KOMISJONI OTSUS (EL, Euratom) 2015/444,

13. märts 2015,

ELi salastatud teabe kaitseks vajalike julgeolekunormide kohta

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut, eriti selle artiklit 249,

võttes arvesse Euroopa Aatomienergiaühenduse asutamislepingut, eriti selle artiklit 106,

võttes arvesse aluslepingutele lisatud Euroopa Liidu privileegide ja immuniteetide protokolli nr 7, eriti selle artiklit 18,

ning arvestades järgmist:

(1) Komisjoni julgeolekusätted ELi salastatud teabe kaitsmise kohta vajavad läbivaatamist ja ajakohastamist, võttes arvesse institutsionaalseid, organisatsioonilisi, operatiivseid ja tehnoloogilisi muutusi.

(2) Euroopa Komisjon on sõlminud oma peamiste tegevuskohtade julgeolekut käsitlevad kokkulepped Belgia, Luksemburgi ja Itaalia valitsustega ([1]).

(3) Komisjon, nõukogu ja Euroopa välisteenistus kohustuvad kohaldama ELi salastatud teabe kaitse suhtes samaväärse tasemega julgeolekustandardeid.

(4) Vajaduse korral tuleb ka Euroopa Parlament ja muud liidu institutsioonid, asutused või organid kaasata liidu ja tema liikmesriikide huvide kaitsmiseks vajalike salastatud teabe kaitsmise põhimõtete, standardite ja eeskirjade kohaldamisse.

(5) 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 neid meetmeid kooskõlas süvakaitse põhimõttega. Selliste meetmete tõhusust hinnatakse pidevalt.

(6) Komisjonis tähendab salastatud teabe kaitseks arendatav füüsiline julgeolek füüsiliste ja tehniliste kaitsemeetmete kohaldamist, et vältida volitamata juurdepääsu ELi salastatud teabele.

(7) ELi salastatud teabe haldamine tähendab haldusmeetmete kohaldamist ELi salastatud teabe kontrollimiseks kogu selle kehtivusaja jooksul, et täiendada käesoleva otsuse 2., 3. ja 5. peatükis sätestatud meetmeid ja aidata seeläbi ära hoida, avastada ja korvata sellise teabe tahtlikku või juhuslikku ohtusattumist või kadumist. Sellised meetmed on eelkõige seotud ELi salastatud teabe loomise, säilitamise, registreerimise, kopeerimise, tõlkimise, salastatuse taseme alandamise, salastatuse kustutamise, veo ja hävitamisega ning need täiendavad komisjoni dokumendihalduse üldeeskirju (otsused 2002/47/EÜ, ESTÜ, Euratom ([2]) ja 2004/563/EÜ, Euratom) ([3]).

([1]) Vrd „Arrangement entre le Gouvernement belge et le Parlement européen, le Conseil, la Commission, le Comité économique et social européen, le Comité des régions, la Banque européenne d'investissement en matière de sécurité", 31. detsember 2004, „Accord de sécurité signé entre la Commission et le Gouvernement luxembourgeois", 20. jaanuar 2007, ja „Accordo tra il Governo italiano e la Commissione europea dell'energia atomica (Euratom) per l'istituzione di un Centro comune di ricerche nucleari di competenza generale", 22. juuli 1959.

([2]) Komisjoni otsus 2002/47/EÜ, ESTÜ, Euratom, 23. jaanuar 2002, millega muudetakse komisjoni kodukorda (EÜT L 21, 24.1.2002, lk 23).

([3]) Komisjoni otsus 2004/563/EÜ, Euratom, 7. juuli 2004, millega muudetakse komisjoni kodukorda (ELT L 251, 27.7.2004, lk 9).

(8) Käesoleva otsuse sätted ei piira järgmiste õigusaktide kohaldamist:

a) määrus (Euratom) nr 3 ([1]);

b) Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 1049/2001 ([2]);

c) Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 45/2001 ([3]);

d) nõukogu määrus (EMÜ, Euratom) nr 354/83 ([4]),

ON VASTU VÕTNUD KÄESOLEVA OTSUSE:

1. PEATÜKK

ALUSPÕHIMÕTTED JA MIINIMUMSTANDARDID

Artikkel 1

Mõisted

Käesolevas otsuses kasutatakse järgmisi mõisteid:

1) „komisjoni talitus" – komisjoni mis tahes peadirektoraat või talitus või komisjoniliikme kabinet;

2) „krüptomaterjal" – krüptoalgoritmid, krüptoriistvara- ja -tarkvaramoodulid ning -tooted, sealhulgas rakendamise üksikasjad ja seotud dokumentatsioon ning kodeerimisandmed;

3) „salastatuse kustutamine" – salastatuse tühistamine;

4) „süvakaitse" – erinevate mitme kaitseliinina võetavate turvameetmete kohaldamine;

5) „dokument" – talletud teave selle füüsilisest kujust ja omadustest olenemata;

6) „taseme alandamine" – salastatuse taseme alandamine;

7) ELi salastatud teabe „töötlemine" – kõik võimalikud toimingud, mida võidakse ELi salastatud teabega selle kehtivusaja jooksul teha. See hõlmab teabe koostamist, registreerimist, töötlemist, vedu, salastatuse taseme alandamist, salastatuse kustutamist ja teabe hävitamist. Side- ja infosüsteemide puhul hõlmab see ka teabe kogumist, kuvamist, edastamist ja säilitamist;

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

9) „rakenduseeskirjad" – eeskirjade või julgeolekuteadete mis tahes kogum, mis on vastu võetud kooskõlas komisjoni otsuse (EL, Euratom) nr 2015/443 5. peatükiga ([5]);

10) „materjal" – mis tahes meedium, andmekandja või valmistatud või valmistamisel olev masin või seade;

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

12) „objektid" – komisjonile kuuluv kinnisvara või muu sarnane vara ja valdused;

([1]) Määrus (Euratom) nr 3, 31. juuli 1958, millega rakendatakse Euroopa Aatomienergiaühenduse asutamislepingu artiklit 24 (EÜT 17, 6.10.1958, lk 406/58).
([2]) Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 1049/2001, 30. mai 2001, üldsuse juurdepääsu kohta Euroopa Parlamendi, nõukogu ja komisjoni dokumentidele (EÜT L 145, 31.5.2001, lk 43).
([3]) Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 45/2001, 18. detsember 2000, üksikisikute kaitse kohta isikuandmete töötlemisel ühenduse institutsioonides ja asutustes ning selliste andmete vaba liikumise kohta (EÜT L 8, 12.1.2001, lk 1).
([4]) Nõukogu määrus (EMÜ, Euratom) nr 354/83, 1. veebruar 1983, mis käsitleb Euroopa Majandusühenduse ja Euroopa Aatomienergiaühenduse ajalooarhiivide avalikkusele kättesaadavaks tegemist (EÜT L 43, 15.2.1983, lk 1).
([5]) Komisjoni otsus (EL, Euratom) 2015/443, 13. märts 2015, komisjoni julgeoleku kohta (Vt käesoleva *Euroopa Liidu Teataja* lk 41).

13) „turvariski juhtimise protsess" – organisatsiooni või selle poolt kasutatavate süsteemide julgeolekut mõjutada võivate ebakindlate sündmuste kindlaksmääramise, kontrollimise ja minimeerimise kogu protsess. See hõlmab igasugust riskidega seotud tegevust, sealhulgas hindamist, käsitlemist, aktsepteerimist ja teavitamist;

14) „personalieeskirjad" – Euroopa Liidu ametnike personalieeskirjad ja Euroopa Liidu muude teenistujate teenistustingimused, mis on sätestatud nõukogu määruses (EMÜ, Euratom, ESTÜ) nr 259/68 ([1]);

15) „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;

16) „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, organisatsioonilist või operatiivset laadi.

Artikkel 2

Reguleerimisese ja reguleerimisala

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

2. Käesolevat otsust kohaldatakse kõigi komisjoni talituste ning kõigi komisjoni objektide suhtes.

3. Olenemata konkreetsetest viidetest teatavatele personali rühmadele kohaldatakse käesolevat otsust komisjoni liikmete, Euroopa Liidu ametnike personalieeskirjade ning liidu muude teenistujate teenistustingimuste kohaldamisalas oleva komisjoni personali, komisjoni lähetatud riikide ekspertide, teenusepakkujate ja nende personali, praktikantide ning kõigi isikute suhtes, kellel on juurdepääs komisjoni hoonetesse või muule varale või komisjoni töödeldavale teabele.

4. Käesoleva otsuse sätete kohaldamine ei piira otsuse 2002/47/EÜ, ESTÜ, Euratom ja otsuse 2004/563/EÜ, Euratom kohaldamist.

Artikkel 3

ELi salastatud teabe, salastatuse tasemete ja märgete määratlus

1. „ELi salastatud teave" – 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 ühele järgmistest tasemetest:

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

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

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 täiendavaid märkeid, mis ei ole ette nähtud liigitamiseks, vaid asjaomases dokumendis käsitletud valdkonda määratlevate, dokumendi koostajat tuvastavate, dokumendi levitamist või kasutamist piiravate või avaldatavuse märgetena.

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

Artikkel 4

Salastatuse tasemete haldamine

1. Komisjoni iga liige või talitus tagab, et tema koostatavale ELi salastatud teabele on määratud asjakohane salastatuse tase, teave on selgelt määratletud ELi 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 3 lõikes 2 osutatud salastatuse taseme märkeid ei muudeta ega kõrvaldata ilma dokumendi koostaja eelneva kirjaliku nõusolekuta, ilma et see piiraks artikli 26 kohaldamist.

3. Vajaduse korral võetakse artikli 60 kohaselt vastu rakenduseeskirjad ELi salastatud teabe töötlemise kohta ning taseme määramise praktiline juhend.

Artikkel 5

Salastatud teabe kaitse

1. ELi salastatud teavet kaitstakse käesoleva otsuse ja selle rakenduseeskirjade kohaselt.

2. ELi salastatud teabe valdaja vastutab selle kaitsmise eest kooskõlas käesoleva otsuse ja selle rakenduseeskirjadega ning vastavalt 4. peatüki sätetele.

3. Kui liikmesriigid sisestavad komisjoni struktuuridesse või võrkudesse riigisisest salastusmärget kandva salastatud teabe, kaitseb komisjon seda teavet kooskõlas nõuetega, mida kohaldatakse samaväärse salastatuse tasemega ELi salastatud teabe suhtes vastavalt I lisas esitatud salastatuse tasemete vastavustabelile.

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

Artikkel 6

Turvariski juhtimine

1. Turvameetmed, mis on vajalikud ELi salastatud teabe kaitsmiseks kogu kehtivusaja 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.

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

3. Kõigi talituste talitluspidevuse plaanidesse lisatakse ennetus- ja taastamismeetmed, et minimeerida ulatuslike rikete või intsidentide mõju ELi salastatud teabe töötlemisele ja säilitamisele.

Artikkel 7

Käesoleva otsuse rakendamine

1. Vajaduse korral võetakse artikli 60 kohaselt vastu rakenduseeskirjad käesoleva otsuse täiendamiseks või toetamiseks.

2. Komisjoni talitused võtavad oma vastutusalas kõik vajalikud meetmed, et tagada käesoleva otsuse ja asjaomaste rakenduseeskirjade täitmine ELi salastatud teabe ja muu salastatud teabe töötlemisel või säilitamisel.

3. Käesoleva otsuse rakendamiseks võetud turvameetmed peavad vastama otsuse (EÜ, Euratom) 2015/443 artiklis 3 esitatud komisjoni julgeolekupõhimõtetele.

4. Personali- ja turvalisusküsimuste peadirektoraadi peadirektor moodustab personali- ja turvalisusküsimuste peadirektoraadis komisjoni julgeolekuasutuse. Komisjoni julgeolekuasutus täidab talle käesoleva otsuse ja selle rakenduseeskirjadega antud ülesandeid.

5. Igas komisjoni talituses täidab kohalik julgeolekuametnik, kellele on osutatud otsuse (EÜ, Euratom) 2015/443 artiklis 20, järgmisi üldisi ülesandeid ELi salastatud teabe kaitsmiseks kooskõlas käesoleva otsusega, tehes tihedat koostööd personali- ja turvalisusküsimuste peadirektoraadiga:

a) komisjoni antavate personali juurdepääsulubade taotluste haldamine;

b) julgeolekukoolituste ja teadlikkuse suurendamise infotundide korraldamisele kaasaaitamine;

c) talituse registri kontrolliametniku juhendamine;

d) teavitamine julgeolekunõuete rikkumisest ja ELi salastatud teabe ohtusattumisest;

e) varuvõtmete ja iga kirjalikult ülestähendatud koodikombinatsiooni haldamine;

f) muude ELi salastatud teabe kaitsega seotud või rakenduseeskirjades sätestatud ülesannete täitmine.

Artikkel 8

Julgeolekunõuete rikkumine ja ELi salastatud teabe ohtusattumine

1. Julgeolekunõuete rikkumine toimub isiku sellise tegevuse või tegevusetuse tagajärjel, mis on vastuolus käesolevas otsuses sätestatud julgeolekunormidega ja otsuse rakenduseeskirjadega.

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

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

4. Kui on teada või kui on alust arvata, et ELi salastatud teave on ohtu sattunud või kadunud, tehakse kooskõlas otsuse (EÜ, Euratom) 2015/443 artikliga 13 julgeolekualane uurimine.

