II

(Teatised)

EUROOPA LIIDU INSTITUTSIOONIDE, ORGANITE JA ASUTUSTE TEATISED

EUROOPA PARLAMENT

EUROOPA PARLAMENDI JUHATUSE OTSUS

15. aprill 2013

konfidentsiaalse teabe käsitlemist Euroopa Parlamendis reguleeriva eeskirja kohta

(2014/C 96/01)

EUROOPA PARLAMENDI JUHATUS,

võttes arvesse Euroopa Parlamendi kodukorra artikli 23 lõiget 12 ning

arvestades järgmist:

(1) seoses raamkokkuleppega Euroopa Parlamendi ja Euroopa Komisjoni vaheliste suhete kohta [1], mis allkirjastati 20. oktoobril 2010 („raamkokkulepe") ning institutsioonidevahelise kokkuleppega Euroopa Parlamendi ja nõukogu vahel, mis käsitleb nõukogu valduses oleva salastatud teabe edastamist Euroopa Parlamendile ja selle töötlemist Euroopa Parlamendi poolt seoses teemadega, mis ei kuulu ühise välis- ja julgeolekupoliitika valdkonda, [2] mis allkirjastati 12. märtsil 2014. aastal („institutsioonidevaheline kokkulepe"), tuleb sätestada konfidentsiaalse teabe käsitlemist Euroopa Parlamendis reguleeriv eeskiri;

(2) Lissaboni lepinguga antakse Euroopa Parlamendile uued ülesanded ning parlamendi tegevuse arendamiseks konfidentsiaalsust nõudvates valdkondades tuleb konfidentsiaalse, sealhulgas ka salastatud teabe käsitlemiseks Euroopa Parlamendis kehtestada üldpõhimõtted, minimaalsed julgeolekustandardid ja asjakohased menetlused;

(3) käesoleva otsusega kehtestatava eeskirja eesmärk on tagada samaväärsed kaitsestandardid ning ühilduvus eeskirjadega, mille on vastu võtnud aluslepingutega või nende alusel asutatud või liikmesriikide poolt moodustatud muud institutsioonid, asutused, talitused ja ametid, et hõlbustada Euroopa Liidu otsustamisprotsessi sujuvat toimimist;

(4) käesoleva otsuse sätete rakendamine ei piira kooskõlas Euroopa Liidu toimimise lepingu (ELi toimimise leping) artikliga 15 vastu võetud kehtivate ega tulevaste, dokumentidele juurdepääsu käsitlevate eeskirjade kohaldamist;

[1] ELT L 304, 20.11.2010, lk 47.
[2] ELT C 95, 1.4.2014, lk 1.

(5) käesoleva otsuse sätete rakendamine ei piira kooskõlas ELi toimimise lepingu artikliga 16 vastu võetud kehtivate ega tulevaste, isikuandmete kaitset käsitlevate eeskirjade kohaldamist,

ON VASTU VÕTNUD JÄRGMISE OTSUSE:

Artikkel 1

Eesmärk

Käesolev otsus reguleerib konfidentsiaalse teabe haldamist ja käitlemist Euroopa Parlamendis, sealhulgas konfidentsiaalse teabe koostamist, vastuvõtmist, edastamist ja säilitamist sellise teabe konfidentsiaalsuse asjakohase kaitse eesmärgil. Käesoleva otsusega rakendatakse institutsioonidevahelist kokkulepet ja raamkokkulepet, eelkõige selle II lisa.

Artikkel 2

Mõisted

Käesolevas otsuses kasutatakse järgmisi mõisteid:

a) „teave" — mis tahes kirjalik või suuline teave, olenemata selle kandjast ja autorist;

b) „konfidentsiaalne teave" — salastatud teave ning muu konfidentsiaalne teave, mida ei ole salastatud;

c) „salastatud teave" — ELi salastatud teave ja samaväärne salastatud teave;

d) „ELi salastatud teave" — igasugune teave ja materjal, mis on „TRÈS SECRET UE / EU TOP SECRET", „SECRET UE / EU SECRET", „CONFIDENTIEL UE / EU CONFIDENTIAL" või „RESTREINT UE / EU RESTRICTED" salastatuse tasemega ja mille loata avaldamine võib eri määral kahjustada liidu või ühe või mitme liikmesriigi huve, olenemata sellest, kas selline teave pärineb aluslepingutega või nende alusel asutatud institutsioonidelt, asutustelt, talitustelt või ametitelt. Sellega seoses kasutatakse järgmisi teabe ja materjali salastatuse tasemeid:

— „TRÈS SECRET UE / EU TOP SECRET" — kasutatakse sellise teabe ja materjali puhul, mille loata avaldamine võib väga tõsiselt kahjustada liidu või ühe või mitme liikmesriigi olulisi huve;

— „SECRET UE / EU SECRET" — kasutatakse sellise teabe ja materjali puhul, mille loata avaldamine võib tõsiselt kahjustada liidu või ühe või mitme liikmesriigi olulisi huve;

— „CONFIDENTIEL UE / EU CONFIDENTIAL" — kasutatakse sellise teabe ja materjali puhul, mille loata avaldamine võib kahjustada liidu või ühe või mitme liikmesriigi olulisi huve;

— „RESTREINT UE / EU RESTRICTED" — kasutatakse sellise teabe ja materjali puhul, mille loata avaldamine võib negatiivselt mõjutada liidu või ühe või mitme liikmesriigi huve;

e) „samaväärne salastatud teave" — liikmesriikide, kolmandate riikide või rahvusvaheliste organisatsioonide väljastatud salastatud teave, mis kannab salastusmärget, mis on samaväärne mõnega ELi salastatud teabe salastusmärgetest ja mille on Euroopa Parlamendile edastanud nõukogu või komisjon;

f) „muu konfidentsiaalne teave" — mis tahes muu mittesalastatud konfidentsiaalne teave, kaasa arvatud andmekaitse eeskirjade või ametisaladuse hoidmise kohustuse alla kuuluv teave, mis on koostatud Euroopa Parlamendis või mille on edastanud Euroopa Parlamendile aluslepingutega või nende alusel asutatud muud institutsioonid, asutused, talitused ja ametid või liikmesriigid;

g) „dokument" — mis tahes talletud teave selle füüsilisest kujust või omadustest olenemata;

h) „materjal" — valmistatud või valmistamisel olevad dokumendid, masinad või seadmed;

i) „teadmisvajadus" — isiku vajadus pääseda juurde konfidentsiaalsele teabele tema ametikohustuste või ülesande täitmiseks;

j) „loa andmine" — Euroopa Parlamendi liikmete puhul presidendi otsus ning Euroopa Parlamendi ametnike ja fraktsioonides töötavate muude töötajate puhul peasekretäri otsus võimaldada isikule juurdepääs salastatud teabele kuni teatava salastatuse tasemeni; otsus põhineb julgeolekukontrolli positiivsel tulemusel, mille on läbi viinud liikmesriigi asutus vastavalt riigisisesele õigusele ja I lisa 2. osa sätetele;

k) „salastatuse taseme alandamine" — madalamale salastatuse astmele üleviimine;

l) „salastatuse kustutamine" — igasuguse salastatuse kõrvaldamine;

m) „märge" — muule konfidentsiaalsele teabele kantud märkus, mille eesmärk on osutada konkreetsetele juhistele, mida selle teabe käitlemisel tuleb järgida, või valdkonnale, mida konkreetne dokument hõlmab. Märge võib olla kantud ka salastatud teabele, et osutada lisanõuetele, mida teabe käitlemisel tuleb täita;

n) „märke kustutamine" — märke eemaldamine;

o) „koostaja" — konfidentsiaalse teabe nõuetekohaselt volitatud autor;

p) „julgeolekuteade" — II lisas sätestatud rakendusmeetmed;

q) „käitlemisjuhend" — Euroopa Parlamendi teenistustele konfidentsiaalse teabe haldamiseks antud tehnilised juhised.

Artikkel 3

Üldpõhimõtted ja miinimumstandardid

1. Euroopa Parlament käsitleb konfidentsiaalset teavet vastavalt I lisa 1. osas sätestatud üldpõhimõtetele ja miinimumstandarditele.

