Utrikesdepartementet (Ministry for Foreign Affairs) UD-RS S 103 39 Stockholm Tel: +46 84051000 Faks: +46 87231176 E-post: ud-nsa@foreign.ministry.se
SLOVEENIA Urad Vlade RS za varovanje tajnih podatkov Gregorčičeva 27 1000 Ljubljana Tel: +386 14781390 Faks: +386 14781399 E-post: gp.uvtp@gov.si	**ÜHENDKUNINGRIIK** UK National Security Authority Room 335, 3rd Floor 70 Whitehall London SW1 A 2AS Tel 1: +44 2072765645 Tel 2: +44 2072765497 Faks: +44 2072765651 E-post: UK-NSA@cabinet-office.x.gsi.gov.uk

▼B

D liide

LÜHENDITE LOETELU

Akronüüm	Tähendus
Coreper	Alaliste esindajate komitee
ÜJKP	Ühine julgeoleku- ja kaitsepoliitika
ÜVJP	Ühine välis- ja julgeolekupoliitika