5. Võetakse kõik vajalikud meetmed, et:

a) teavitada teabe koostajat;

b) tagada asjaolude kindlakstegemise huvides, et uurimisega tegelevad töötajad, kes ei ole rikkumisega vahetult seotud;

c) hinnata liidu või liikmesriikide huvidele tekitatud võimalikku kahju;

d) võtta sobivaid meetmeid sellise juhtumi kordumise ennetamiseks ning

e) teavitada asjaomaseid asutusi võetud meetmetest.

6. Iga isiku suhtes, kes on vastutav käesolevas otsuses sätestatud julgeolekunormide rikkumise eest, võib kohaldada distsiplinaarmeetmeid vastavalt personalieeskirjadele. Iga isiku suhtes, kes on vastutav ELi salastatud teabe ohtusattumise või kadumise eest, kohaldatakse distsiplinaar- ja/või õiguslikke meetmeid vastavalt kohaldatavatele õigusnormidele.

2. PEATÜKK

TÖÖTAJATEGA SEOTUD JULGEOLEK

Artikkel 9

Mõisted

Käesolevas peatükis kasutatakse järgmisi mõisteid:

1) „luba juurdepääsuks ELi salastatud teabele" – komisjoni julgeolekuasutuse otsus, mis on tehtud liikmesriigi pädeva asutuse kinnituse põhjal, et komisjoni ametnikule, muule teenistujale või lähetatud riiklikule eksperdile võib eeldusel, et tema teadmisvajadus on kindlaks määratud ja talle on nõuetekohaselt selgitatud tema kohustusi, lubada kindlaksmääratud kuupäevani juurdepääsu teatava salastatuse tasemega (CONFIDENTIEL UE/EU CONFIDENTIAL või kõrgem) ELi salastatud teabele; sellist isikut loetakse „komisjoni julgeolekukontrolli läbinuks";

2) „personali julgeolekukontroll" – selliste meetmete kohaldamine, millega tagatakse juurdepääs ELi salastatud teabele ainult isikutele:

   a) kellel on teadmisvajadus;

   b) kes on läbinud vajalikul tasemel julgeolekukontrolli, kui see on asjakohane, ning

   c) keda on teavitatud nende vastutusest;

3) „juurdepääsuluba" – liikmesriigi pädeva asutuse avaldus, mis tehakse pärast julgeolekukontrolli lõpuleviimist liikmesriigi pädevate asutuste poolt ja mis kinnitab, et isikule võib lubada kindlaksmääratud kuupäevani juurdepääsu teatava salastatuse tasemega (CONFIDENTIEL UE/EU CONFIDENTIAL või kõrgem) ELi salastatud teabele, tingimusel et tema teadmisvajadus on kindlaks tehtud ja teda on nõuetekohaselt teavitatud tema vastutusest;

4) „juurdepääsutõend" – pädeva asutuse väljastatud tõend, mis kinnitab, et isikul on komisjoni julgeolekuasutuse väljastatud kehtiv juurdepääsuluba või komisjoni antav juurdepääsuluba juurdepääsuks ELi salastatud teabele, millel on kirjas, millisel salastatuse tasemel (CONFIDENTIEL UE/EU CONFIDENTIAL või kõrgem) ELi salastatud teabele võib asjaomasele isikule juurdepääsu lubada, vastava juurdepääsuloa kehtivusaeg ja tõendi enda kehtivuse lõppemise kuupäev;

5) „julgeolekukontroll" – kontroll, mille teeb liikmesriigi pädev asutus kõnealuses liikmesriigis kehtivate õigusnormide kohaselt, et saada kinnitust selle kohta, et ei ole teada midagi kahtlust äratavat, mis takistaks andmast isikule juurdepääsu teatava salastatuse tasemega (CONFIDENTIEL UE/EU CONFIDENTIAL või kõrgem) ELi salastatud teabele.

Artikkel 10

Aluspõhimõtted

1. Isikule antakse juurdepääs ELi salastatud teabele pärast seda, kui:

(1) tema teadmisvajadus on kindlaks tehtud;

(2) teda on teavitatud ELi salastatud teabe kaitseks vajalikest julgeolekunormidest ja vastavatest julgeolekustandarditest ja -suunistest ning ta on kinnitanud oma vastutust seoses kõnealuse teabe kaitsmisega;

(3) ta on juurdepääsuks CONFIDENTIEL UE/EU CONFIDENTIAL või kõrgemal tasemel salastatud teabele läbinud asjaomase taseme julgeolekukontrolli või tal on vastavalt siseriiklikele õigusnormidele muud ametiülesannetest tulenevad volitused.

2. Kõik isikud, kes võivad oma tööülesannete tõttu vajada juurdepääsu CONFIDENTIEL UE/EU CONFIDENTIAL või kõrgemal tasemel ELi salastatud teabele, peavad enne, kui neile antakse juurdepääs sellisele ELi salastatud teabele, läbima asjaomase taseme julgeolekukontrolli. Asjaomane isik esitab kirjaliku nõusoleku julgeolekukontrolli menetluse läbimiseks. Nõusoleku esitamata jätmine tähendab, et kõnealust isikut ei ole võimalik määrata ametisse või täitma kohustust või ülesannet, mis eeldab juurdepääsu CONFIDENTIEL UE/EU CONFIDENTIAL või kõrgemal tasemel salastatud teabele,

3. Julgeolekukontrolli menetluse alusel peab olema võimalik kindlaks teha, kas isikule võib tema lojaalsust ja usaldusväärsust arvesse võttes lubada juurdepääsu ELi salastatud teabele.

4. Isiku lojaalsus ja usaldusväärsus seoses tema julgeolekukontrolli läbimisega juurdepääsuks CONFIDENTIEL UE/EU CONFIDENTIAL või kõrgemal tasemel salastatud teabele tehakse kindlaks julgeolekukontrolli abil, mille sooritavad liikmesriigi pädevad asutused kooskõlas siseriiklike õigusnormidega.

5. Komisjoni julgeolekuasutus vastutab ainuisikuliselt suhtlemise eest riiklike julgeolekuasutusega või muude pädevate siseriiklike asutustega julgeolekukontrolliga seotud küsimustes. Kogu suhtlus komisjoni talituste ja personali ning riiklike julgeolekuasutuste ja muude pädevate asutuste vahel toimub komisjoni julgeolekuasutuse kaudu.

Artikkel 11

Komisjoni julgeolekukontrolli kord

1. Komisjoni iga peadirektor või talituse juhataja teeb kindlaks oma talituse ametikohad, millel töötajad vajavad oma ülesannete täitmiseks juurdepääsu CONFIDENTIEL UE/EU CONFIDENTIAL või kõrgemal tasemel salastatud teabele ja peavad seetõttu läbima julgeolekukontrolli.

2. Niipea kui on teada, et isik määratakse ametikohale, kus on nõutav juurdepääs CONFIDENTIEL UE/EU CONFIDENTIAL või kõrgemal tasemel salastatud teabele, teavitab komisjoni vastava talituse kohalik julgeolekuametnik komisjoni julgeolekuasutust, kes saadab seejärel kõnealusele isikule julgeolekukontrolli ankeedi, mille on väljastanud selle liikmesriigi riiklik julgeolekuasutus, kelle kodanikuna isik on Euroopa Liidu institutsioonide töötajaks nimetatud. Kõnealune isik annab kirjaliku nõusoleku julgeolekukontrolli menetluse läbimiseks ning tagastab täidetud ankeedi võimalikult peatselt komisjoni julgeolekuasutusele.

3. Komisjoni julgeolekuasutus edastab täidetud julgeolekukontrolli ankeedi selle liikmesriigi riiklikule julgeolekuasutusele, kelle kodanikuna asjaomane isik on Euroopa Liidu institutsioonide töötajaks nimetatud, taotledes sellele ELi salastatud teabe tasemele vastava julgeolekukontrolli tegemist, millele asjaomane isik juurdepääsu vajab.

4. Kui komisjoni julgeolekuasutusele saab teatavaks juurdepääsuluba taotlevat isikut puudutav julgeolekukontrolli seisukohast oluline teave, teatab komisjoni julgeolekuasutus asjakohaste õigusnormide kohaselt toimides sellest pädevale riiklikule julgeolekuasutusele.

5. Pärast julgeolekukontrolli lõpuleviimist ja võimalikult kiiresti pärast asjaomaselt riiklikult julgeolekuasutuselt julgeolekukontrolli tulemuste üldise hinnangu saamist:

a) võib komisjoni julgeolekuasutus anda asjaomasele isikule loa juurdepääsuks ELi salastatud teabele ning lubada juurdepääsu ELi salastatud teabele kuni vastava salastatuse tasemeni ja tema kindlaksmääratud kuupäevani kuni viieks aastaks, juhul kui julgeolekukontrolli tulemused kinnitavad isiku lojaalsust ja usaldusväärsust kahjustavate asjaolude puudumist;

b) kohustub komisjoni julgeolekuasutus, juhul kui julgeolekukontroll sellist kinnitust ei anna, teavitama kooskõlas asjakohaste õigusnormidega asjaomast isikut, kellel on õigus taotleda ärakuulamist komisjoni julgeolekuasutuse poolt, kes omakorda võib nõuda riiklikult julgeolekuasutuselt täiendavaid selgitusi, kui see on siseriiklike õigusnormide kohaselt võimalik. Julgeolekukontrolli tulemuse kinnitamise korral juurdepääsuluba ELi salastatud teabele ei väljastata.

6. Julgeolekukontrolli, sealhulgas selle tulemuste suhtes kohaldatakse asjaomases liikmesriigis kehtivaid õigusnorme, sealhulgas neid, mis käsitlevad edasikaebamist. Komisjoni julgeolekuasutuse otsuse võib personalieeskirjade kohaselt edasi kaevata.

7. Komisjon 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 komisjonis täidab. Liidu institutsioon, organ või asutus, kus isik tööle asub, teatab asjaomasele riiklikule julgeolekuasutusele tööandja muutumisest.

8. Kui isiku teenistusperiood ei alga 12 kuu jooksul julgeolekukontrolli tulemuse teatamisest komisjoni julgeolekuasutusele või kui isiku teenistus katkeb 12 kuuks, mille jooksul ta ei tööta komisjonis või üheski muus liidu institutsioonis, organis või asutuses või liikmesriigi valitsusasutuse ametikohal, pöördub komisjoni julgeolekuasutus juurdepääsuloa kehtivuse ja nõuetekohasuse kohta kinnituse saamiseks asjaomase riikliku julgeolekuasutuse poole.

9. Kui komisjoni julgeolekuasutusele saab teatavaks kehtivat komisjoni antavat juurdepääsuluba omava isikuga seotud turvariski puudutav teave, teatab julgeolekuasutus asjakohaste õigusnormide kohaselt toimides sellest pädevale riiklikule julgeolekuasutusele.

10. Kui riiklik julgeolekuasutus teatab komisjoni julgeolekuasutusele kehtivat ELi salastatud teabele juurdepääsu luba omava isiku kohta lõike 5 punkti a kohaselt antud kinnituse tühistamisest, võib komisjoni julgeolekuasutus paluda riiklikult julgeolekuasutuselt selgitust, kui selle andmine on siseriiklike õigusnormide kohaselt võimalik. Kui riiklik julgeolekuasutus kinnitab isiku usaldusväärsust kahjustavat teavet, tühistatakse komisjoni antav juurdepääsuluba ning isikule keelatakse juurdepääs ELi salastatud teabele ja ametikohtadele, mille puhul selline juurdepääs on võimalik või mille puhul isik võiks ohustada julgeolekut.

11. Käesoleva otsuse reguleerimisalasse kuuluva isiku ELi salastatud teabele juurdepääsu loa tühistamise või peatamise otsusest ja vajaduse korral selle põhjustest teavitatakse asjaomast isikut, kes võib paluda, et komisjoni julgeolekuasutus kuulaks ära tema selgitused. Riikliku julgeolekuasutuse esitatud teabe suhtes kohaldatakse asjaomases liikmesriigis kehtivaid asjakohaseid õigusakte. Komisjoni julgeolekuasutuse sellekohase otsuse võib personalieeskirjade kohaselt edasi kaevata.

12. Komisjoni talitused teevad kindlaks, et riiklikud eksperdid, kes on lähetatud CONFIDENTIEL UE/EU CONFIDENTIAL või sellest kõrgemal tasemel ELi salastatud teabele komisjoni antavat juurdepääsuluba nõudvale ametikohale, esitavad kooskõlas siseriiklike õigusnormidega kehtiva juurdepääsuloa või juurdepääsutõendi enne tööle asumist komisjoni julgeolekuasutusele, kes annab selle alusel komisjoni juurdepääsuloa ELi salastatud teabele kuni tasemeni, mis on samaväärne riiklikul juurdepääsuloal osutatud tasemega, ja maksimaalse kehtivusajaga kuni tööülesannete täitmise lõpuni.

Ametiülesannetest tulenevat juurdepääsuõigust omavate isikute juurdepääs ELi salastatud teabele

13. Komisjoni liikmeid, kellel on aluslepingu kohaselt ametiülesannetest tulenev juurdepääs ELi salastatud teabele, teavitatakse nende julgeolekualastest kohustustest seoses ELi salastatud teabe kaitsmisega.

Juurdepääsulubade ja komisjoni antavate juurdepääsulubade registrid

14. Kooskõlas käesoleva otsusega peab komisjoni julgeolekuasutus ELi salastatud teabele juurdepääsuks antud juurdepääsulubade ja komisjoni antavate juurdepääsulubade registreid. Kõnealused registrid sisaldavad vähemalt andmeid selle kohta, millisel salastatuse tasemel ELi salastatud teabele võib asjaomasele isikule juurdepääsu lubada, ning juurdepääsuloa andmise kuupäeva ja kehtivusaja kohta.