2. Euroopa Parlament loob vastavalt kõnealustele üldpõhimõtetele ja miinimumstandarditele teabeturbe juhtimissüsteemi. Teabeturbe juhtimissüsteem koosneb julgeolekuteadetest, käitlemisjuhendist ja asjakohasest kodukorrast. Teabeturbe juhtimissüsteemi ülesandeks on hõlbustada Euroopa Parlamendi tegevust ja haldustööd, tagades samas Euroopa Parlamendi käsitletava mis tahes konfidentsiaalse teabe kaitse täielikus kooskõlas sellise teabe koostaja poolt julgeolekuteates sätestatud eeskirjadega.

Konfidentsiaalse teabe töötlemine julgeolekuteates 3 sätestatud Euroopa Parlamendi automatiseeritud side- ja infosüsteemide abil toimub vastavalt infokindluse põhimõtetele.

3. Euroopa Parlamendi liikmed võivad tutvuda salastatud teabega ilma julgeolekukontrolli läbimata kuni tasemeni RESTREINT UE / EU RESTRICTED (kaasa arvatud).

4. Kui asjaomane teave on salastatud tasemega CONFIDENTIEL UE / EU CONFIDENTIAL või samaväärne teave, antakse sellele juurdepääs Euroopa Parlamendi liikmele, kellele president on loa andnud vastavalt lõikele 5 või kes on alla kirjutanud deklaratsioonile, millega ta kinnitab, et ta ei avalda teabe sisu kolmandatele isikutele, kohustub CONFIDENTIEL UE / EU CONFIDENTIAL salastatuse tasemega teavet kaitsma ja on teadlik nende nõuete rikkumise tagajärgedest.

5. Kui asjaomane teave on salastatud tasemega SECRET UE / EU SECRET või TRÈS SECRET / EU TOP SECRET või samaväärne teave, antakse sellele juurdepääs Euroopa Parlamendi liikmele, kellele president on loa andnud pärast seda, kui:

a) parlamendiliige on läbinud vastavalt käesoleva otsuse I lisa 2. osale julgeolekukontrolli või

b) liikmesriigi pädev asutus on teatanud, et asjaomasel parlamendiliikmel on selleks oma tööülesannete tõttu vastavalt riigisisestele õigusaktidele nõuetekohased volitused.

6. Enne salastatud teabele juurdepääsu võimaldamist teavitatakse Euroopa Parlamendi liiget kohustusest kaitsta sellist teavet vastavalt I lisale ja parlamendiliige kinnitab, et ta on sellest kohustusest teadlik. Teda teavitatakse samuti sellise kaitse tagamise vahenditest.

7. Euroopa Parlamendi ametnikud ja fraktsioonides töötavad muud töötajad võivad tutvuda konfidentsiaalse teabega, kui nende teadmisvajadus on kindlaks tehtud, ning nad võivad tutvuda kõrgema salastatuse tasemega teabega kui RESTREINT UE / EU RESTRICTED, kui nad on läbinud vastava tasemega julgeolekukontrolli. Neile võimaldatakse salastatud teabele juurdepääs ainult siis, kui neid on teavitatud nende kohustusest sellist teavet kaitsta ja sellise kaitse tagamise vahenditest ning neile on antud selle kohta kirjalikud juhised ning kui nad on allkirjastanud deklaratsiooni, milles nad kinnitavad, et on nimetatud juhised kätte saanud ja kohustuvad neid vastavalt kehtivatele eeskirjadele järgima.

Artikkel 4

Konfidentsiaalse teabe koostamine ja halduslik käitlemine Euroopa Parlamendis

1. Konfidentsiaalset teavet võivad koostada ja/või teavet salastada, nagu on sätestatud julgeolekuteates, Euroopa Parlamendi president, asjaomaste parlamendikomisjonide esimehed, peasekretär ja/või muu isik, kellele peasekretär on selleks andnud nõuetekohase kirjaliku loa.

2. Salastatud teabe koostamisel kohaldab selle koostaja sobivat salastatuse taset kooskõlas I lisas sätestatud rahvusvaheliste standardite ning määratlustega. Üldreeglina määrab teabe koostaja kindlaks ka adressaadid, kellele antakse luba tutvuda teabega vastavalt selle salastatuse tasemele. See teave antakse edasi salastatud teabe üksusele, kui dokument on antud hoiule nimetatud üksusele.

3. Ametisaladuse hoidmise kohustuse alla kuuluvat muud konfidentsiaalset teavet käsitletakse vastavalt I ja II lisale ning käitlemisjuhendile.

Artikkel 5

Konfidentsiaalse teabe vastuvõtmine Euroopa Parlamendis

1. Euroopa Parlamendi poolt saadud konfidentsiaalne teave edastatakse:

a) RESTREINT UE / EU RESTRICTED salastatuse tasemega või samaväärse teabe ja muu konfidentsiaalse teabe puhul vastava taotluse esitanud parlamendi organi või ametikandja sekretariaati või otse salastatud teabe üksusele;

b) CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE / EU SECRET või TRÈS SECRET UE / EU TOP SECRET salastatuse tasemega või samaväärse teabe puhul salastatud teabe üksusele.

2. Konfidentsiaalse teabe registreerimise, säilitamise ja jälgitavusega tegeleb olenevalt asjaoludest teabe vastu võtnud parlamendi organi või ametikandja sekretariaat või salastatud teabe üksus.

3. Kui komisjon edastab konfidentsiaalset teavet vastavalt raamkokkuleppele II lisa punktile 3.2 või kui nõukogu edastab salastatud teavet vastavalt institutsioonidevahelise kokkuleppe artikli 5 lõikele 4, antakse teabe konfidentsiaalsuse tagamiseks ettenähtud ja ühiselt kokkulepitud tingimused koos konfidentsiaalse teabega olenevalt asjaoludest hoiule parlamendi organi või ametikandja sekretariaadile või salastatud teabe üksusele.

4. Lõikes 3 osutatud tingimusi võib mutatis mutandis kohaldada ka siis, kui konfidentsiaalse teabe edastavad aluslepingutega või nende alusel asutatud muud institutsioonid, asutused, talitused ja ametid või liikmesriigid.

5. TRÈS SECRET UE / EU TOP SECRET salastatuse tasemele või samaväärsele tasemele vastava kaitse tagamiseks moodustab esimeeste konverents järelevalvekomisjoni. TRÈS SECRET UE / EU TOP SECRET salastatuse tasemega või samaväärne teave edastatakse Euroopa Parlamendile kooskõlas täiendavate tingimustega, milles lepivad omavahel kokku Euroopa Parlament ning teavet edastav liidu institutsioon.

Artikkel 6

Salastatud teabe edastamine Euroopa Parlamendi poolt kolmandatele osapooltele

Euroopa Parlament võib teabe koostaja või Euroopa Parlamendile salastatud teabe edastanud liidu institutsiooni eelneval kirjalikul nõusolekul edastada salastatud teabe kolmandatele osapooltele tingimusel, et nad tagavad, et salastatud teabe käitlemisel järgitakse nende teenistustes ja tööruumides eeskirju, mis on samaväärsed käesolevas otsuses sätestatud eeskirjaga.

Artikkel 7

Turvatud rajatised

1. Konfidentsiaalse teabe haldamiseks rajab Euroopa Parlament turvaala ja turvatud lugemissaalid.

2. Turvaalas on olemas vahendid salastatud teabe registreerimiseks, arhiveerimiseks, edastamiseks ja käitlemiseks ning sellega tutvumiseks. Turvaala koosneb muu hulgas lugemissaalist ja koosolekuruumist, kus on võimalik salastatud teabega tutvuda, ja seda haldab salastatud teabe üksus.

3. Väljaspool turvaala võib rajada turvatud lugemissaale, kus võib tutvuda RESTREINT UE / EU RESTRICTED salastatuse tasemega või samaväärse teabega ja muu konfidentsiaalse teabega. Turvatud lugemissaale haldavad olenevalt asjaoludest Euroopa Parlamendi organi või ametikandja sekretariaadi pädevad teenistused või salastatud teabe üksus. Nendes saalides ei ole koopiamasinaid, telefone, fakse, skannereid ega muid dokumentide paljundamiseks või edastamiseks ettenähtud tehnilisi seadmeid.

Artikkel 8

Konfidentsiaalse teabe registreerimine, käitlemine ja säilitamine

1. RESTREINT UE / EU RESTRICTED salastatuse tasemega või samaväärset teavet ja muud konfidentsiaalset teavet registreerivad ja säilitavad Euroopa Parlamendi organi või ametikandja sekretariaadi pädevad teenistused või salastatud teabe üksus, olenevalt sellest, kes teabe sai.