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

Komisjoni antavate juurdepääsulubade kehtivuse pikendamine

16. Pärast komisjoni antava juurdepääsuloa esmakordset andmist ja tingimusel, et isik on vaheaegadeta olnud Euroopa Komisjoni või muu liidu institutsiooni, organi või asutuse teenistuses ja vajab endiselt juurdepääsu ELi salastatud teabele, tuleb komisjoni antavat juurdepääsuluba kehtivuse pikendamiseks läbi vaadata reeglina iga viie aasta järel alates asjaomaste lubade andmise aluseks olnud viimase julgeolekukontrolli tulemustest teavitamise kuupäevast.

17. Komisjoni julgeolekuasutus võib pikendada olemasoleva komisjoni antava juurdepääsuloa kehtivust kuni 12 kuuks, kui asjaomane riiklik julgeolekuasutus või muu pädev riiklik asutus ei ole andnud teada usaldusväärsust kahjustavatest asjaoludest kahe kuu jooksul alates pikendamistaotluse ja sellele vastava julgeolekukontrolli ankeedi esitamise kuupäevast. Kui selle 12kuulise perioodi lõppedes ei ole asjaomane riiklik julgeolekuasutus või muu pädev riiklik asutus komisjoni julgeolekuasutust oma seisukohast teavitanud, antakse asjaomasele isikule selliseid tööülesandeid, mille täitmine ei nõua komisjoni antavat juurdepääsuluba.

Artikkel 12

Komisjoni julgeolekukontrolli käsitlevad infotunnid

1. Pärast komisjoni julgeolekuasutuse korraldatud ja komisjoni julgeolekukontrolli käsitlevates infotundides osalemist kinnitavad kõik julgeolekukontrolli läbinud isikud kirjalikult, et nad mõistavad oma kohustusi seoses ELi salastatud teabe kaitsmisega ning on teadlikud tagajärgedest, mis kaasnevad ELi salastatud teabe ohtusattumisega. Nimetatud kirjalike kinnituste registrit peab komisjoni julgeolekuasutus.

2. 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 komisjoni julgeolekuasutusele mis tahes tegevusest, mida nad peavad kahtlustäratavaks või ebatavaliseks.

3. 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.

Artikkel 13

Komisjoni antavad ajutised juurdepääsuload

1. Erakorralistel asjaoludel, kui see on talituse huvide tõttu nõuetekohaselt põhjendatud, võib komisjoni julgeolekuasutus pärast selle liikmesriigi riikliku julgeolekuasutusega konsulteerimist, mille kodanik asjaomane isik on, ning isiku usaldusväärsust kahjustavate asjaolude puudumise kinnitamiseks tehtud eelkontrollide tulemusest olenevalt anda enne täieliku julgeolekukontrolli lõpulejõudmist isikutele konkreetse ülesande täitmiseks ajutise loa juurdepääsuks ELi salastatud teabele, ilma et see piiraks juurdepääsulubade kehtivuse pikendamise sätteid. Nimetatud ajutisi lube antakse juurdepääsuks ELi salastatud teabele ühekordselt kuni kuueks kuuks ja need ei võimalda juurdepääsu TRES SECRET UE/EU TOP SECRET tasemel salastatud teabele.

2. Pärast artikli 12 lõike 1 kohaselt selgituste saamist kinnitavad kõik ajutise loa saanud isikud kirjalikult, et nad mõistavad oma kohustusi seoses ELi salastatud teabe kaitsmisega ning on teadlikud tagajärgedest, mis kaasnevad ELi salastatud teabe ohtusattumisega. Nimetatud kirjalike kinnituste registrit peab komisjoni julgeolekuasutus.

Artikkel 14

Osalemine komisjoni korraldatud salajastel koosolekutel

1. Komisjoni talitused, kes korraldavad koosolekuid, kus käsitletakse CONFIDENTIEL UE/EU CONFIDENTIAL või kõrgemal tasemel salastatud teavet, teavitavad kohaliku julgeolekuametniku või koosoleku korraldaja vahendusel komisjoni julgeolekuasutust aegsasti kõnealuste koosolekute kuupäevadest, kellaaegadest, toimumiskohtadest ja osalejatest.

2. Kui artikli 11 lõikest 13 ei tulene teisiti, võivad isikud, kellele on tehtud ülesandeks osaleda komisjoni koosolekutel, kus käsitletakse CONFIDENTIEL UE/EU CONFIDENTIAL või kõrgemal tasemel salastatud teavet, teha seda alles pärast nende juurdepääsuloa olemasolu või julgeolekukontrolli läbimise kontrollimist. Juurdepääsu salajastele koosolekutele ei võimaldata isikutele, kelle juurdepääsutõendit või muud tõendusmaterjali julgeolekukontrolli läbimise kohta ei ole komisjon näinud, või komisjoni kuuluvatele osalejatele, kellel puudub komisjoni antav juurdepääsuluba.

3. Enne salajase koosoleku korraldamist palub vastutav korraldaja või koosolekut korraldava komisjoni talituse kohalik julgeolekuametnik väliskülalistel esitada komisjoni julgeolekuasutusele juurdepääsutõend või muu tõendusmaterjal julgeolekukontrolli läbimise kohta. Komisjoni julgeolekuasutus teavitab kohalikku julgeolekuametnikku või koosoleku korraldajat esitatud juurdepääsutõendist või muust tõendusmaterjalist juurdepääsuloa olemasolu kohta. Vajaduse korral võib kasutada koondnimekirja, milles on esitatud asjakohane tõendusmaterjal julgeolekukontrolli läbimise kohta.

4. Kui pädevad asutused annavad komisjoni julgeolekuasutusele teada, et sellise isiku juurdepääsuluba, kelle tööülesanded eeldavad osalemist komisjoni korraldatud koosolekutel, on tühistatud, teavitab komisjoni julgeolekuasutus sellest koosoleku korraldamise eest vastutava komisjoni talituse kohalikku julgeolekuametnikku.

Artikkel 15

Võimalik juurdepääs ELi salastatud teabele

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

3. PEATÜKK

SALASTATUD TEABE KAITSEKS ARENDATAV FÜÜSILINE JULGEOLEK

Artikkel 16

Aluspõhimõtted

1. 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 alusel. Nimetatud meetmed tehakse kindlaks riskijuhtimisprotsessi käigus kooskõlas käesoleva otsuse ja selle rakenduseeskirjadega.

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

a) tagada, et ELi salastatud teavet töödeldakse ja säilitatakse 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.

3. Füüsilise julgeoleku meetmeid rakendatakse kõikide objektide, hoonete, ametiruumide ning muude ruumide ja alade suhtes, kus töödeldakse või säilitatakse ELi salastatud teavet, sealhulgas alade suhtes, kus paiknevad 5. peatükis osutatud side- ja infosüsteemid.

4. Alad, kus säilitatakse CONFIDENTIEL UE/EU CONFIDENTIAL või kõrgemal tasemel ELi salastatud teavet, luuakse käesoleva peatüki kohaste turvaaladena ning need akrediteerib komisjoni turvalisuse akrediteerimise asutus.

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

Artikkel 17

Füüsilise julgeoleku nõuded ja meetmed

1. Füüsilise julgeoleku meetmed valitakse välja komisjoni julgeolekuasutuse koostatava ohuhinnangu alusel, konsulteerides vajaduse korral teiste komisjoni talituste, liidu institutsioonide, asutuste või organite ja/või liikmesriikide pädevate asutustega. Komisjon kohaldab 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, selle institutsioonide, organite või asutuste või liikmesriikide vastu, ning sabotaažist, terrorismist ja õõnestavast või muust kriminaalsest tegevusest tulenevale ohule.

2. Süvakaitse põhimõttele tuginedes määrab komisjoni julgeolekuasutus kindlaks, milliseid asjakohaseid füüsilise julgeoleku meetmeid rakendada. Selleks koostab komisjoni julgeolekuasutus miinimumstandardid, normid ja kriteeriumid, mis sätestatakse rakenduseeskirjades.

3. Komisjoni julgeolekuasutusel on lubatud korraldada sisse- ja väljapääsudes läbiotsimisi, et takistada loata esemete toomist objektidele või hoonetesse või ELi salastatud teabe sealt loata väljaviimist.

4. Kui on oht, et ELi salastatud teavet võidakse jälgida, isegi kui see toimub juhuslikult, võtavad komisjoni asjaomased talitused selle takistamiseks asjakohaseid meetmeid, mille on kindlaks määranud komisjoni julgeolekuasutus.

5. Uute rajatiste puhul määratakse komisjoni julgeolekuasutuse heakskiidul kindlaks füüsilise julgeoleku nõuded ja nende funktsionaalne kirjeldus osana rajatiste planeerimise ja projekteerimise protsessist. Olemasolevate rajatiste puhul rakendatakse füüsilise julgeoleku nõudeid rakenduseeskirjades sätestatud miinimumstandardite, normide ja kriteeriumide kohaselt.

Artikkel 18

ELi salastatud teabe füüsilise kaitse seadmed

1. ELi salastatud teabe füüsiliseks kaitsmiseks luuakse kaht tüüpi füüsiliselt kaitstud alad:

a) haldustegevuse alad ning

b) turvaalad (sealhulgas tehniliselt kaitstud turvaalad).

2. Komisjoni turvalisuse akrediteerimise asutus tõendab, et ala vastab nõuetele, mille alusel võib selle tunnistada haldustegevuse alaks, turvaalaks või tehniliselt kaitstud turvaalaks.

3. 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 komisjoni julgeolekuasutus või muu pädev asutus on selleks nõuetekohaselt volitanud, ning

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

4. 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;

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

5. 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.

6. Pealtkuulamise vastu kaitstud turvaalad määratakse tehniliselt kaitstud turvaaladeks. Kohaldatakse järgmisi täiendavaid nõudeid:

a) alad varustatakse sissetungi avastamise süsteemiga; kui alad ei ole kasutuses, on need lukustatud, ja kui alad on kasutusel, neid valvatakse. Kõiki võtmeid hallatakse vastavalt artiklile 20;

b) kõiki sellistele aladele sisenevaid isikuid ja esemeid kontrollitakse;

c) selliseid alasid kontrollib regulaarselt füüsiliselt ja/või tehniliselt komisjoni julgeolekuasutus. Sellised kontrollid tehakse ka iga loata sisenemise või sellise sisenemise kahtluse korral ning

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

7. Olenemata punkti 6 alapunktist d vaatab komisjoni 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.

8. Turvaalasid, kus töötajad ei viibi 24 tundi ööpäevas, kontrollitakse vajaduse korral tavapärase tööaja lõppedes ja pisteliselt väljaspool tavapärast tööaega, välja arvatud juhul, kui alale on paigaldatud sissetungi avastamise süsteem.

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

10. Komisjoni asjaomase talituse kohalik julgeolekuametnik koostab turvanõuete rakendamise korra iga oma vastutusalas oleva turvaala kohta, määrates kooskõlas käesoleva otsuse ja selle rakenduseeskirjade sätetega kindlaks:

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 komisjoni julgeolekukontrolli läbimisest tulenevalt lubatud alale siseneda saatjata;

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

e) muud asjakohased meetmed ja toimingud.

11. Turvaaladele ehitatakse turvakambrid. Turvakambrite seinad, põrandad, laed, aknad ja lukustatavad uksed peavad olema komisjoni julgeolekuasutuse heakskiiduga ja pakkuma samaväärset kaitset kui samal tasemel ELi salastatud teabe säilitamiseks heakskiidetud seifid.

Artikkel 19

Füüsilised kaitsemeetmed ELi salastatud teabe töötlemiseks ja säilitamiseks

1. 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

c) väljaspool turvaala või haldustegevuse ala, tingimusel et valdaja veab ELi salastatud teavet vastavalt artiklile 31 ja kohustub järgima rakendusmeetmetes sätestatud kompenseerivaid meetmeid, mis tagavad ELi salastatud teabe kaitse volitamata isikute juurdepääsu eest.

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

3. 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) kohustub järgima rakenduseeskirjades sätestatud kompenseerivaid meetmeid, mis tagavad ELi salastatud teabe kaitse volitamata isikute juurdepääsu eest,

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

   iii) on paberkujul dokumentide puhul teavitanud sellest asjaomast registrit.

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

5. TRES SECRET UE/EU TOP SECRET tasemel ELi salastatud teavet töödeldakse turvaalal, mille rajamise ja haldamise eest vastutab komisjoni julgeolekuasutus ning mille on vastaval tasemel akrediteerinud komisjoni turvalisuse akrediteerimise asutus.

6. TRÈS SECRET UE/EU TOP SECRET tasemel ELi salastatud teavet säilitatakse turvaalal, mille on vastaval tasemel akrediteerinud komisjoni turvalisuse akrediteerimise asutus, ühel järgmistest tingimustest:

a) seifis vastavalt artikli 18 sätetega, kasutades ühte või mitut järgmistest täiendavatest kontrollimeetmetest:

   (1) julgeolekukontrolli läbinud turvatöötajate või valvetöötajate pidev kaitse või kontroll;

   (2) heakskiidetud sissetungi avastamise süsteem koos turvateenistuse reageerimisüksusega,

   või

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

Artikkel 20

ELi salastatud teabe kaitseks kasutatavate võtmete ja koodide haldamine

1. Ametiruumide, muude ruumide, turvakambrite ning seifide võtmete ja koodide haldamise kord kehtestatakse rakenduseeskirjades artikli 60 kohaselt. Selline kord peab kaitsma volitamata juurdepääsu eest.

2. 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 seifi saamisel;

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.

4. PEATÜKK

ELI SALASTATUD TEABE HALDAMINE

Artikkel 21

Aluspõhimõtted

1. Kõiki ELi salastatud dokumente tuleb hallata kooskõlas komisjoni dokumendihalduse poliitikaga ning seetõttu registreerida, kataloogida, säilitada ja hiljem hävitada, valimisse kaasata või ajalooarhiividesse saata vastavalt Euroopa Komisjoni toimikute suhtes kehtivale ühtsele komisjoniülesele säilitustähtaegade loetelule.

2. CONFIDENTIEL UE/EU CONFIDENTIAL või kõrgemal tasemel salastatud teave registreeritakse julgeolekukaalutlustel enne levitamist ja selle vastuvõtmisel. TRÈS SECRET UE/EU TOP SECRET tasemel salastatud teave registreeritakse selleks ettenähtud registrites.

3. Komisjonis luuakse kooskõlas artikli 27 sätetega ELi salastatud teabe registrisüsteem.

4. Komisjoni julgeolekuasutus kontrollib regulaarselt komisjoni talitusi ja objekte, kus toimub ELi salastatud teabe töötlemine või säilitamine.

5. ELi salastatud teabe edastamine talituste ja objektide vahel väljaspool füüsiliselt kaitstud alasid toimub järgmiselt:

a) üldjuhul edastatakse ELi salastatud teave elektrooniliselt, kaitstuna 5. peatüki kohaselt heakskiidetud krüptovahenditega;

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

   i) elektroonilisel andmekandjal (nt USB mälupulk, CD, kõvaketas), kaitstuna 5. peatüki kohaselt heakskiidetud krüptovahenditega, või

   ii) kõigil muudel juhtudel rakenduseeskirjade kohaselt.

Artikkel 22

Salastatuse tasemed ja märked

1. Teave peab olema salastatud, kui see vajab artikli 3 lõike 1 kohaselt kaitset seoses oma konfidentsiaalsusega.

2. ELi salastatud teabe koostaja vastutab selle salastatuse taseme määramise eest vastavalt asjaomastele salastamise rakenduseeskirjadele, standarditele ja suunistele ning teabe esialgse levitamise eest.

3. ELi salastatud teabe salastatuse tase määratakse artikli 3 lõike 2 ning asjaomaste rakenduseeskirjade kohaselt.

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

5. 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.

6. 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.

7. 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.

8. 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 juurdelisatud dokumentideta, kasutades selleks asjakohast märget, näiteks:

CONFIDENTIEL UE/EU CONFIDENTIAL

Manus(t)eta RESTREINT UE/EU RESTRICTED

Artikkel 23

Märked

Lisaks ühele artikli 3 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;

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

Artikkel 24

Salastusmärgete lühendid

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

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

TRES 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

Artikkel 25

ELi salastatud teabe koostamine

1. ELi salastatud dokumendi koostamisel:

a) märgitakse igale leheküljele selgelt salastatuse tase;

b) nummerdatakse iga lehekülg;

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

d) märgitakse dokumendile koostamise kuupäev;

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

2. Kui punkti 1 ei ole võimalik ELi salastatud teabe suhtes kohaldada, võetakse kooskõlas rakenduseeskirjadega muid sobivaid meetmeid.

Artikkel 26

ELi salastatud teabe salastatuse taseme alandamine ja salastatuse kustutamine

1. Teabe koostamise ajal märgib koostaja võimaluse korral, kas ELi salastatud teabe salastatuse taset võib teataval kuupäeval või konkreetse sündmuse järel alandada või selle kustutada.

2. Komisjoni iga talitus vaatab korrapäraselt läbi tema koostatud ELi salastatud teabe, et teha kindlaks, kas salastatuse tase on jätkuvalt kehtiv. Rakenduseeskirjadega kehtestatakse süsteem, mille abil vaadatakse vähemalt iga viie aasta järel läbi sellise registreeritud ELi salastatud teabe salastatuse tase, mille on koostanud komisjon. 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.

3. RESTREINT UE/EU RESTRICTED tasemel salastatud ja komisjoni koostatud teabe salastatus loetakse automaatselt kustutatuks kolmekümne aasta möödudes kooskõlas määrusega (EMÜ, Euratom) nr 354/83, mida on muudetud nõukogu määrusega (EÜ, Euratom) nr 1700/2003 ([1]).

Artikkel 27

ELi salastatud teabe registrisüsteem komisjonis

1. Ilma et see piiraks artikli 52 lõike 5 sätete kohaldamist, määratakse igas komisjoni talituses, kus töödeldakse või säilitatakse CONFIDENTIEL UE/EU CONFIDENTIAL või SECRET UE/EU SECRET tasemel salastatud teavet, ELi salastatud teabe kohalik register, mille ülesanne on tagada ELi salastatud teabe töötlemine käesoleva otsuse kohaselt.

2. ELi salastatud teabe registrit haldab peasekretariaat ja see on ELi salastatud teabe keskregister komisjonis. Register toimib:

— ELi salastatud teabe kohaliku registrina komisjoni peasekretariaadile;

— ELi salastatud teabe registrina komisjoniliikmete kabinettidele, kui neil puudub vastav kohalik ELi salastatud teabe register;

— ELi salastatud teabe registrina peadirektoraatidele või talitustele, millel puudub kohalik ELi salastatud teabe register;

— peamise sisenemis- ja väljumispunktina RESTREINT UE/EU RESTRICTED tasemest kuni SECRET UE/EU SECRET tasemeni salastatud teabe puhul, mida komisjon ja tema talitused vahetavad kolmandate riikide ja rahvusvaheliste organisatsioonidega, ning erikorra kohaldamisel teabe puhul, mida vahetatakse teiste liidu institutsioonide, organite ja asutustega.

3. Komisjoni julgeolekuasutus määrab komisjonisisese registri, mis toimib TRÈS SECRET UE/EU TOP SECRET tasemel salastatud teabe puhul keskse vastuvõtva ja edastava asutusena. Vajaduse korral võib määrata allregistreid kõnealust teavet registreerimise eesmärgil töötlema.

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

5. ELi salastatud teabe registrid luuakse 3. peatükis määratletud turvaaladena ning need akrediteerib komisjoni turvalisuse akrediteerimise asutus.

Artikkel 28

Registri kontrolliametnik

1. Iga ELi salastatud teabe registrit haldab registri kontrolliametnik.

2. Registri kontrolliametnik peab olema läbinud nõuetekohase julgeolekukontrolli.

3. Registri kontrolliametnik jääb komisjoni talituse kohaliku julgeolekuametniku järelevalve alla seoses ELi salastatud dokumentide töötlemist käsitlevate sätete kohaldamise ning asjaomaste julgeolekunormide, -standardite ja -suuniste järgimisega.

4. Registri kontrolliametnik täidab oma vastutusalas oleva ELi salastatud teabe registri haldamisel järgmisi peamisi ülesandeid kooskõlas käesoleva otsuse ning asjaomaste rakenduseeskirjade, standardite ja suunistega:

— ELi salastatud teabe registreerimise, säilitamise, reprodutseerimise, tõlkimise, edastamise, saatmise, hävitamise või ajalooarhiivide talitusse saatmisega seotud tegevuse juhtimine;

— teabe salastatuse säilitamise vajaduse regulaarne kontrollimine;

— muude ELi salastatud teabe kaitsega seotud ja rakenduseeskirjades sätestatud ülesannete täitmine.

Artikkel 29

ELi salastatud teabe registreerimine julgeolekukaalutlustel

1. Käesolevas otsuses tähendab julgeolekukaalutlustel registreerimine (edaspidi „registreerimine") selliste menetluste kohaldamist, mille abil talletatakse ELi salastatud teabe kehtivusaja iga etapp, sealhulgas teabe levitamine.

([1]) Nõukogu määrus (EÜ, Euratom) nr 1700/2003, 22. september 2003, millega muudetakse määrust (EMÜ, Euratom) nr 354/83, mis käsitleb Euroopa Majandusühenduse ja Euroopa Aatomienergiaühenduse ajalooarhiivide üldsusele kättesaadavaks tegemist (ELT L 243, 27.9.2003, lk 1).

2. Kogu CONFIDENTIEL UE/EU CONFIDENTIAL ja sellest kõrgemal tasemel salastatud teave või materjal registreeritakse selleks määratud registrites, kui struktuuriüksus selle saab või välja saadab.

3. Kui ELi salastatud teavet töödeldakse või säilitatakse side- ja infosüsteemi abil, võib registreerimiseks kasutada side- ja infosüsteemis sisalduvaid protsesse.

4. Üksikasjalikumad sätted ELi salastatud teabe julgeolekukaalutlustel registreerimise kohta nähakse ette rakenduseeskirjades.

Artikkel 30

ELi salastatud dokumentide kopeerimine ja tõlkimine

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

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

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

Artikkel 31

ELi salastatud teabe vedu

1. ELi salastatud teabe veol tuleb seda kaitsta loata avalikustamise eest.

2. ELi salastatud teabe veo suhtes kohaldatakse kaitsemeetmeid, mis:

— on vastavuses veetava ELi salastatud teabe salastatuse tasemega ning

— on kohandatud konkreetsetele veotingimustele sõltuvalt eelkõige sellest, kas ELi salastatud teavet veetakse:

  — komisjoni hoones või hoonetekompleksis;

  — ühes ja samas liikmesriigis paiknevate komisjoni hoonete piires;

  — liidu piires;

  — liidust kolmanda riigi territooriumile, ning

  — on kohandatud vastavalt ELi salastatud teabe iseloomule ja vormile.

3. Nimetatud kaitsemeetmed sätestatakse üksikasjalikult rakenduseeskirjades, või juhul kui tegemist on artiklis 42 osutatud projektide ja programmidega, programmi või projekti julgeolekujuhiste lahutamatu osana.

4. Rakenduseeskirjad või programmi või projekti julgeolekujuhised peavad sisaldama sätteid, mis on vastavuses ELi salastatud teabe salastatuse tasemega ja käsitlevad alljärgnevat:

— veo liik, nt käsipost, sõjaline või diplomaatiline kullerteenus, postiteenus või kommertskullerteenus;

— ELi salastatud teabe pakendamine;

— tehnilised vastumeetmed ELi salastatud teabe veoks elektroonilisel andmekandjal;

— mis tahes muud menetluslikud, füüsilised või elektroonilised meetmed;

— registreerimismenetlused;

— julgeolekukontrolli läbinud töötajate kasutamine.

5. Kui ELi salastatud teavet veetakse elektroonilisel andmekandjal, ja olenemata artikli 21 lõikest 5, võib asjaomastes rakenduseeskirjades esitatud kaitsemeetmeid täiendada asjakohaste tehniliste vastumeetmetega, mille on heaks kiitnud komisjoni julgeolekuasutus, et minimeerida teabe ohtu sattumise või kadumise riski.

Artikkel 32

ELi salastatud teabe hävitamine

1. ELi salastatud dokumendid, mida ei ole enam vaja, võib hävitada, võttes arvesse arhiveerimisega seotud õigusnorme ning komisjoni õigusnorme dokumentide haldamise ja arhiveerimise kohta, eelkõige ühtset komisjoniülest säilitustähtaegade loetelu.

2. CONFIDENTIEL UE/EU CONFIDENTIAL ja kõrgemal tasemel salastatud teabe hävitab vastutava ELi salastatud teabe registri kontrolliametnik dokumendi valdaja või pädeva asutuse ülesandel. Registri kontrolliametnik ajakohastab vastavalt registreerimisraamatuid ja muud registreerimisteavet.

3. SECRET UE/EU SECRET või TRÈS SECRET UE/EU TOP SECRET tasemel salastatud dokumendid hävitab registri kontrolliametnik ning hävitamise juures viibib tunnistaja, kes on läbinud vähemalt hävitatava dokumendi salastatuse tasemele vastava julgeolekukontrolli.

4. Registri kontrolliametnik ja tunnistaja, kui viimase kohalolek on nõutav, kirjutavad alla dokumendi hävitamise aktile, mida säilitatakse registris. ELi salastatud teabe registri vastutav kontrolliametnik säilitab TRÈS SECRET UE/EU TOP SECRET tasemel salastatud dokumentide hävitamise akte vähemalt kümme aastat ja CONFIDENTIEL UE/EU CONFIDENTIAL ning SECRET UE/EU SECRET tasemel salastatud dokumentide hävitamise akte vähemalt viis aastat.

5. Salastatud, sealhulgas RESTREINT UE/EU RESTRICTED tasemel salastatud dokumendid hävitatakse viisil, mis on sätestatud rakenduseeskirjades ning vastab asjakohastele ELi või samaväärsetele standarditele.

6. ELi salastatud teabe salvestamiseks kasutatud elektroonilised salvestusvahendid hävitatakse vastavalt rakenduseeskirjades sätestatud menetlustele.

Artikkel 33

ELi salastatud teabe hävitamine hädaolukorras

1. ELi salastatud teavet valdavad komisjoni talitused koostavad kohalikel tingimustel põhinevaid plaane Euroopa Liidu salastatud materjali kaitsmiseks kriisiolukorras, sealhulgas vajaduse korral hädaolukorras hävitamise ja evakueerimise plaanid. Nad teevad teatavaks juhised, mida peetakse vajalikuks, et välistada ELi salastatud teabe sattumine volitamata isikute kätte.

2. CONFIDENTIEL UE/EU CONFIDENTIAL ja SECRET UE/EU SECRET tasemel salastatud materjali kaitsmiseks ja/või hävitamiseks kriisiolukorras võetavad meetmed ei tohi mingil juhul kahjustada TRES SECRET UE/EU TOP SECRET tasemel salastatud materjali, sealhulgas šifreerimisvahendite kaitsmist või hävitamist, mis on olulisemad kui kõik muud ülesanded.