2. RESTREINT UE / EU RESTRICTED salastatuse tasemega või samaväärse teabe ja muu konfidentsiaalse teabe käitlemise suhtes kohaldatakse järgmisi nõudeid:

a) dokumendid antakse isiklikult üle sekretariaadi juhatajale, kes need registreerib ja esitab nende kättesaamise kohta kinnituse;

b) kui dokumente parajasti ei kasutata, on nad sekretariaadi vastutusel lukustatud kohas hoiul;

c) teavet ei tohi mingil juhul salvestada ühelegi muule kandjale ega edastada ühelegi teisele isikule. Dokumente võib paljundada üksnes julgeolekuteates kindlaks määratud nõuetekohaselt akrediteeritud seadmete abil;

d) teabele juurdepääsu õigus on ainult neil, kelle teabe koostaja või teabe Euroopa Parlamendile edastanud liidu institutsioon on kindlaks määranud vastavalt artikli 4 lõikele 2 või artikli 5 lõigetele 3, 4 ja 5;

e) Euroopa Parlamendi organi või ametikandja sekretariaat märgib üles kõik isikud, kes on teabega tutvunud, ning tutvumise kuupäeva ja kellaaja, ning edastab dokumentide tutvumisega seoses kogutud teabe salastatud teabe üksusele siis, kui teave antakse hoiule salastatud teabe üksusele.

3. CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE / EU SECRET või TRÈS SECRET UE / EU TOP SECRET salastatuse tasemega või samaväärset teavet registreerib, käitleb ja säilitab salastatud teabe üksus, kes teeb seda turvaalal ja vastavalt salastatuse tasemele ja julgeolekuteates sätestatule.

4. Lõigetes 1 ja 3 sätestatud eeskirjade rikkumise korral teavitab olenevalt asjaoludest parlamendi organi või ametikandja sekretariaadi või salastatud teabe üksuse vastutav ametnik sellest peasekretäri, kes teavitab sellest omakorda Euroopa Parlamendi presidenti, kui rikkuja on parlamendiliige.

Artikkel 9

Pääs turvatud rajatistesse

1. Turvaalasse pääsevad ainult järgmised isikud:

a) isikud, kellel on artikli 3 lõigete 4–7 kohaselt õigus tutvuda turvaalas hoitava teabega ja kes on esitanud artikli 10 lõike 1 kohase taotluse;

b) isikud, kellel on artikli 4 lõike 1 kohaselt õigus salastatud teavet koostada ja kes on esitanud artikli 10 lõike 1 kohase taotluse;

c) salastatud teabe üksuses töötavad Euroopa Parlamendi ametnikud;

d) side- ja infosüsteemide haldamise eest vastutavad Euroopa Parlamendi ametnikud;

e) vajaduse korral turvalisuse ja tuleohutuse eest vastutavad Euroopa Parlamendi ametnikud;

f) puhastusteenust osutavad töötajad, kuid üksnes salastatud teabe üksuse ametniku juuresolekul ja tema range järelevalve all.

2. Salastatud teabe üksus võib turvaalasse pääsemise õiguse andmisest keelduda igaühe puhul, kellele ei oleks selleks luba antud. Juurdepääsu andmisest keeldumise otsuse vaidlustamine esitatakse juhul, kui pääsu taotles Euroopa Parlamendi liige, Euroopa Parlamendi presidendile ja muudel juhtudel peasekretärile.

3. Peasekretär võib anda loa korraldada turvaalas asuvas koosolekuruumis piiratud arvul osalejatega koosoleku.

4. Turvatud lugemissaali pääsevad ainult järgmised isikud:

a) konfidentsiaalse teabega tutvumise või selle koostamise eesmärgil Euroopa Parlamendi liikmed, ametnikud ja fraktsioonides töötavad muud Euroopa Parlamendi töötajad, kelle isikusamasus on nõuetekohaselt kindlaks tehtud;

b) side- ja infosüsteemide haldamise eest vastutavad Euroopa Parlamendi ametnikud, teabe saanud parlamendi organi või ametikandja sekretariaadi vastutavad ametnikud ja salastatud teabe üksuse ametnikud;

c) vajaduse korral turvalisuse ja tuleohutuse eest vastutavad Euroopa Parlamendi ametnikud;

d) puhastusteenust osutavad töötajad, kuid olenevalt asjaoludest üksnes parlamendi organi või ametikandja sekretariaadis või salastatud teabe üksuses töötava ametniku juuresolekul ja tema range järelevalve all.

5. Parlamendi organi või ametikandja pädev sekretariaat või salastatud teabe üksus — olenevalt asjaoludest — võib turvatud lugemissaali pääsemise õiguse andmisest keelduda igaühe puhul, kellele ei ole selleks luba antud. Juurdepääsu andmisest keeldumise otsuse vaidlustamine esitatakse juhul, kui pääsu taotles Euroopa Parlamendi liige, Euroopa Parlamendi presidendile ja muudel juhtudel peasekretärile.

Artikkel 10

Konfidentsiaalse teabega tutvumine ja selle koostamine turvatud rajatistes

1. Isik, kes soovib konfidentsiaalse teabega tutvuda või seda koostada turvaalas, teatab eelnevalt oma nime salastatud teabe üksusele. Üksus kontrollib selle isiku isikusamasust ja teeb kindlaks, kas tal on vastavalt artikli 3 lõigetele 3–7, artikli 4 lõikele 1 või artikli 5 lõigetele 3, 4 ja 5 lubatud konfidentsiaalse teabega tutvuda või seda koostada.

2. Isik, kes soovib vastavalt artikli 3 lõigetele 3 ja 7 tutvuda RESTREINT EU / EU RESTRICTED salastatuse tasemega või samaväärse teabega või muu konfidentsiaalse teabega turvatud lugemissaalis, teatab eelnevalt oma nime Euroopa Parlamendi organi või ametikandja sekretariaadi pädevatele teenistustele või salastatud teabe üksusele.

3. Turvatud rajatises konfidentsiaalse teabega tutvumiseks Euroopa Parlamendi organi või ametikandja sekretariaadi või salastatud teabe üksuse ametniku juuresolekul antakse luba vaid ühele isikule korraga, välja arvatud erandlike asjaolude korral (näiteks kui lühikese aja jooksul on esitatud palju taotlusi).

4. Teabega tutvumise ajal on keelatud kontaktid väliskeskkonnaga (sh telefoni või muude tehnikavahendite abil), märkmete tegemine ning konfidentsiaalse teabe paljundamine või fotografeerimine.

5. Enne turvatud rajatisest lahkumise lubamist kontrollib Euroopa Parlamendi organi või ametikandja sekretariaadi või salastatud teabe üksuse ametnik, et konfidentsiaalne teave, millega tutvuti, on alles, puutumatu ja terviklik.

6. Nende eeskirjade rikkumise korral teavitab Euroopa Parlamendi organi või ametikandja sekretariaadi või salastatud teabe üksuse ametnik sellest peasekretäri, kes teavitab sellest omakorda Euroopa Parlamendi presidenti, kui rikkuja on parlamendiliige.

Artikkel 11

Väljaspool turvatud rajatisi toimuval kinnisel koosolekul konfidentsiaalse teabega tutvumise miinimumstandardid

1. Parlamendikomisjonide või muude Euroopa Parlamendi poliitiliste ja haldusorganite liikmed võivad RESTREINT UE / EU RESTRICTED salastatuse tasemega või samaväärse teabega ja muu konfidentsiaalse teabega tutvuda väljaspool turvatud rajatisi toimuval kinnisel koosolekul.