3. Hädaolukorras, kus esineb otsene ELi salastatud teabe 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.

4. Üksikasjalikumad sätted ELi salastatud teabe hävitamise kohta nähakse ette rakenduseeskirjades.

5. PEATÜKK

ELI SALASTATUD TEABE KAITSE SIDE- JA INFOSÜSTEEMIDES

Artikkel 34

Infokindluse aluspõhimõtted

1. Infokindlus side- ja infosüsteemide valdkonnas tähendab kindlust, et sellised süsteemid kaitsevad neis töödeldavat teavet ning toimivad ettenähtud korras, ettenähtud ajal ja õiguspäraste kasutajate juhtimisel.

2. Tõhus infokindlus tagab asjakohasel tasemel:

autentsuse: tagatis, et teave on ehtne ja pärineb heausksest allikast;

käideldavuse: teave on volitatud isiku taotluse korral kättesaadav ja kasutatav;

konfidentsiaalsuse: teavet ei avalikustata volitamata isikutele, üksustele või töötlemiseks;

tervikluse: vara ja teabe täpsuse ja terviklikkuse kaitse;

salgamise vääramise: võime tõestada tegevuse või sündmuse toimumist selliselt, et kõnealuse sündmuse või tegevuse toimumist ei saa hiljem eitada.

3. Infokindluse aluseks on riskijuhtimisprotsess.

Artikkel 35

Mõisted

Käesolevas peatükis kasutatakse järgmisi mõisteid:

a) „akrediteerimine" – turvalisuse akrediteerimise asutuse poolt side- ja infosüsteemile antav ametlik luba ja heakskiit töödelda ELi salastatud teavet süsteemi töökeskkonnas pärast julgeolekukava ametlikku kinnitamist ja nõuetekohast rakendamist;

b) „akrediteerimisprotsess" – ülesanded, mis tuleb täita enne akrediteerimist turvalisuse akrediteerimise asutuse poolt. Need ülesanded esitatakse akrediteerimisprotsessi standardis;

c) „side- ja infosüsteem" – süsteem, mis võimaldab elektroonilises vormis oleva teabe töötlemist. Side- ja infosüsteem hõlmab kõiki selle toimimiseks vajalikke vahendeid, sealhulgas infrastruktuuri, töökorralduse, töötajate ja teabega seotud ressursse;

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

e) „risk" – võimalus, et teatav 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;

f) „riski aktsepteerimine" – otsus leppida jääkriski edasise olemasoluga pärast riski käsitlemist;

g) „riski hindamine" – ohtude ja haavatavuse kindlakstegemine ning sellega seotud riskianalüüsi, st riski tõenäosuse ja mõju analüüsi koostamine;

h) „riskiteavitus" – side- ja infosüsteemide kasutajaskonna riskiteadlikkuse suurendamine, heakskiitvate asutuste teavitamine sellistest riskidest ja riske käsitlev aruandlus töötlejatele;

i) „riski käsitlemine" – riski leevendamine, kõrvaldamine, vähendamine (tehniliste, füüsiliste, korralduslike või menetluslike meetmete asjakohase kombineerimise abil), riski ülekandmine või seire.

Artikkel 36

ELi salastatud teabe töötlemine side- ja infosüsteemides

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

2. ELi salastatud teabe töötlemisel side- ja infosüsteemides vastavalt komisjoni infosüsteemide julgeolekupoliitikale, millele on osutatud komisjoni otsuses K(2006) 3602, ([1]) viitab sellele, et:

a) infosüsteemide julgeolekupoliitika rakendamiseks infosüsteemi kogu kasutusaja vältel kohaldatakse mudelit „planeeri-teosta-kontrolli-tegutse";

b) julgeolekuvajadused tuleb kindlaks teha ettevõtlusele avalduva mõju hindamise kaudu;

c) infosüsteemi ja selles sisalduvate andmete kohta tuleb koostada vara ametlik liigitus;

([1]) Otsus K(2006) 3602, 16. august 2006, milles käsitletakse Euroopa Komisjoni kasutatavate infosüsteemide turvalisust.

d) kõik infosüsteemide turvalisuse poliitikas kindlaksmääratud kohustuslikud julgeolekumeetmed peavad olema rakendatud;

e) kohaldada tuleb riskijuhtimisprotsessi, mis koosneb järgmistest etappidest: ohtude ja haavatavuse kindlakstegemine, riskihindamine, riskide käsitlemine, riski aktsepteerimine ja riskidest teatamine;

f) koostatakse julgeolekukava, sealhulgas julgeolekupoliitika ja turvanõuete rakendamise kord, rakendatakse ja kontrollitakse seda ja vaadatakse see läbi.

3. Kõik töötajad, kes osalevad ELi salastatud teavet töötleva side- ja infosüsteemi loomisel, arendamisel, katsetamisel, rakendamisel, haldamisel või kasutamisel, teavitavad turvalisuse akrediteerimise asutust kõigist võimalikest teabe turvalisusega seotud puudujääkidest, intsidentidest, rikkumistest või teabe ohtu sattumisest, mis võivad mõjutada side- ja infosüsteemi ja/või selles sisalduva ELi salastatud teabe kaitset.

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

a) eelistatud on tooted, mille on heaks kiitnud nõukogu või selle peasekretär nõukogu krüptovahendite heakskiitmise asutuse ülesannetes ning komisjoni julgeolekualase eksperdirühma soovitusel;

b) kui see on õigustatud konkreetsetel operatiivsetel põhjustel, võib komisjoni krüptovahendite heakskiitmise asutus loobuda komisjoni julgeolekualase eksperdirühma soovitusel punktis a sätestatud nõuetest ja anda konkreetseks tähtajaks ajutise heakskiidu.

5. ELi salastatud teabe elektroonilise edastamise, töötlemise ja säilitamise ajal kasutatakse heakskiidetud krüptovahendeid. Olenemata nimetatud nõudest võib erakorraliste asjaolude või spetsiifiliste tehniliste tingimuste korral pärast komisjoni krüptovahendite heakskiitmise asutuselt heakskiidu saamist kohaldada erimenetlusi.

6. Rakendatakse turvameetmeid, et kaitsta CONFIDENTIEL UE/EU CONFIDENTIAL või 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.

7. Komisjoni julgeolekuasutus seab sisse järgmised asutused:

— infokindluse asutus;

— turvalisuse akrediteerimise asutus;

— TEMPEST-asutus;

— krüptovahendite heakskiitmise asutus;

— krüptomaterjalide jaotamise asutus.

8. Komisjoni julgeolekuasutus määrab igale süsteemile infokindluse rakendusasutuse.

9. Lõigetes 7 ja 8 nimetatud asutuste ülesanded sätestatakse rakenduseeskirjades.

Artikkel 37

ELi salastatud teavet töötlevate side- ja infosüsteemide akrediteerimine

1. Kõik ELi salastatud teavet töötlevad side- ja infosüsteemid läbivad akrediteerimisprotsessi, mis tugineb infokindluse põhimõtetele ja mille üksikasjalikkus peab olema vastavuses nõutud kaitsetasemega.

2. Akrediteerimisprotsess peab sisaldama komisjoni turvalisuse akrediteerimise asutuselt saadud ametlikku kinnitust side- ja infosüsteemi julgeolekukavale, tagamaks, et:

a) artikli 36 lõikes 2 osutatud riskijuhtimisprotsessi on rakendatud nõuetekohaselt;

b) süsteemi omanik on teadlikult aktsepteerinud jääkriski; ning

c) kooskõlas käesoleva otsusega on saavutatud side- ja infosüsteemi ning selles töödeldava ELi salastatud teabe piisav kaitsetase.

3. Komisjoni turvalisuse akrediteerimise asutus väljastab akrediteerimisteatise, milles määratakse kindlaks ELi salastatud teabe maksimaalne salastatuse tase, mida side- ja infosüsteem võib töödelda, ning vastavad töötingimused. See ei piira nende ülesannete täitmist, mis on usaldatud Euroopa Parlamendi ja nõukogu määruse (EL) nr 512/2014 ([1]) artiklis 11 määratletud turvalisuse akrediteerimise ametile.

4. Ühine turvalisuse akrediteerimise amet vastutab komisjoni mitut osapoolt hõlmava side- ja infosüsteemi akrediteerimise eest. Amet moodustatakse kõigi osapoolte turvalisuse akrediteerimise asutuste esindajatest ja selle eesistuja on komisjoni turvalisuse akrediteerimise asutuse esindaja.

5. Akrediteerimisprotsess koosneb teatavatest osapoolte täidetavatest ülesannetest. Akrediteerimist käsitlevate toimikute ja dokumentide ettevalmistamise eest vastutab täielikult side- ja infosüsteemi omanik.

6. Akrediteerimise eest vastutab komisjoni turvalisuse akrediteerimise asutus, kellel on side- ja infosüsteemi kasutusaja mis tahes hetkel õigus:

a) nõuda akrediteerimisprotsessi rakendamist;

b) auditeerida või kontrollida side- ja infosüsteemi;

c) juhul kui töötingimused ei ole enam täidetud, nõuda julgeoleku tõhustamise kava koostamist ja tulemuslikku elluviimist kindlaksmääratud aja jooksul, tühistades vajaduse korral side- ja infosüsteemiga töötamise loa, kuni töötingimused on taas täidetud.

7. Akrediteerimisprotsess määratakse kindlaks ELi salastatud teavet töötleva side- ja infosüsteemi akrediteerimisprotsessi standardis, mis võetakse vastu kooskõlas otsuse K(2006) 3602 artikli 10 lõikega 3.

Artikkel 38

Erakorralised asjaolud

1. Olenemata käesoleva peatüki sätetest võib erakorraliste asjaolude, nagu ähvardava või reaalse kriisi, konflikti, sõjaolukorra või operatiivsete erakorraliste asjaolude korral rakendada allpool kirjeldatud konkreetseid menetlusi.

2. ELi salastatud teavet võib pädeva asutuse nõusolekul edastada, kasutades madalama salastatuse taseme jaoks heakskiidetud krüptovahendeid või krüpteerimata kujul, 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 nõutavat krüptoseadet ning

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

3. Punktis 1 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 viivitamata muude vahendite abil.

4. Pädevale asutusele ja komisjoni julgeolekualasele eksperdirühmale esitatakse sellekohane aruanne.

6. PEATÜKK

TÖÖSTUSJULGEOLEK

Artikkel 39

Aluspõhimõtted

1. Tööstusjulgeolek tähendab meetmete kohaldamist selleks, et tagada ELi salastatud teabe kaitsmine

a) salastatud lepingute raames järgmiselt:

   i) kandidaatide ja pakkujate poolt kogu pakkumismenetluse ja lepingu sõlmimise menetluse vältel;

   ii) lepinglaste ja all-lepinglaste poolt kogu salastatud lepingute kehtivusaja vältel;

([1]) Euroopa Parlamendi ja nõukogu määrus (EL) nr 512/2014, 16. aprill 2014, millega muudetakse määrust (EL) nr 912/2010, millega luuakse Euroopa GNSSi Agentuur (ELT L 150, 20.5.2014, lk 72).

b) salastatud toetuslepingute raames järgmiselt:

i) taotlejate poolt toetuse eraldamismenetluse vältel;

ii) toetusesaajate poolt kogu salastatud toetuslepingute kehtivusaja vältel.

2. Sellised lepingud või toetuslepingud ei käsitle TRÈS SECRET UE/EU TOP SECRET tasemel salastatud teavet.

3. Kui ei ole sätestatud teisiti, kohaldatakse salastatud lepingutele või lepinglastele osutavaid käesoleva peatüki sätteid ka salastatud all-lepingute ja all-lepinglaste suhtes.

Artikkel 40

Mõisted

Käesolevas peatükis kasutatakse järgmisi mõisteid:

a) „salastatud leping" – nõukogu määruse (EÜ, Euratom) nr 1605/2002 ([1]) kohane raamleping või leping, mille komisjon või selle talitus on sõlminud lepinglasega vallas- või kinnisvara tarnimise, tööde tegemise või teenuste osutamise eesmärgil ning mille täitmise eelduseks on või mille täitmisega kaasneb ELi salastatud teabe loomine, töötlemine või säilitamine;

b) „salastatud all-leping" – leping, mille komisjoni või selle talituse lepinglane on sõlminud teise lepinglasega (st all-lepinglasega) vallas- või kinnisvara tarnimise, tööde tegemise või teenuste osutamise eesmärgil ning mille täitmise eelduseks on või mille täitmisega kaasneb ELi salastatud teabe loomine, töötlemine või säilitamine;

c) „salastatud toetusleping" – kokkulepe, mille alusel komisjon eraldab toetuse määruse (EÜ, Euratom) nr 1605/2002 I osa VI jaotise kohaselt ning mille täitmise eelduseks on või mille täitmisega kaasneb ELi salastatud teabe loomine, töötlemine või säilitamine;

d) „määratud julgeolekuasutus" – asutus, kes vastutab liikmesriigi julgeolekuasutuse ees tööstus- või muudele üksustele riigi kõigi tööstusjulgeolekuga seotud poliitikaküsimuste edastamise eest ning kõnealuse poliitika rakendamisel suuniste ja abi andmise eest. Määratud julgeolekuasutuse ülesandeid võib täita riiklik julgeolekuasutus või muu pädev asutus.

Artikkel 41

Salastatud lepingute või toetuslepingute menetlus

1. Iga komisjoni talitus kui lepingu sõlmija tagab, et salastatud lepingute või toetuslepingute sõlmimisel järgitakse käesolevas peatükis sätestatud ja lepingus osutatud või sisalduvaid tööstusjulgeoleku miinimumstandardeid.