2. Lõikes 1 osutatud juhul tagab koosoleku eest vastutava Euroopa Parlamendi organi või ametikandja sekretariaat, et täidetud on järgmised tingimused:

a) koosolekuruumi lubatakse siseneda vaid isikutel, kelle pädeva komisjoni või organi juhataja on määranud sellel koosolekul osalema;

b) kõik dokumendid nummerdatakse, jagatakse koosoleku alguses välja ja kogutakse koosoleku lõppedes taas kokku ning nende kohta ei tehta märkmeid, neid ei paljundata ning nendest ei tehta fotosid;

c) koosoleku protokollis ei mainita arutlusel olnud teabe sisu. Protokollida võib ainult vastuvõetud otsused;

d) Euroopa Parlamendi teabesaajatele suuliselt edastatava konfidentsiaalse teabe suhtes kohaldatakse samaväärset kaitsetaset nagu kirjaliku konfidentsiaalse teabe suhtes;

e) koosolekuruumides ei hoita mingeid lisadokumente;

f) koosoleku alguses jagatakse osalejatele ja tõlkidele ainult vajalik arv dokumentide koopiaid;

g) koosoleku juhataja selgitab kohe koosoleku alguses dokumentide salastatust/salastusmärkeid;

h) osalejad ei vii dokumente koosolekuruumist välja;

i) koosoleku lõpus kogub Euroopa Parlamendi organi või ametikandja sekretariaat kõik dokumendid kokku ja loeb need üle; ja

j) koosolekuruumi, kus tutvutakse kõnealuse konfidentsiaalse teabega või arutatakse seda, ei võeta kaasa elektroonilisi sidevahendeid ega muid elektroonilisi seadmeid.

3. Kui kinnisel koosolekul arutatakse raamkokkuleppe II lisa punktis 3.2.2 ja institutsioonidevahelise kokkuleppe artikli 6 lõikes 5 sätestatud erandite kohaselt CONFIDENTIEL UE / EU CONFIDENTIAL salastatuse tasemega või samaväärset teavet, tagab koosoleku eest vastutava Euroopa Parlamendi organi või ametikandja sekretariaat lisaks vastavuse tagamisele lõikes 2 sätestatule, et koosolekul osalema määratud isikud täidavad artikli 3 lõigete 4 ja 7 nõudeid.

4. Lõikes 3 osutatud juhul annab salastatud teabe üksus kinnise koosoleku eest vastutava parlamendi organi või ametikandja sekretariaadile arutlusele tulevate dokumentide vajaliku arvu koopiad, mis antakse pärast koosolekut salastatud teabe üksusele tagasi.

Artikkel 12

Konfidentsiaalse teabe arhiveerimine

1. Turvaalal tagatakse turvatud arhiveerimissüsteemi olemasolu. Turvatud arhiivi haldamise eest vastutab salastatud teabe üksus, kes järgib arhiveerimise standardnõudeid.

2. Salastatud teabe üksusesse hoiule antud salastatud teave ning parlamendi organi või ametikandja sekretariaati hoiule antud RESTREINT UE / EU RESTRICTED salastatuse tasemega või samaväärne teave viiakse üle turvaalas asuvasse turvatud arhiivi kuus kuud pärast seda, kui sellega viimati tutvuti, ning kõige hiljem üks aasta pärast seda, kui see hoiule anti. Muu konfidentsiaalse teabe, mida ei hoita salastatud teabe üksuses, arhiveerib Euroopa Parlamendi asjaomase organi või ametikandja sekretariaat, kes tegutseb dokumendihalduse üldeeskirjade kohaselt.

3. Turvatud arhiivis hoitava konfidentsiaalse teabega saab tutvuda järgmistel tingimustel:

a) konfidentsiaalse teabega on õigus tutvuda ainult isikutel, kes on nimeliselt, ametikohustuste või ametikoha järgi märgitud konfidentsiaalse teabe esitamisel täidetud saatelehele;

b) konfidentsiaalse teabega tutvumise taotlus esitatakse salastatud teabe üksusele, kes tagab arhiividokumendi edastamise turvatud lugemissaali;

c) kohaldatakse artiklis 10 sätestatud konfidentsiaalse teabega tutvumise korda ja tingimusi.

Artikkel 13

Konfidentsiaalse teabe salastatuse taseme alandamine, salastatuse kustutamine ja märke kustutamine

1. Konfidentsiaalse teabe salastatuse taset võib alandada, salastatuse kustutada ja märke kustutada ainult teabe koostaja eelneval loal ja vajaduse korral pärast arutelu muude huvitatud osapooltega.

2. Salastatuse taseme alandamine või salastatuse kustutamine kinnitatakse kirjalikult. Teabe koostaja vastutab selle eest, et adressaate teavitatakse muudatustest, ning adressaadid omakorda vastutavad selle eest, et muudatustest teavitatakse järgmisi adressaate, kellele nemad on saatnud kõnealuse dokumendi või selle koopia. Võimaluse korral määravad teabe koostajad salastatud dokumentidele kuupäeva, ajavahemiku või sündmuse, millal võib salastatuse taset alandada või salastatuse kustutada. Kui see ei ole võimalik, vaatavad nad dokumendid hiljemalt iga viie aasta järel läbi, et teha kindlaks, kas esialgne salastatuse tase on endiselt vajalik.

3. Turvatud arhiivis hoitavat konfidentsiaalset teavet kontrollitakse asjakohase ajavahemiku järel, kuid mitte hiljem kui 25. aastal pärast teabe koostamist, et otsustada, kas teabe salastatus tuleks kustutada, salastatuse taset tuleks alandada või märge kustutada. Sellise teabe kontrollimine ja avalikustamine toimub vastavalt nõukogu 1. veebruari 1983. aasta määrusele (EMÜ, Euratom) nr 354/83, mis käsitleb Euroopa Majandusühenduse ja Euroopa Aatomienergiaühenduse ajalooarhiivide avalikkusele kättesaadavaks tegemist ([1]). Salastatuse kustutab salastatud teabe koostaja või vastutav teenistus kooskõlas I lisa 1. osa punktiga 10.

4. Pärast salastatuse taseme kustutamist viiakse turvatud arhiivis hoitud endine salastatud teave üle Euroopa Parlamendi ajalooarhiivi, kus seda säilitatakse ja käsitletakse kohaldatavate eeskirjade kohaselt.

5. Pärast märke kustutamist kohaldatakse endise muu konfidentsiaalse teabe suhtes Euroopa Parlamendi dokumendihalduse eeskirju.

Artikkel 14

Julgeolekunõuete rikkumine ning konfidentsiaalse teabe kadumine või ohtusattumine

1. Konfidentsiaalsuse rikkumise korral üldiselt ning eelkõige käesoleva otsuse rikkumise korral kohaldatakse Euroopa Parlamendi liikmete puhul Euroopa Parlamendi kodukorras sätestatud karistusi puudutavaid asjakohaseid sätteid.

2. Euroopa Parlamendi töötajate poolt toime pandud rikkumisel kohaldatakse Euroopa Liidu ametnike personalieeskirjades ning Euroopa Liidu muude teenistujate teenistustingimustes sätestatud menetlusi ja karistusi, mis on ette nähtud määruses (EMÜ, Euratom, ESTÜ) nr 259/68 ([2]) („personalieeskirjad").

([1]) EÜT L 43, 15.2.1983, lk 1.
([2]) EÜT L 56, 4.3.1968, lk 1.

3. Julgeolekuteates 6 määratletud rikkumise korral korraldab olenevalt asjaoludest president ja/või peasekretär vajaliku juurdluse.

4. Kui konfidentsiaalse teabe edastas Euroopa Parlamendile liidu institutsioon või liikmesriik, teavitab olenevalt asjaoludest president ja/või peasekretär asjaomast liidu institutsiooni või liikmesriiki salastatud teabe tõendatud või kahtlustatavast kadumisest või ohtusattumisest ning uurimistulemustest ja edaspidiste rikkumise vältimiseks võetud meetmetest.

Artikkel 15

Käesoleva otsuse ja selle rakenduseeskirjade kohandamine ning iga-aastane aruanne käesoleva otsuse kohaldamise kohta

1. Peasekretär teeb ettepaneku käesoleva otsuse ja seda rakendavate lisade vajaliku kohandamise kohta ning edastab selle otsuse tegemiseks juhatusele.

2. Peasekretär vastutab selle eest, et Euroopa Parlamendi teenistused rakendavad käesolevat otsust, ja annab käesolevas otsuses sätestatud põhimõtete kohaselt välja teabeturbe juhtimissüsteemiga seotud küsimuste käitlemisjuhendi.

3. Peasekretär esitab igal aastal juhatusele käesoleva otsuse kohaldamise kohta aruande.

Artikkel 16

Ülemineku- ja lõppsätted

1. Salastatud teabe üksuses või mõnes muus Euroopa Parlamendi arhiivis hoitavat mittesalastatud teavet, mida loetakse konfidentsiaalseks ja mis on pärit varasemast ajast kui 1. aprill 2014, loetakse käesoleva otsuse kohaldamisel muuks konfidentsiaalseks teabeks. Teabe koostaja võib igal ajal selle salastatuse taset muuta.

2. Erandina käesoleva otsuse artikli 5 lõike 1 punktist a ja artikli 8 lõikest 1 tegeleb nõukogu poolt institutsioonidevahelise kokkuleppe kohaselt esitatud RESTREINT UE / EU RESTRICTED salastatuse tasemega või samaväärse teabe hoidmise, registreerimise ja säilitamisega alates 1. aprill 2014 12 kuu jooksul salastatud teabe üksus. Selle teabega võib tutvuda vastavalt institutsioonidevahelise kokkuleppe artikli 4 lõike 2 punktidele a ja c ning artikli 5 lõikele 4.

3. Juhatuse 6. juuni 2011. aasta otsus konfidentsiaalse teabe käsitlemist Euroopa Parlamendis reguleeriva eeskirja kohta tunnistatakse kehtetuks.

Artikkel 17

Jõustumine

Käeolev otsus jõustub selle *Euroopa Liidu Teatajas* avaldamise päeval.

I LISA

1. osa

KONFIDENTSIAALSE TEABE KAITSMIST KÄSITLEVAD JULGEOLEKU ÜLDPÕHIMÕTTED JA MIINIMUMSTANDARDID

1. **SISSEJUHATUS**

Käesolevate sätetega kehtestatakse konfidentsiaalse teabe kaitsmist käsitlevad julgeoleku üldpõhimõtted ja miinimumstandardid, mida tuleb austada ja/või järgida Euroopa Parlamendil kõikides töökohtades ning samuti kõigil salastatud teabe ja muu konfidentsiaalse teabe saajatel, et tagada julgeolek ja kindlustunne kõigile asjaomastele isikutele, et rakendatakse ühist kaitsestandardit. Neid täiendavad lisas II sätestatud julgeolekuteated ja muud sätted, millega reguleeritakse konfidentsiaalse teabe töötlemist parlamendikomisjonide ning parlamendi muude organite ja ametikandjate poolt.

2. **ALUSPÕHIMÕTTED**

Euroopa Parlamendi julgeolekupoliitika on parlamendi üldise sisemise halduspoliitika lahutamatu osa ja põhineb seega parlamendi üldise poliitika juhtpõhimõtetel. Nende põhimõtete hulka kuuluvad seaduslikkus, läbipaistvus, aruandekohustuse põhimõte, subsidiaarsus ja proportsionaalsus.

Seaduslikkus tähendab vajadust püsida julgeolekufunktsioonide täitmisel rangelt õiguslikus raamistikus ning järgida kohaldatavaid õigusnorme. Samuti tähendab see, et julgeolekualased kohustused peavad põhinema asjakohastel õigussätetel. Personalieeskirjade sätted, eelkõige artikkel 17, mille kohaselt peab teenistuja hoiduma tööülesannete täitmisel saadud teabe loata avaldamisest, ja eeskirjade VI jaotis distsiplinaarmeetmete kohta kehtivad täies mahus. Samuti tähendab see, et Euroopa Parlamendi vastutusalas toimuvate julgeoleku rikkumistega tegeletakse parlamendi kodukorda ja tema distsiplinaarmeetmete poliitikat järgides.

Läbipaistvus tähendab selguse vajadust kõikide julgeolekueeskirjade ja -sätete puhul, vajadust tasakaalu järele eri teenistuste ja valdkondade vahel (füüsiline julgeolek võrreldуna teabekaitsega jne) ning vajadust järjepideva ja struktureeritud teadliku julgeolekupoliitika järele. Lisaks tähendab see vajadust selgete kirjalike juhtnööride järele julgeolekumeetmete rakendamiseks.

Aruandekohustus tähendab, et julgeolekualased kohustused tuleb selgelt määratleda. Lisaks tähistab see vajadust regulaarselt kontrollida, kas neid kohustusi täidetakse nõuetekohaselt.

Subsidiaarsus tähendab, et julgeolek tuleb organiseerida kõige madalamal võimalikul tasemel ning võimalikult lähedal Euroopa Parlamendi peadirektoraatidele ja teenistustele.

Proportsionaalsus tähendab seda, et julgeolekumeetmed peavad piirduma rangelt ainult sellega, mis on tingimata vajalik, ning et need meetmed on vastavuses kaitstavate huvidega ning tegeliku või potentsiaalse ohuga nendele huvidele, et neid huve oleks võimalik kaitsta võimalikult vähehäirival viisil.

3. **TEABETURBE ALUSED**

Usaldusväärse teabeturbe aluseks on järgmised tingimused:

a) olemas on nõuetekohased side- ja infosüsteemid. Nende eest vastutab Euroopa Parlamendi julgeolekuasutus (nagu on määratletud julgeolekuteates 1);

b) Euroopa Parlamendis on olemas infokindluse asutus (nagu on määratletud julgeolekuteates 1), mis vastutab koostöös julgeolekuasutusega teabe ja nõuannete andmise eest side- ja infosüsteemide ohtude tehniliste külgede kohta ja milliste vahenditega nende ohtude eest kaitsta;

c) Euroopa Parlamendi vastutavad teenistused ja muude liidu institutsioonide julgeolekuteenistused teevad tihedat koostööd.

4. **TEABETURBE PÕHIMÕTTED**

4.1. ***Eesmärgid***

Teabeturbe peamised eesmärgid on järgmised:

a) kaitsta konfidentsiaalset teavet spionaaži, kahjustamise ja loata avaldamise eest;

b) kaitsta side- ja infosüsteemides ning -võrkudes käideldavat salastatud teavet konfidentsiaalsuse, terviklikkuse ja kättesaadavuse ohtuseadmise eest;

c) kaitsta Euroopa Parlamendi hooneid, kus hoitakse salastatud teavet, sabotaaži ja kuritahtliku kahjustamise eest;

d) julgeolekule esinenud ründe korral hinnata tekitatud kahju, piirata selle tagajärgi, korraldada julgeolekujuurdlus ja võtta vajalikke heastamismeetmeid.

4.2. ***Salastamine***

4.2.1. Salastatuse puhul eeldab kaitstava teabe ja materjalide valik ning vajaliku kaitsetaseme hindamine hoolikust ja kogemusi. On äärmiselt oluline, et kaitse tase vastaks konkreetse kaitstava teabe või materjali tundlikkusele julgeoleku kontekstis. Teabe sujuva liikumise tagamiseks tuleb vältida nii üle- kui alasalastamist.

4.2.2. Salastamissüsteem on vahend, mille abil saab käesolevas jaotises sätestatud põhimõtteid ellu viia. Samalaadset salastamissüsteemi järgitakse spionaaži, sabotaaži, terrorismi ja muude ohtude ärahoidmise kavandamise ja korraldamise puhul, et kõige rohkem kaitsta kõige olulisemaid salastatud teavet sisaldavaid hooneid ja kõige tundlikumaid kohti neis hoonetes.

4.2.3. Vastutus teabe salastamise eest lasub ainuisikuliselt asjaomase teabe koostajal.

4.2.4. Salastatuse tase võib põhineda ainult asjaomase teabe sisul.

4.2.5. Mitmest osast koosneva teabe salastamisel rakendatakse sellist salastatuse taset, mis on vähemalt sama kõrge kui kõige kõrgema salastatuse tasemega osa puhul. Kogu teabele võib siiski omistada ka kõrgema salastatuse taseme kui selle osadele.

4.2.6 Salastatus määratakse ainult siis, kui see on vajalik, ja nii kauaks, kui see on vajalik.

4.3. ***Julgeolekumeetmete eesmärgid***

Julgeolekumeetmed:

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

b) on kavandatud nii, et oleks võimalik tuvastada isikuid, kelle positsioon võib (juurdepääsu, suhete või muu tõttu) seada ohtu salastatud teabe ja sellist teavet sisaldavate oluliste rajatiste julgeoleku, ning tagada nende töölt kõrvaldamine või viimine teisele tööle;

c) takistavad loata isikute juurdepääsu konfidentsiaalsele teabele ja rajatistele, mis sisaldavad konfidentsiaalset teavet;

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

e) tagavad konfidentsiaalse teabe terviklikkuse (vältides rikkumist, loata muutmist ja kustutamist) ja kättesaadavuse (ei takistata nende isikute juurdepääsu, kellel on seda vaja ja kellele on selleks antud luba), ja eriti siis, kui seda teavet säilitatakse, töödeldakse või edastatakse elektroonilisel kujul.