2. Lõike 1 kohaldamisel küsivad komisjoni pädevad talitused nõu personali- ja turvalisusküsimuste peadirektoraadilt, eriti selle julgeolekudirektoraadilt, ning kohustuvad tagama, et lepingute, all-lepingute ja toetuslepingute näidisvormid sisaldavad ELi salastatud teabe kaitse aluspõhimõtteid ja miinimumstandardeid käsitlevaid sätteid, mida lepinglased, all-lepinglased ja toetuslepingutega hõlmatud toetusesaajad peavad täitma.

3. Komisjon teeb tihedat koostööd asjaomase liikmesriigi riikliku või määratud julgeolekuasutuse või muu pädeva asutusega.

4. Kui lepingu sõlmija kavatseb algatada menetluse salastatud lepingu või toetuslepingu sõlmimiseks, pöördub ta menetluse salastatud iseloomu ja menetluse osadega seotud küsimustes komisjoni julgeolekuasutuse poole kõigis menetluse etappides.

5. Salastatud lepingute, all-lepingute, toetuslepingute ja lepinguteadete vormid ja näidised, juhised töötlemisluba eeldavate olukordade tarbeks, programmi või projekti julgeolekujuhised, julgeolekuaspekte käsitlevad dokumendid, külastused ning salastatud lepingute või salastatud toetuslepingute kohane ELi salastatud teabe edastamine ja vedu sätestatakse tööstusjulgeoleku rakenduseeskirjades pärast konsulteerimist komisjoni julgeolekualase eksperdirühmaga.

([1]) Nõukogu määrus (EÜ, Euratom) nr 1605/2002, 25. juuni 2002, mis käsitleb Euroopa ühenduste üldeelarve suhtes kohaldatavat finantsmäärust (EÜT L 248, 16.9.2002, lk 1).

6. Komisjon võib sõlmida salastatud lepinguid või toetuslepinguid, et usaldada ülesandeid, millega kaasneb juurdepääs ELi salastatud teabele või sellise teabe töötlemine või säilitamine, ettevõtjatele, kes on registreeritud liikmesriigis või kolmandas riigis, kellega on sõlmitud leping või halduskokkulepe vastavalt käesoleva otsuse 7. peatükile.

Artikkel 42

Salastatud lepingu või toetuslepingu turvaelemendid

1. Salastatud lepingud või toetuslepingud peavad sisaldama järgmisi turvaelemente:

Programmi või projekti julgeolekujuhised

a) „Programmi või projekti julgeolekujuhised" – loetelu julgeolekumenetlustest, mida kohaldatakse konkreetse programmi või projekti suhtes julgeolekumenetluste standardimiseks. Seda võib programmi või projekti kestel muuta.

b) Personali- ja turvalisusküsimuste peadirektoraat koostab üldised programmi või projekti julgeolekujuhised; ELi salastatud teabe töötlemise või säilitamisega seotud programmide või projektide eest vastutavad komisjoni talitused võivad vajaduse korral koostada spetsiifilisi programmi või projekti julgeolekujuhiseid, mis põhinevad üldistel programmi või projekti julgeolekujuhistel.

c) Spetsiifiline programmi või projekti julgeolekujuhised koostatakse eelkõige selliste programmide ja projektide tarbeks, mida iseloomustab märkimisväärne maht, ulatus või keerukus või lepinglaste, toetusesaajate ning muude partnerite ja sidusrühmade arvukus ja/või mitmekesisus, näiteks nende õigusliku seisundi poolest. Spetsiifilise programmi või projekti julgeolekujuhised koostab programmi või projekti haldav komisjoni talitus või talitused, kes teeb tihedat koostööd personali- ja turvalisusküsimuste peadirektoraadiga.

d) Personali- ja turvalisusküsimuste peadirektoraat esitab nii üldised kui ka spetsiifilised programmi või projekti julgeolekujuhised nõuannete saamiseks komisjoni julgeolekualasele eksperdirühmale.

Julgeolekuaspekte käsitlev dokument

a) „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.

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

c) Julgeolekuaspekte käsitlev dokument sisaldab sätteid, milles nõutakse, et lepinglane või toetusesaaja järgiks käesolevas otsuses sätestatud miinimumstandardeid. Lepingu sõlmija kohustub tagama, et julgeolekuaspekte käsitlevas dokumendis on sätestatud, et nimetatud miinimumstandardite mittejärgimine võib olla piisav alus lepingu või toetuslepingu lõpetamiseks.

2. Nii programmi või projekti julgeolekujuhised kui ka julgeolekuaspekte käsitlevad dokumendid sisaldavad kohustusliku turvaelemendina salastatuse taseme määramise juhendit:

a) „salastatuse taseme määramise juhend" – dokument, milles kirjeldatakse programmi, projekti, lepingu või toetuslepingu salastatud osasid, määrates kindlaks neile kohaldatavad salastatuse tasemed. Salastatuse taseme määramise juhendit võib kogu programmi, projekti, lepingu või toetuslepingu kehtivuse aja jooksul täiendada ja nende teabeelementide salastatuse taset võib muuta või alandada; kui salastatuse taseme määramise juhend on olemas, on see julgeolekuaspekte käsitleva dokumendi osa.

b) Enne salastatud lepingu sõlmimist või sellise lepingu sõlmimise pakkumismenetluse algatamist määrab komisjoni talitus kui lepingu sõlmija kindlaks kandidaatidele ja pakkujatele või lepinglastele edastatava teabe salastatuse taseme ning samuti lepinglaste poolt koostatava teabe salastatuse taseme. Selleks koostab ta pärast komisjoni julgeolekuasutusega konsulteerimist lepingu täitmiseks kasutatava salastatuse taseme määramise juhendi kooskõlas käesoleva otsuse ja selle rakenduseeskirjadega.

c) Salastatud lepingu eri osade salastatuse taseme määramisel kohaldatakse järgmisi põhimõtteid:

i) salastatuse taseme määramise juhendi koostamisel võtab komisjoni talitus kui lepingu sõlmija arvesse kõiki asjaomaseid julgeolekuaspekte, sealhulgas salastatuse taset, mille teabe koostaja on määranud lepingus kasutatavale ja heakskiidetud teabele;

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

iii) lepingu täitmise käigus lepinglaste koostatud või neile esitatud teabe salastatuse taseme muutumise korral ning kui salastatuse taseme määramise juhendit edaspidi muudetakse, võtab lepingu sõlmija vajaduse korral komisjoni julgeolekuasutuse kaudu ühendust liikmesriikide riikliku või määratud julgeolekuasutuse või muu asjaomase pädeva julgeolekuasutusega.

Artikkel 43

Lepinglaste ja toetusesaajate personali juurdepääs ELi salastatud teabele

Lepingu või toetuslepingu sõlmija tagab, et salastatud leping või salastatud toetusleping sisaldab sätteid selle kohta, et lepinglase, all-lepinglase või toetusesaaja personal, kes vajab salastatud lepingu, all-lepingu või toetuslepingu täitmiseks juurdepääsu ELi salastatud teabele, saab sellise juurdepääsu üksnes juhul, kui:

a) nad on läbinud vastava taseme julgeolekukontrolli või on muul viisil nõuetekohaselt volitatud ja nende teadmisvajadus on kindlaks tehtud;

b) neid on teavitatud ELi salastatud teabe kaitseks vajalikest kehtivatest julgeolekunormidest ning nad on kinnitanud oma vastutust seoses kõnealuse teabe kaitsmisega;

c) nad on läbinud vastava riikliku või määratud julgeolekuasutuse või muu pädeva asutuse julgeolekukontrolli juurdepääsuks CONFIDENTIEL UE/EU CONFIDENTIAL või SECRET UE/EU SECRET tasemel salastatud teabele.

Artikkel 44

Töötlemisluba

1. „Töötlemisluba" – riikliku julgeolekuasutuse, määratud julgeolekuasutuse või muu pädeva julgeolekuasutuse haldusotsus selle kohta, et lähtudes julgeoleku seisukohast, võib ettevõtja pakkuda piisaval tasemel kaitset teataval salastatuse tasemel ELi salastatud teabele.

2. Liikmesriigi riikliku või määratud julgeolekuasutuse või muu pädeva julgeolekuasutuse väljastatud töötlemisluba, millel peab kooskõlas siseriiklike õigusnormidega olema kirjas, et ettevõtja suudab oma valdustes kaitsta asjaomasel salastatuse tasemel (CONFIDENTIEL UE/EU CONFIDENTIAL või SECRET UE/EU SECRET) ELi salastatud teavet, esitatakse komisjoni julgeolekuasutusele, kes edastab selle lepingu või toetuslepingu sõlmijana tegutsevale komisjoni talitusele, enne kui kandidaadile, pakkujale, lepinglasele või toetuse taotlejale või saajale tohib edastada ELi salastatud teavet või võimaldada sellele juurdepääsu.

3. Kui see on asjakohane, teavitab lepingu sõlmija komisjoni julgeolekuasutuse kaudu asjakohast riiklikku või määratud julgeolekuasutust või muud pädevat julgeolekuasutust sellest, et lepingu täitmiseks on vaja töötlemisluba. Töötlemis- või juurdepääsuluba on nõutav, kui hanke- või toetusmenetluse käigus on vaja väljastada CONFIDENTIEL UE/EU CONFIDENTIAL või SECRET UE/EU SECRET tasemel ELi salastatud teavet.

4. Kui nõutakse töötlemisluba, ei sõlmi lepingu või toetuslepingu sõlmija eelistatud pakkuja või osalejaga salastatud lepingut või toetuslepingut enne, kui ta on saanud selle liikmesriigi riiklikult või määratud julgeolekuasutuselt või muult pädevalt julgeolekuasutuselt, kus on asjaomase lepinglase või all-lepinglase asukoht, kinnituse selle kohta, et on väljastatud asjakohane töötlemisluba.

5. Kui töötlemisloa väljastanud riiklik või määratud julgeolekuasutus või muu pädev julgeolekuasutus on teavitanud komisjoni julgeolekuasutust töötlemisluba mõjutavatest muudatustest, teatab komisjoni julgeolekuasutus sellest lepingu või toetuslepingu sõlmijana tegutsevale komisjoni talitusele. All-lepingust teavitatakse riiklikku või määratud julgeolekuasutust või muud pädevat julgeolekuasutust.

6. Töötlemisloa tühistamine asjaomase riikliku või määratud julgeolekuasutuse või muu pädeva julgeolekuasutuse poolt on lepingu või toetuslepingu sõlmijale piisav alus salastatud lepingu lõpetamiseks või kandidaadi, pakkuja või taotleja hankekonkursilt kõrvaldamiseks. Sellekohane säte lisatakse koostatavatesse näidislepingutesse ja näidistoetuslepingutesse.

Artikkel 45

Salastatud lepinguid ja toetuslepinguid käsitlevad sätted

1. Kandidaadile, pakkujale või taotlejale hankemenetluse käigus ELi salastatud teabe edastamise korral sisaldab pakkumiskutse või konkursikutse sätet, millega kohustatakse kandidaati, pakkujat või taotlejat, kes pakkumist või projekti ei esita või kes ei osutu väljavalituks, tagastama kindlaksmääratud tähtaja jooksul kõik salastatud dokumendid.

2. Lepingu või toetuslepingu sõlmija teavitab komisjoni julgeolekuasutuse kaudu pädevat riiklikku või määratud julgeolekuasutust või muud pädevat julgeolekuasutust salastatud lepingu või toetuslepingu sõlmimisest ja sellega seotud andmetest, nagu lepinglas(t)e või toetusesaajate nimed, lepingu kehtivusaeg ja maksimaalne salastatuse tase.

3. Sellise lepingu või toetuslepingu lõpetamisel teavitab lepingu või toetuslepingu sõlmija komisjoni julgeolekuasutuse kaudu viivitamata selle liikmesriigi riiklikku või määratud julgeolekuasutust või muud pädevat julgeolekuasutust, kus lepinglane või toetusesaaja on registreeritud.

4. Üldiselt nõutakse, et lepinglane või toetusesaaja tagastab salastatud lepingu või toetuslepingu lõpetamisel või toetusesaaja osalemise katkestamisel tema valduses oleva ELi salastatud teabe lepingu või toetuslepingu sõlmijale.

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

6. Kui lepinglasel või toetusesaajal lubatakse ELi salastatud teavet säilitada pärast salastatud lepingu või toetuslepingu lõppemist, järgib kõnealune lepinglane või toetusesaaja jätkuvalt käesolevas otsuses sisalduvaid miinimumstandardeid ning kaitseb ELi salastatud teabe konfidentsiaalsust.

Artikkel 46

Salastatud lepinguid käsitlevad erisätted

1. ELi salastatud teabe kaitse tingimused, mille alusel lepinglane võib sõlmida all-lepinguid, määratakse kindlaks pakkumiskutses ja salastatud lepingus.

2. Lepinglane peab enne salastatud lepingu mis tahes osa täitmiseks all-lepingu sõlmimist saama selleks lepingu sõlmijalt loa. Kolmandas riigis registreeritud all-lepinglastega ei sõlmita all-lepinguid, millega kaasneb juurdepääs ELi salastatud teabele, kui puudub 7. peatükis sätestatud salastatud teabe kaitse õigusraamistik.

3. Lepinglane vastutab selle tagamise eest, et all-lepinguga seotud mis tahes tegevus oleks kooskõlas käesolevas otsuses sätestatud miinimumstandarditega, ning ei anna ELi salastatud teavet all-lepinglasele ilma lepingu sõlmija eelneva kirjaliku nõusolekuta.