5. ÜHISED MIINIMUMSTANDARDID

Euroopa Parlament tagab, et kõik salastatud teabe saajad nii institutsioonisiseselt kui tema volituste piires, nimelt kõik tema teenistused ja lepingupartnerid, järgivad ühiseid julgeoleku miinimumstandardeid, et kõnealust teavet oleks võimalik edastada kindla teadmisega, et seda käideldakse samasuguse hoolega. Sellised miinimumstandardid hõlmavad ka Euroopa Parlamendi ametnike ja fraktsioonides töötavate muude Euroopa Parlamendi töötajate julgeolekukontrolli kriteeriume ning konfidentsiaalse teabe kaitsmise korda.

Euroopa Parlament võimaldab kolmandatel osapooltel pääseda ligi konfidentsiaalsele teabele ainult tingimusel, et nad tagavad, et teavet käideldakse kooskõlas selliste sätetega, mis on vähemalt rangelt samaväärsed kõnealuste ühiste miinimumstandarditega.

Ühiseid miinimumstandardeid kohaldatakse ka siis, kui Euroopa Parlament annab lepingu või toetuslepinguga tööstus- või muudele üksustele sellised ülesanded, mis on seotud konfidentsiaalse teabega.

6. EUROOPA PARLAMENDI AMETNIKE JA FRAKTSIOONIDES TÖÖTAVATE MUUDE EUROOPA PARLAMENDI TÖÖTAJATE JULGEOLEK

6.1. *Euroopa Parlamendi ametnike ja fraktsioonides töötavate muude Euroopa Parlamendi töötajate julgeolekujuhend*

Euroopa Parlamendi ametnikel ja fraktsioonides töötavatel muudel Euroopa Parlamendi töötajatel, kellel on ametikoha tõttu juurdepääs salastatud teabele, antakse tööleasumisel ja seejärel regulaarsete ajavahemike järel põhjalikud juhtnöörid julgeoleku vajalikkuse ja sellega seotud korra kohta. Kõnealused töötajad kinnitavad kirjalikult, et on kohaldatavad julgeolekusätted läbi lugenud ja mõistavad neid täielikult.

6.2. *Juhtkonna vastutus*

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

6.3. *Euroopa Parlamendi ametnike ja fraktsioonides töötavate muude Euroopa Parlamendi töötajate julgeolekustaatus*

Kehtestatakse kord, mis tagab, et juhul, kui mõne Euroopa Parlamendi ametniku või fraktsioonis töötava muu Euroopa Parlamendi töötaja kohta saadakse teada teda kahjustavat teavet, tehakse kindlaks, kas see isik puutub töö käigus kokku salastatud teabega või kas tal on juurdepääs kaitstud side- või infosüsteemidele, ja sellest teavitatakse Euroopa Parlamendi vastutavat teenistust. Kui liikmesriigi pädev julgeolekuasutus teeb kindlaks, et sellise isiku näol on tegemist ohuga julgeolekule, tagandatakse või kõrvaldatakse ta nende tööülesannete täitmiselt, millega seoses ta võib julgeoleku ohtu seada.

7. FÜÜSILINE JULGEOLEK

Füüsiline julgeolek tähendab füüsiliste ja tehniliste kaitsemeetmete kohaldamist, et takistada volitamata isikute juurdepääsu salastatud teabele.

7.1. ***Kaitsevajadus***

Salastatud teabe kaitsmise tagamiseks rakendatavate füüsiliste julgeolekumeetmete tase on proportsionaalne teabe ja materjali salastatuse taseme, mahu ja neile suunatud ohuga. Kõik salastatud teabe valdajad järgivad sellise teabe salastatuse taseme määramisel ühtseid tavasid ja peavad kaitset vajava teabe ja materjali säilitamisel, edastamisel ja hävitamisel kinni ühistest kaitsestandarditest.

7.2. ***Kontrollimine***

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

7.3. ***Hoonete julgeolek***

Hooned, kus hoitakse salastatud teavet või kaitstud side- ja infosüsteeme, peavad olema kaitstud loata juurdepääsu eest.

Salastatud teabe kaitsmise viis (nt trellitatud aknad, ukselukud, uksevalve, juurdepääsu kontrollimise automaatsüsteemid, turvakontrollid ja valvepatrullid, häiresüsteemid, sissetungimise avastamise süsteemid ja valvekoerad) sõltub järgmisest:

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

b) asjaomase teabe ja materjali turvakonteinerite kvaliteet ning

c) hoone füüsilised omadused ja asukoht.

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

7.4. ***Hädaolukorra lahendamise plaanid***

Salastatud teabe kaitsmiseks hädaolukorra puhul koostatakse üksikasjalikud plaanid.

8. **JULGEOLEKUTÄHISED, MÄRKED, MÄRKIMINE JA SALASTATUSE TASEMETE HALDAMINE**

8.1. ***Julgeolekutähised***

Lubatud on kasutada vaid käesoleva otsuse artikli 2 punktis d määratletud salastatuse tasemeid.

Salastatuse taseme kehtivuse piiramiseks (salastatud teabe puhul tähendab see automaatset salastatuse taseme alandamist või salastatuse kustutamist) võib kasutada kokkuleppelist julgeolekutähist.

Julgeolekutähiseid kasutatakse ainult koos salastatuse tasemega.

Julgeolekutähised on täpsemalt reguleeritud julgeolekuteates 2 ja need on määratletud käitlemisjuhendis.

8.2. ***Märked***

Märget kasutatakse selleks, et osutada konkreetsetele konfidentsiaalse teabe käitlemise juhistele. Märked võivad osutada ka konkreetses dokumendis käsitletavale valdkonnale või dokumendi levitamisele teadmisvajaduse põhjal, või (mittesalastatud teabe) embargo lõpu tähistamisele.

Märge ei ole salastatuse tase ja seda ei kasutata salastatuse taseme asemel.

Märked on täpsemalt reguleeritud julgeolekuteates 2 ja need on määratletud käitlemisjuhendis.

8.3. ***Salastatuse taseme märkimine ja julgeolekutähiste lisamine***

Salastatuse taseme märkimine ja julgeolekutähiste ning märgete lisamine toimub vastavalt julgeolekuteate 2 jaole E ja käitlemisjuhendile.

8.4. ***Salastatuse tasemete haldamine***

8.4.1 *Üldist*

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

Teabe salastamise ja salastatuse taseme alandamise või salastatuse kustutamise eest vastutab ainuisikuliselt teabe koostaja.

Euroopa Parlamendi ametnikud salastavad teabe, alandavad salastatuse taset või kustutavad salastatuse peasekretäri juhtnööride kohaselt või volitusel.

Salastatud dokumentide käsitlemise üksikasjalik kord on sätestatud viisil, et dokumentides sisalduvale teabele oleks tagatud piisav kaitse.

TRÈS SECRET UE / EU TOP SECRET salastatuse tasemega teabe koostamise volitusega isikute arv hoitakse võimalikult väiksena ning nende isikute nimed kantakse salastatud teabe üksuse koostatud nimekirja.

8.4.2 *Salastatuse taseme rakendamine*

Dokumendi salastatuse tase määratakse dokumendis sisalduva teabe tundlikkuse põhjal, võttes arvesse artikli 2 punktis d esitatud määratlusi. Salastamine peab toimuma õigesti ja kaalutletult.

Lisadega kirja või teate puhul on selle salastatuse tase vähemalt sama mis kõige kõrgema salastatuse tasemega lisal. Kui kiri või teade lahutatakse lisadest, peab koostaja selgelt osutama kirja või teate salastatuse tasemele.

Salastatava dokumendi koostaja järgib eespool sätestatud eeskirju ning väldib liiga kõrge ja liiga madala salastatuse taseme omistamist.

Ühe dokumendi eri leheküljed, lõiked, jaotised, lisad, manused ja täiendavad dokumendid võivad vajada eri salastatuse taset ning tuleb seega salastada sellele vastavalt. Kogu dokumendi salastatuse taseme määrab dokumendi kõige kõrgema salastatuse tasemega osa.

9. **KONTROLLIMINE**

Salastatud teabe kaitseks võetud julgeolekumeetmete regulaarset sisekontrolli teeb Euroopa Parlamendi turvaküsimuste ja riskihindamise direktoraat, kes võib paluda abi nõukogu või komisjoni julgeolekuasutuselt.