4. Lepinglase või all-lepinglase koostatud või töödeldava ELi salastatud teabe korral on teabe koostajaks komisjon, kelle õigusi teostab lepingu sõlmija.

Artikkel 47

Salastatud lepingutega seotud külastused

1. Kui komisjoni töötajatel või lepinglase või toetusesaaja töötajatel on salastatud lepingu või toetuslepingu täitmiseks vaja üksteise objektidel juurdepääsu CONFIDENTIEL UE/EU CONFIDENTIAL või SECRET UE/EU SECRET tasemel salastatud teabele, tuleb külastusi korraldada koostöös riiklike või määratud julgeolekuasutuste või muude asjaomaste pädevate julgeolekuasutusega. Komisjoni julgeolekuasutusele antakse sellistest külastustest teada. Riiklikud või määratud julgeolekuasutused või muud pädevad julgeolekuasutused võivad siiski seoses konkreetsete programmide või projektidega kokku leppida korra, millealusel võib selliseid külastusi korraldada otse.

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

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

4. Üksikasjalikumad sätted nähakse ette rakenduseeskirjades.

5. Käesolevas otsuses ja lõikes 4 osutatud rakenduseeskirjades ette nähtud ning salastatud lepingutega seotud külastusi käsitlevate sätete järgimine on kohustuslik.

Artikkel 48

ELi salastatud teabe edastamine ja vedu seoses salastatud lepingute või salastatud toetuslepingutega

1. ELi salastatud teabe elektroonilise edastamise suhtes kohaldatakse käesoleva otsuse 5. peatüki asjakohaseid sätteid.

2. ELi salastatud teabe veo suhtes kohaldatakse käesoleva otsuse 4. peatüki ja rakenduseeskirjade sätteid kooskõlas siseriiklike õigusnormidega.

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

a) julgeolek kindlustatakse lähtekohast lõppsihtkohta vedamise kõigil etappidel;

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

c) enne CONFIDENTIEL UE/EU CONFIDENTIAL või SECRET UE/EU SECRET tasemel salastatud materjali piiriülest vedu koostab saatja veoplaani, mille kiidab heaks asjaomane riiklik või määratud julgeolekuasutus või muu asjaomane pädev julgeolekuasutus;

d) veod toimuvad võimalikult täpselt punktist punkti ja need lõpetatakse nii kiiresti, kui asjaolud seda võimaldavad;

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

Artikkel 49

ELi salastatud teabe edastamine kolmandates riikides paiknevatele lepinglastele või toetusesaajatele

ELi salastatud teave edastatakse kolmandates riikides paiknevatele lepinglastele ja toetusesaajatele vastavalt turvameetmetele, mis on kokku lepitud komisjoni julgeolekuasutuse või komisjoni talituse kui lepingu või toetuslepingu sõlmija ning selle asjaomase kolmanda riigi riikliku või määratud julgeolekuasutuse vahel, kus lepinglane või toetusesaaja on registreeritud.

Artikkel 50

RESTREINT UE/EU RESTRICTED tasemel salastatud teabe töötlemine salastatud lepingute või salastatud toetuslepingute kontekstis

1. RESTREINT UE/EU RESTRICTED tasemel salastatud ning salastatud lepingute või salastatud toetuslepingute kontekstis töödeldava või säilitatava teabe kaitse põhineb proportsionaalsuse ja kulutasuvuse põhimõtetel.

2. RESTREINT UE/EU RESTRICTED tasemel salastatud teabe töötlemist hõlmavate salastatud lepingute või salastatud toetuslepingute kontekstis ei ole nõutav töötlemisluba ega juurdepääsuluba.

3. Kui leping või toetusleping hõlmab RESTREINT UE/EU RESTRICTED tasemel salastatud teabe töötlemist lepinglase või toetusesaaja side- ja infosüsteemis, tagab lepingu või toetuslepingu sõlmija pärast konsulteerimist komisjoni julgeolekuasutusega, et lepingus või toetuslepingus täpsustatakse side- ja infosüsteemi akrediteerimiseks või heakskiitmiseks vajalikud tehnilised ja haldusnõuded, mis on vastavuses hinnatud riskiga ja milles on arvesse võetud kõiki olulisi tegureid. Sellise side- ja infosüsteemi akrediteerimise või heakskiitmise ulatus lepitakse kokku komisjoni julgeolekuasutuse ja asjaomase riikliku või määratud julgeolekuasutuse vahel.

7. PEATÜKK

SALASTATUD TEABE VAHETAMINE TEISTE LIIDU INSTITUTSIOONIDE, ASUTUSTE JA ORGANITEGA, LIIKMESRIIKIDEGA, KOLMANDATE RIIKIDEGA NING RAHVUSVAHELISTE ORGANISATSIOONIDEGA

Artikkel 51

Aluspõhimõtted

1. Kui komisjon või üks selle talitustest otsustab, et on olemas vajadus vahetada ELi salastatud teavet teise liidu institutsiooni, asutuse või organiga või kolmanda riigi või rahvusvahelise organisatsiooniga, astutakse vajalikud sammud, et luua sellekohane õigus- või haldusraamistik, mis võib sisaldada kooskõlas asjaomaste õigusnormidega sõlmitud salastatud teabe kaitse lepinguid või halduskokkuleppeid.

2. Ilma et see piiraks artikli 57 sätteid, vahetatakse ELi salastatud teavet teise liidu institutsiooni, asutuse või organiga või kolmanda riigi või rahvusvahelise organisatsiooniga üksnes sellise nõuetekohase õigus- või haldusraamistiku olemasolul ja tingimusel, et suudetakse pakkuda piisavaid tagatisi, et asjaomane liidu institutsioon, asutus või organ või kolmas riik või rahvusvaheline organisatsioon rakendab salastatud teabe kaitseks samaväärseid aluspõhimõtteid ja miinimumstandardeid.

Artikkel 52

ELi salastatud teabe vahetamine teiste liidu institutsioonide, asutuste ja organitega

1. Enne halduskokkuleppe sõlmimist teise liidu institutsiooni, asutuse või organiga taotleb komisjon kinnitust, et asjaomane liidu institutsioon, asutus või organ:

a) on kehtestanud ELi salastatud teabe kaitseks õigusraamistiku, milles sätestatud aluspõhimõtted ja miinimumstandardid on samaväärsed käesolevas otsuses ja selle rakenduseeskirjades sisalduvatega;

b) kohaldab julgeolekustandardeid ja -suuniseid personali turvalisuse, füüsilise julgeoleku, ELi salastatud teabe haldamise ning side- ja infosüsteemide turvalisuse kohta, et tagada komisjoniga samaväärne ELi salastatud teabe kaitstuse tase;

c) tähistab enda koostatud salastatud teabe sarnaselt ELi salastatud teabele.

2. Personali- ja turvalisusküsimuste peadirektoraat on tihedas koostöös komisjoni teiste pädevate talitustega komisjonis juhtiv talitus halduskokkulepete sõlmimiseks teiste liidu institutsioonide, asutuste või organitega ELi salastatud teabe vahetamise eesmärgil.

3. Halduskokkulepped saavad üldjuhul teoks kirjavahetuse kujul, millele on komisjoni nimel alla kirjutanud personali- ja turvalisusküsimuste peadirektoraadi peadirektor.

4. Enne halduskokkuleppe sõlmimist ELi salastatud teabe vahetamise kohta teeb komisjoni julgeolekuasutus hindamiskülastuse, et hinnata ELi salastatud teabe kaitseks ettenähtud õigusraamistikku ning veenduda ELi salastatud teabe kaitsmiseks võetud meetmete tulemuslikkuses. Halduskokkulepe jõustub ja ELi salastatud teavet vahetatakse üksnes juhul, kui nimetatud hindamiskülastuse tulemused on rahuldavad ning pärast külastust esitatud soovitusi on järgitud. Selleks et kontrollida, kas halduskokkulepet täidetakse ja kehtivad julgeolekumeetmed vastavad kokkulepitud aluspõhimõtetele ja miinimumstandarditele, tehakse regulaarseid järelhindamiskülastusi.

5. Komisjonis jääb teiste liidu institutsioonide, asutuste ja organitega vahetatava salastatud teabe peamiseks sisenemis- ja väljumispunktiks peasekretariaadi hallatav ELi salastatud teabe register. Kui see osutub aga turvakaalutlustel või korralduslikel või operatiivsetel põhjustel ELi salastatud teabe kaitsmisel asjakohasemaks, toimivad komisjoni asjaomaste talituste pädevusse kuuluvates küsimustes vahetatava salastatud teabe sisenemis- ja väljumispunktina käesoleva otsuse ja selle rakenduseeskirjade alusel komisjoni talitustes loodud ELi salastatud teabe kohalikud registrid.

6. Komisjoni julgeolekualast eksperdirühma teavitatakse halduskokkulepete sõlmimise protsessist lõike 2 kohaselt.

Artikkel 53

ELi salastatud teabe vahetamine liikmesriikidega

1. ELi salastatud teavet võib vahetada liikmesriikidega ja avaldada liikmesriikidele, tingimusel et nad kaitsevad seda teavet kooskõlas nõuetega, mida kohaldatakse sama taseme riigisisest salastusmärget kandva salastatud teabe suhtes vastavalt I lisas esitatud salastatuse tasemete vastavustabelile.

2. Kui liikmesriigid sisestavad Euroopa Liidu struktuuridesse või võrkudesse riigisisest salastusmärget kandva salastatud teabe, kaitseb komisjon seda teavet kooskõlas nõuetega, mida kohaldatakse samaväärse salastatuse tasemega ELi salastatud teabe suhtes vastavalt I lisas esitatud salastatuse tasemete vastavustabelile.

Artikkel 54

ELi salastatud teabe vahetamine kolmandate riikide ja rahvusvaheliste organisatsioonidega

1. Kui komisjon otsustab, et tal on pikaajaline vajadus vahetada salastatud teavet kolmandate riikide või rahvusvaheliste organisatsioonidega, astutakse vajalikud sammud, et luua sellekohane õigus- või haldusraamistik, mis võib sisaldada kooskõlas asjaomaste õigusnormidega sõlmitud salastatud teabe kaitse lepinguid või halduskokkuleppeid.

2. Lõikes 1 osutatud salastatud teabe kaitse lepingud ja 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 samaväärsed käesolevas otsuses sätestatud miinimumstandarditega.

3. Komisjon võib sõlmida artikli 56 kohaselt halduskokkuleppe, kui ELi salastatud teave ei ole üldjuhul kõrgemal salastatuse tasemel kui RESTREINT UE/EU RESTRICTED.

4. Lõikes 3 osutatud salastatud teabe vahetuseks ettenähtud 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 samaväärsed käesolevas otsuses sätestatud miinimumstandarditega. Komisjoni julgeolekualase eksperdirühmaga konsulteeritakse salastatud teabe kaitse lepingute või halduskokkulepete sõlmimisel.

5. Komisjoni talitus kui ELi salastatud teabe koostaja komisjonis teeb otsuse komisjonist 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, või allikmaterjal, mida see võib sisaldada, ei ole komisjoni koostatud, küsib seda salastatud teavet valdav komisjoni talitus avaldamiseks kõigepealt teabe koostaja kirjalikku nõusolekut. Kui teabe koostajat ei ole võimalik välja selgitada, võtab salastatud teavet valdav komisjoni talitus pärast konsulteerimist komisjoni julgeolekualase eksperdirühmaga teabe koostaja ülesanded enda kanda.

Artikkel 55

Salastatud teabe kaitse lepingud

1. Salastatud teabe kaitse lepingud kolmandate riikide või rahvusvaheliste organisatsioonidega sõlmitakse kooskõlas Euroopa Liidu toimimise lepingu artikliga 218.

2. Salastatud teabe kaitse lepingutega:

a) kehtestatakse liidu ja kolmanda riigi või rahvusvahelise organisatsiooni vahelist salastatud teabe vahetamist reguleerivad aluspõhimõtted ja miinimumstandardid;

b) nähakse ette tehniline rakenduskord, milles lepivad kokku asjaomaste liidu institutsioonide ja organite pädevate julgeolekuasutuste ning asjaomase kolmanda riigi või rahvusvahelise organisatsiooni pädev julgeolekuasutus. Sellises rakenduskorras võetakse arvesse asjaomases kolmandas riigis või rahvusvahelises organisatsioonis kehtivate julgeolekunormide, -struktuuride ja -menetlustega tagatud kaitsetaset;

c) nähakse ette, et enne lepingu kohast salastatud teabe vahetamist tuleb teha kindlaks, et teabe saaja suudab saadud teavet nõuetekohasel viisil kaitsta ja turvata.

3. Kui komisjon otsustab artikli 51 lõike 1 kohaselt, et tal on vajadus vahetada salastatud teavet, konsulteerib ta vajaduse korral Euroopa välisteenistuse, nõukogu peasekretariaadi ning teiste liidu institutsioonide ja organitega, et teha kindlaks, kas tuleks esitada soovitus Euroopa Liidu toimimise lepingu artikli 218 lõike 3 alusel.

4. ELi salastatud teavet vahetatakse elektrooniliselt vaid juhul, kui see on salastatud teabe kaitse lepingus või tehnilises rakenduskorras sõnaselgelt ette nähtud.