Liidu institutsioonide julgeolekuasutused ja pädevad teenistused võivad emma-kumma poole algatatud kokkulepitud protsessi raames hinnata vastastikku asjakohaste institutsioonidevaheliste kokkulepete kohaselt vahetatud salastatud teabe kaitsmiseks võetud julgeolekumeetmeid.

10. **SALASTATUSE JA MÄRKE KUSTUTAMISE MENETLUS**

10.1. Salastatud teabe üksus kontrollib oma registris sisalduvat konfidentsiaalset teavet ning taotleb dokumendi koostajalt nõusolekut dokumendi salastatuse või märke kustutamise kohta hiljemalt 25. aastal pärast dokumendi koostamise kuupäeva. Dokumente, mille salastatust või märget esimesel kontrollimisel ei kustutatud, kontrollitakse regulaarselt vähemalt iga viie aasta järel uuesti. Lisaks dokumentidele, mida säilitatakse turvaalas asuvates turvatud arhiivides ja mis on nõuetekohaselt salastatuks tunnistatud, võib salastatuse kustutamise menetlus hõlmata ka Euroopa Parlamendi organi või ametikandja sekretariaadis või Euroopa Parlamendi ajalooarhiivide eest vastutavas teenistuses hoitavat muud konfidentsiaalset teavet.

10.2 Dokumendi salastatuse või märke kustutamise otsuse teeb üldjuhul dokumendi koostaja ainuisikuliselt, kuid erandjuhul teeb ta otsuse koos teavet valdava parlamendi organi või ametikandjaga enne kui dokumendis olev teave antakse üle Euroopa Parlamendi ajalooarhiivide eest vastutavale teenistusele. Salastatud teabe salastatust või märget võib kustutada ainult siis, kui teabe koostaja on selleks andnud kirjaliku nõusoleku. Muu konfidentsiaalse teabe puhul otsustab dokumendi märke kustutamise teavet valdava parlamendi organi või ametikandja sekretariaat koos teabe koostajaga.

10.3. Salastatud teabe üksus vastutab teabe koostaja nimel selle eest, et dokumendi adressaate teavitatakse salastatuse taset ja märget puudutavatest muudatustest, ning adressaadid omakorda vastutavad selle eest, et muudatustest teavitatakse järgmisi adressaate, kellele nemad on saatnud kõnealuse dokumendi või selle koopia.

10.4. Salastatuse kustutamine ei mõjuta dokumendil esineda võivaid julgeolekutähiseid ega märkeid.

10.5. Salastatuse kustutamisel kriipsutatakse kõikide lehekülgede päises ja jaluses toodud esialgne salastatuse tase läbi. Dokumendi esimesel leheküljel või tiitellehel peab olema tempel koos viitega salastatud teabe üksusele. Märke kustutamisel kriipsutatakse kõikide lehekülgede päises toodud esialgne märge läbi.

10.6. Kustutatud salastatusega või kustutatud märkega dokumendi tekst peab olema registreeritud ja lisatud elektroonilisse andmebaasi või muusse sarnasesse süsteemi.

10.7. Dokumentide puhul, mille suhtes kehtib üksikisiku eraelu- ja isikupuutumatuse või füüsilise või juriidilise isiku ärihuvidega seotud erand või mis sisaldavad tundlikku teavet, kohaldatakse määruse (EMÜ, Euratom) nr 354/83 artiklit 2.

10.8. Lisaks punktidele 10.1. kuni 10.7. kohaldatakse järgmist korda:

a) salastatud teabe üksus konsulteerib kolmandate isikutega seotud dokumentide puhul enne salastatuse või märke kustutamise menetluse alustamist asjaomase kolmanda isikuga;

b) üksikisiku eraelu- ja isikupuutumatusega seotud erandi puhul võetakse salastatuse või märke kustutamisel eelkõige arvesse olenevalt asjaoludest kas asjaomase isiku nõusolekut või fakti, et asjaomast isikut ei ole võimalik tuvastada;

c) füüsilise või juriidilise isiku ärihuvidega seotud erandi puhul võib asjaomast isikut teavitada *Euroopa Liidu Teatajas* avaldatava teate kaudu, jättes võimalike tähelepanekute esitamiseks aega neli nädalat pärast teate avaldamise kuupäeva.

2. osa

JULGEOLEKUKONTROLLI KORD

11. **EUROOPA PARLAMENDI LIIKMETE JULGEOLEKUKONTROLLI KORD**

11.1. Euroopa Parlamendi liikmetele antakse CONFIDENTIEL UE / EU CONFIDENTIAL salastatuse tasemega või samaväärsele teabele juurdepääsuks luba vastavalt käesoleva lisa punktides 11.3 ja 11.4 osutatud menetlusele või käesoleva otsuse artikli 3 lõike 4 kohase, teabe mitteavaldamist kinnitava deklaratsiooni alusel.

11.2 Juurdepääsuks SECRET UE / EU SECRET ja TRÈS SECRET UE / EU TOP SECRET salastatuse tasemega või samaväärsele teabele peab Euroopa Parlamendi liikmetele olema antud luba punktides 11.3. ja 11.14. osutatud korra kohaselt.

11.3. Luba antakse ainult Euroopa Parlamendi liikmele, kes on läbinud liikmesriigi pädeva asutuse julgeolekukontrolli punktides 11.9 kuni 11.14 osutatud korra kohaselt. Parlamendiliikmetele loa andmise eest vastutab president.

11.4 President võib anda kirjaliku loa pärast seda, kui on saanud liikmesriigi pädeva asutuse seisukoha, mille aluseks on punktides 11.8. kuni 11.13. osutatud korra kohaselt teostatud julgeolekukontroll.

11.5. Euroopa Parlamendi turvaküsimuste ja riskihindamise direktoraat haldab ajakohastatud loetelu Euroopa Parlamendi liikmetest, kellele on antud luba, sealhulgas ajutine luba punkti 11.15. tähenduses.

11.6. Loa kehtivusaeg on viis aastat või tööülesannete kestus, milleks luba anti, sõltuvalt sellest, kumb on lühem. Kehtivusaega võib pikendada punktis 11.4. sätestatud korras.

11.7. President tühistab loa, kui ta leiab, et see on põhjendatud. Loa tühistamise otsus tehakse teatavaks asjaomasele Euroopa Parlamendi liikmele, kes võib taotleda, et president kuulaks ära tema selgitused enne loa tühistamist, ning liikmesriigi pädevale asutusele.

11.8. Julgeolekukontroll toimub koostöös asjaomase Euroopa Parlamendi liikmega ja presidendi taotlusel. Liikmesriigi pädev asutus julgeolekukontrolli teostamiseks on selle liikmesriigi vastav asutus, mille kodanik asjaomane parlamendiliige on.

11.9. Julgeolekukontrolli raames täidab Euroopa Parlamendi liige isikliku infolehe.

11.10. President märgib oma taotluses liikmesriigi pädevale asutusele, millise salastatuse tasemega teavet soovitakse Euroopa Parlamendi liikmele kättesaadavaks teha, et liikmesriigi pädev asutus saaks teostada julgeolekukontrolli.

11.11 Kogu liikmesriigi pädeva asutuse teostatava julgeolekukontrolli protsessi ja selle tulemuste suhtes kohaldatakse kõnealuses liikmesriigis kehtivaid asjakohaseid õigusnorme, sealhulgas kaebusi käsitlevaid õigusnorme.

11.12. Kui liikmesriigi pädeva asutuse seisukoht on positiivne, võib president kõnealusele Euroopa Parlamendi liikmele loa anda.

11.13. Liikmesriigi pädeva asutuse negatiivne seisukoht tehakse teatavaks asjaomasele Euroopa Parlamendi liikmele, kes võib taotleda, et president kuulaks ära tema selgitused. Kui president peab seda vajalikuks, võib ta paluda, et liikmesriigi pädev asutus annaks täiendavaid selgitusi. Kui negatiivne seisukoht kinnitatakse, siis luba ei anta.

11.14. Kõigile Euroopa Parlamendi liikmetele, kellele antakse luba punkti 11.3. tähenduses, antakse loa andmisel ja pärast seda korrapäraste ajavahemike järel vajalikke juhiseid salastatud teabe kaitsmise ja sellise kaitse tagamise vahendite kohta. Parlamendiliikmed kirjutavad alla deklaratsioonile, milles nad kinnitavad, et on nimetatud juhistega tutvunud.