5. Komisjonis jääb kolmandate riikide ja rahvusvaheliste organisatsioonidega vahetatava salastatud teabe peamiseks sisenemis- ja väljumispunktiks peasekretariaadi hallatav ELi salastatud teabe register. Kui see osutub aga turvakaalutlustel või korralduslikel või operatiivsetel põhjustel ELi salastatud teabe kaitsmisel asjakohasemaks, toimivad komisjoni asjaomaste talituste pädevusse kuuluvates küsimustes vahetatava salastatud teabe sisenemis- ja väljumispunktina käesoleva otsuse ja selle rakenduseeskirjade alusel komisjoni talitustes loodud ELi salastatud teabe kohalikud registrid.

6. Selleks et hinnata asjaomase kolmandas riigi või rahvusvahelise organisatsiooni julgeolekunormide, -struktuuride ja -menetluste tõhusust, osaleb komisjon hindamiskülastustel koostöös teiste liidu institutsioonide, asutuste või organitega ning vastastikusel kokkuleppel asjaomase kolmanda riigi või rahvusvahelise organisatsiooniga hindamiskülastusi. Selliste hindamiskülastuste käigus hinnatakse järgmisi aspekte:

a) salastatud teabe kaitsmise suhtes kohaldatav õigusraamistik;

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

c) praktikas kohaldatavad turvameetmed ja -kord ning

d) avaldatava ELi salastatud teabe tasemele vastavad julgeolekukontrolli menetlused.

Artikkel 56

Halduskokkulepped

1. Kui liidu poliitilise või õigusraamistikuga seoses esineb pikaajaline vajadus vahetada kolmanda riigi või rahvusvahelise organisatsiooniga teavet, mille salastatuse tase ei ületa üldjuhul taset RESTREINT UE/EU RESTRICTED ja kui komisjoni julgeolekuasutus on pärast komisjoni julgeolekualase eksperdirühmaga konsulteerimist teinud kindlaks eelkõige selle, et kõnealuse poole julgeolekusüsteem ei ole salastatud teabe kaitse lepingu sõlmimiseks nõuetekohasel tasemel, võib komisjon sõlmida kõnealuse kolmanda riigi või rahvusvahelise organisatsiooni asjaomaste asutustega halduskokkuleppe.

2. Sellised halduskokkulepped sõlmitakse üldjuhul kirjavahetuse vormis.

3. Enne kokkuleppe sõlmimist tehakse hindamiskülastus. Komisjoni julgeolekualasele eksperdirühmale antakse teada hindamiskülastuse tulemustest. Kui erakorralistel põhjustel on vaja ELi salastatud teavet vahetada kiiresti, võib ELi salastatud teavet avaldada, eeldusel et sellise hindamiskülastuse võimalikult peatseks korraldamiseks tehakse kõik võimalik.

4. ELi salastatud teavet ei vahetata elektrooniliselt, välja arvatud juhul, kui see on halduskokkuleppes sõnaselgelt ette nähtud.

Artikkel 57

ELi salastatud teabe erakorraline ajutine avaldamine

1. Kui puudub salastatud teabe kaitse leping või halduskokkulepe ja kui komisjon või mõni selle talitustest teeb kindlaks, et liidu poliitilise või õigusraamistikuga seoses esineb erakorraline vajadus avaldada ELi salastatud teavet kolmandale riigile või rahvusvahelisele organisatsioonile, toimib komisjoni julgeolekuasutus järgmiselt: kontrollib vastavalt võimalusele, kas kolmanda riigi või rahvusvahelise organisatsiooni julgeolekuasutuste julgeolekunormid, -struktuurid ja menetlused tagavad talle avaldatava ELi salastatud teabe kaitse vastavalt standarditele, mis on vähemalt sama ranged kui käesolevas otsuses sätestatud standardid.

2. Komisjon teeb otsuse ELi salastatud teabe asjaomasele kolmandale riigile või rahvusvahelisele organisatsioonile avaldamise kohta julgeolekuküsimuste eest vastutava komisjoniliikme ettepanekul pärast konsulteerimist komisjoni julgeolekualase eksperdirühmaga.

3. Pärast ELi salastatud teabe avaldamise otsust ning teabe koostaja, kaasa arvatud selles sisalduva allikmaterjali koostaja eelneva kirjaliku nõusoleku olemasolul edastab komisjoni pädev asutus asjaomase teabe, mis varustatakse avaldatavuse märkega kolmanda riigi või rahvusvahelise organisatsiooni kohta, kellele see avaldati. Enne teabe tegelikku avaldamist või selle avaldamise ajal võtab asjaomane kolmas pool endale kirjalikult kohustuse kaitsta saadavat ELi salastatud teavet vastavalt käesolevas otsuses sätestatud aluspõhimõtetele ja miinimumstandarditele.

8. PEATÜKK

LÕPPSÄTTED

Artikkel 58

Varasemate otsuste asendamine

Käesoleva otsusega tunnistatakse kehtetuks ja asendatakse komisjoni otsus 2001/844/EÜ, ESTÜ, Euratom ([1]).

Artikkel 59

Enne käesoleva otsuse jõustumist koostatud salastatud teave

1. Kõik otsuse 2001/844/EÜ, ESTÜ, Euratom kohaselt salastatud ELi salastatud teavet sisaldavad dokumendid on jätkuvalt kaitstud vastavalt käesoleva otsuse asjakohastele sätetele.

2. Kogu salastatud teave, mis oli komisjoni valduses otsuse 2001/844/EÜ, ESTÜ, Euratom jõustumise kuupäeval, välja arvatud Euratomi salastatud teave:

a) on juhul, kui see on koostatud komisjonis, automaatselt ümber liigitatud tasemele RESTREINT UE, kui selle autor ei soovinud seda 31. jaanuariks 2002 ümber liigitada ega teavitanud sellest kõiki asjaomase dokumendi adressaate;

b) säilitab juhul, kui selle autor on väljastpoolt komisjoni, oma algse liigituse ja kui autor ei ole nõus selle salastatust kustutama ega teabe salastatuse taset alandama, käsitletakse seda samaväärse salastatuse tasemega ELi salastatud teabena.

Artikkel 60

Rakenduseeskirjad ja julgeolekuteated

1. Vajaduse korral koostab komisjon käesoleva otsuse rakenduseeskirjade kohta eraldi volitamisotsuse julgeolekuküsimuste eest vastutavale komisjoniliikmele, järgides täielikult kodukorda.

2. Julgeolekuküsimuste eest vastutav komisjoni liige võib pärast eespool nimetatud komisjoni otsuse alusel volituste saamist avaldada julgeolekuteateid, milles on esitatud käesoleva otsuse ja selle rakenduseeskirjade reguleerimisalasse kuuluvad julgeolekusuunised ja parimad tavad.

3. Komisjon võib delegeerida käesoleva artikli lõigetes 1 ja 2 nimetatud ülesanded eraldi delegeerimisotsusega personali- ja turvalisusküsimuste peadirektoraadi peadirektorile, järgides täielikult kodukorda.

Artikkel 61

Jõustumine

Käesolev otsus jõustub järgmisel päeval pärast selle avaldamist *Euroopa Liidu Teatajas*.

Brüssel, 13. märts 2015

Komisjoni nimel

president

Jean-Claude JUNCKER

([1]) Komisjoni otsus 2001/844/EÜ, ESTÜ, Euratom, 29. november 2001, millega muudetakse komisjoni kodukorda (EÜT L 317, 3.12.2001, lk 1).

I LISA

SALASTATUSE TASEMETE VASTAVUS

EL	TRES SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Euratom	EURA TOP SECRET	EURA SECRET	EURA CONFIDENTIAL	EURA 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
Luksemburg	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Ungari	„Szigorúan titkos!”	„Titkos!”	„Bizalmas!”	„Korlátozott terjesztésű!”
Malta	L-Ogħla Segretezza	Sigriet	Kunfidenzjali	Ristrett
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

EL	TRES SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
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 ([4])	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	Samaväärne märge puudub ([5])	UK OFFICIAL – SENSITIVE

([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.

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

([5]) Ühendkuningriik töötleb ja kaitseb „CONFIDENTIEL UE/EU CONFIDENTIAL” tasemel ELi salastatud teavet vastavalt salastatuse taseme „UK SECRET” suhtes kohaldatavatele julgeolekualase kaitse nõuetele.

II LISA

LÜHENDITE LOETELU

Akronüüm	Tähendus
CA	Krüptoloogiaamet
CAA	Krüptovahendite heakskiitmise asutus
CCTV	Videovalve
CDA	Krüptomaterjalide jaotamise asutus
CIS	Side- ja infosüsteemid, milles töödeldakse ELi salastatud teavet
DSA	Määratud julgeolekuasutus
EUCI	ELi salastatud teave
FSC	Töötlemisluba
IA	Infokindlus
IAA	Infokindluse asutus
IDS	Sissetungi avastamise süsteem
IT	Infotehnoloogia
LSO	Kohalik julgeolekuametnik
NSA	Riiklik julgeolekuasutus
PSC	Juurdepääsuluba
PSCC	Juurdepääsutõend
PSI	Programmi/projekti julgeolekujuhised
RCO	Registri kontrolliametnik
SAA	Turvalisuse akrediteerimise asutus
SAL	Julgeolekuaspekte käsitlev dokument
SCG	Salastatuse taseme määramise juhend
SecOPs	Turvanõuete rakendamise kord
TA	TEMPEST-asutus
TFEU	Euroopa Liidu toimimise leping

III LISA

RIIKLIKE JULGEOLEKUASUTUSTE LOETELU

BELGIA

Autorité nationale de Sécurité
SPF Affaires étrangères, Commerce extérieur et Coopération au Développement
15, rue des Petits Carmes
1000 Bruxelles/Brussel
Sekretariaadi tel +32 25014542
Faks +32 25014596
E-post: nvo-ans@diplobel.fed.be

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

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

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

SAKSAMAA

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

EESTI

Riigi julgeoleku volitatud esindaja osakond
Kaitseministeerium
Sakala 1
15094 Tallinn
Tel +372 7170113 0019, +372 7170117
Faks +372 7170213
E-post: nsa@mod.gov.ee

KREEKA

Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Διακλαδική Διεύθυνση Στρατιωτικών Πληροφοριών (ΔΔΣΠ)
Διεύθυνση Ασφαλείας και Αντιπληροφοριών
ΣΤΓ 1020 -Χολαργός (Αθήνα)
Ελλάδα
Tel +30 2106572045 (ώρες γραφείου)
+ 30 2106572009 (ώρες γραφείου)
Faks +30 2106536279; + 30 2106577612

Hellenic National Defence General Staff (HNDGS)
Military Intelligence Sectoral Directorate
Security Counterintelligence Directorate
GR-STG 1020 Holargos – Athens
Tel +30 2106572045
+ 30 2106572009
Faks +30 2106536279, +30 2106577612

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

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

Office of the National Security Council
Croatian NSA
Jurjevska 34
10000 Zagreb
Horvaatia
Tel +385 14681222
Faks + 385 14686049
Veebisait: www.uvns.hr

IIRIMAA

National Security Authority
Department of Foreign Affairs
76 – 78 Harcourt Street
Dublin 2
Tel +353 14780822
Faks +353 14082959

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

KÜPROS

ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ
ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Υπουργείο Άμυνας
Λεωφόρος Εμμανουήλ Ροΐδη 4
1432 Λευκωσία, Κύπρος
Tel +357 22807569, +357 22807643,
+357 22807764
Faks +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

LÄTI

National Security Authority
Constitution Protection Bureau of the Republic of Latvia
P.O.Box 286
1001 Riga
Tel +371 67025418
Faks +371 67025454
E-post: ndi@sab.gov.lv

LEEDU

Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija
(The Commission for Secrets Protection Coordination of the Republic of Lithuania National Security Authority)
Gedimino 40/1
01110 Vilnius
Tel +370 706 66701, +370 706 66702
Faks +370 706 66700
E-post: nsa@vsd.lt

LUKSEMBURG

Autorité nationale de Sécurité
Boîte postale 2379
1023 Luxembourg
Üldtelefon +352 24782210
Otsetelefon +352 24782253
Faks +352 24782243

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:
1357 Budapest, PO Box 2
E-post: nbf@nbf.hu
Veebisait: www.nbf.hu

MALTA

Ministry for Home Affairs and National Security
P.O. Box 146
MT-Valletta
Tel +356 21249844
Faks +356 25695321

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

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 22 58 57 944
Faks +48 22 58 57 443
E-post: nsa@abw.gov.pl
Veebisait: www.abw.gov.pl

PORTUGAL

Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Rua da Junqueira, 69
1300-342 Lisboa
Tel +351 213031710
Faks +351 213031711

RUMEENIA

Oficiul Registrului Național al Informațiilor Secrete de Stat
(Romanian NSA – ORNISS National Registry Office for Classified Information)
4 Mures Street
012275 Bucharest
Tel +40 212245830
Faks +40 212240714
E-post: nsa.romania@nsa.ro
Veebisait: www.orniss.ro

SLOVEENIA

Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
1000 Ljubljana
Tel +386 14781390
Faks +386 14781399
E-post: gp.uvtp@gov.si

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

SOOME

National Security Authority
Ministry for Foreign Affairs
P.O. Box 453
FI-00023 Government
Tel 16055890
Faks +358 916055140
E-post: NSA@formin.fi

ROOTSI

Utrikesdepartementet
(Ministry for Foreign Affairs)
SSSB
S-103 39 Stockholm
Tel +46 84051000
Faks +46 87231176
E-post: ud-nsa@foreign.ministry.se

ÜHENDKUNINGRIIK

UK National Security Authority
Room 335, 3rd Floor
70 Whitehall
London
SW1 A 2AS
Tel 1 +44 2072765649
Tel 2 +44 2072765497
Faks: +44 2072765651
E-post: UK-NSA@cabinet-office.x.gsi.gov.uk