11.15. Erandkorras võib president pärast liikmesriigi pädevale asutusele teatamist ja tingimusel, et nimetatud asutus ei ole sellele teatele ühe kuu jooksul reageerinud, anda Euroopa Parlamendi liikmele enne punktis 11.11. osutatud julgeolekukontrolli tulemuste selgumist kuni kuueks kuuks ajutise loa. Sel viisil antud ajutine luba ei anna juurdepääsu TRÈS SECRET UE / EU TOP SECRET salastatuse tasemega ega samaväärsele teabele.

12. EUROOPA PARLAMENDI AMETNIKE JA FRAKTSIOONIDES TÖÖTAVATE MUUDE EUROOPA PARLAMENDI TÖÖTAJATE JULGEOLEKUKONTROLLI KORD

12.1. Juurdepääs salastatud teabele antakse ainult sellistele Euroopa Parlamendi ametnikele ja fraktsioonides töötavatele muudele Euroopa Parlamendi töötajatele, kes oma ülesannete ja üksuse vajaduste tõttu peavad sellist teavet teadma või kasutama.

12.2. Juurdepääsuks CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE / EU SECRET ja TRÈS SECRET UE / EU TOP SECRET salastatuse tasemega või samaväärsele teabele peavad Euroopa Parlamendi ametnikud ja muud asjaomases fraktsioonis töötavad Euroopa Parlamendi töötajad saama loa punktides 12.3. ja 12.4. sätestatud korra kohaselt.

12.3. Luba antakse ainult punktis 12.1. osutatud isikutele, kes on läbinud liikmesriigi pädeva asutuse julgeolekukontrolli punktides 12.9. kuni 12.14. osutatud korra kohaselt. Euroopa Parlamendi ametnikele ja fraktsioonides töötavatele muudele Euroopa Parlamendi töötajatele loa andmise eest vastutab peasekretär.

12.4. Peasekretär annab kirjaliku loa pärast seda, kui on saanud liikmesriigi pädeva asutuse seisukoha, mille aluseks on punktides 12.8. kuni 12.13. osutatud korra kohaselt teostatud julgeolekukontroll.

12.5. Euroopa Parlamendi turvaküsimuste ja riskihindamise direktoraat haldab Euroopa Parlamendi teenistuste esitatud ajakohastatud loetelu kõikidest ametikohtadest, mille puhul on nõutav julgeolekukontrolli läbimine, ja kõikidest isikutest, kellele on antud luba, sealhulgas ajutine luba punkti 12.15. tähenduses.

12.6. Loa kehtivusaeg on viis aastat või tööülesannete kestus, milleks luba anti, sõltuvalt sellest, kumb on lühem. Kehtivusaega võib pikendada punktis 12.4. osutatud korras.

12.7. Peasekretär tühistab loa, kui ta leiab, et see on põhjendatud. Loa tühistamise otsus tehakse teatavaks asjaomasele Euroopa Parlamendi ametnikule või fraktsioonis töötavale muule Euroopa Parlamendi töötajale, kes võib taotleda, et peasekretär kuulaks ära tema selgitused enne loa tühistamist, ning liikmesriigi pädevale asutusele.

12.8. Julgeolekukontroll toimub koostöös asjaomase Euroopa Parlamendi ametnikuga või mõne muu asjaomases fraktsioonis töötava Euroopa Parlamendi töötajaga ja peasekretäri taotlusel. Liikmesriigi pädev asutus julgeolekukontrolli teostamiseks on selle liikmesriigi vastav asutus, mille kodanik kõnealune isik on. Kui see on riigisiseste õigusnormide kohaselt lubatud, võib liikmesriigi pädev asutus teostada julgeolekukontrolli mittekodanike suhtes, kes vajavad juurdepääsu CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE / EU SECRET või TRÈS SECRET UE / EU TOP SECRET salastatuse tasemega teabele.

12.9. Julgeolekukontrolli raames täidab Euroopa Parlamendi ametnik või fraktsioonis töötav muu Euroopa Parlamendi töötaja isikliku infolehe.

12.10. Peasekretär märgib oma taotluses liikmesriigi pädevale asutusele, millise salastatuse tasemega teavet soovitakse Euroopa Parlamendi ametnikule või mõnele muule asjaomases fraktsioonis töötavale Euroopa Parlamendi töötajale kättesaadavaks teha, et liikmesriigi pädev asutus saaks teostada julgeolekukontrolli ja esitada oma seisukoha seoses kõnealusele isikule antava loa tasemega.

12.11. Kogu liikmesriigi pädeva asutuse teostatava julgeolekukontrolli protsessi ja selle tulemuste suhtes kohaldatakse kõnealuses liikmesriigis kehtivaid asjakohaseid õigusnorme, sealhulgas kaebusi käsitlevaid õigusnorme.

12.12. Kui liikmesriigi pädeva asutuse seisukoht on positiivne, võib peasekretär kõnealusele Euroopa Parlamendi ametnikule või mõnele muule asjaomases fraktsioonis töötavale Euroopa Parlamendi töötajale loa anda.

12.13. Liikmesriigi pädeva asutuse negatiivne seisukoht tehakse teatavaks asjaomasele Euroopa Parlamendi ametnikule või mõnele muule asjaomases fraktsioonis töötavale Euroopa Parlamendi töötajale, kes võib taotleda, et peasekretär kuulaks ära tema selgitused. Kui peasekretär peab seda vajalikuks, võib ta paluda, et liikmesriigi pädev asutus annaks täiendavaid selgitusi. Kui negatiivne seisukoht kinnitatakse, siis luba ei anta.

12.14. Kõigile Euroopa Parlamendi ametnikele ja fraktsioonides töötavatele muudele Euroopa Parlamendi töötajatele, kellele antakse luba punktide 12.4. ja 12.5. tähenduses, antakse loa andmisel ja pärast seda korrapäraste ajavahemike järel vajalikke juhiseid salastatud teabe kaitsmise ja sellise kaitse tagamise vahendite kohta. Euroopa Parlamendi ametnikud ja fraktsioonides töötavad muud töötajad kirjutavad alla deklaratsioonile, milles nad kinnitavad, et on nimetatud juhistega tutvunud ja kohustuvad neid järgima.

12.15. Erandkorras võib peasekretär pärast liikmesriigi pädevale asutusele teatamist ja tingimusel, et nimetatud asutus ei ole sellele teatele ühe kuu jooksul reageerinud, anda Euroopa Parlamendi ametnikule või fraktsioonis töötavale muule Euroopa Parlamendi töötajale enne punktis 12.11. osutatud julgeolekukontrolli tulemuste selgumist kuni kuueks kuuks ajutise loa. Ajutine luba ei anna juurdepääsu TRÈS SECRET UE / EU TOP SECRET salastatuse tasemega ega samaväärsele teabele.

II LISA

SISSEJUHATUS

Nende sätetega kehtestatakse julgeolekuteated, millega tagatakse konfidentsiaalse teabe turvaline käsitlemine ja haldamine Euroopa Parlamendi poolt ning reguleeritakse seda. Julgeolekuteated koos käitlemisjuhendiga moodustavad Euroopa Parlamendi teabeturbe juhtimissüsteemi, millele on osutatud käesoleva otsuse artikli 3 lõikes 2:

JULGEOLEKUTEADE 1

Julgeolekukorraldus Euroopa Parlamendis konfidentsiaalse teabe kaitseks

JULGEOLEKUTEADE 2

Konfidentsiaalse teabe haldamine

JULGEOLEKUTEADE 3

Konfidentsiaalse teabe töötlemine automatiseeritud side- ja infosüsteemide abil

JULGEOLEKUTEADE 4

Füüsiline julgeolek

JULGEOLEKUTEADE 5

Tööstusjulgeolek

JULGEOLEKUTEADE 6

Julgeolekunõuete rikkumine ning konfidentsiaalse teabe kadumine või ohtusattumine

JULGEOLEKUTEADE 1

JULGEOLEKUKORRALDUS EUROOPA PARLAMENDIS KONFIDENTSIAALSE TEABE KAITSEKS

1. Peasekretär vastutab käesoleva otsuse üldise ja järjepideva rakendamise eest.

Peasekretär võtab kõik vajalikud meetmed tagamaks, et konfidentsiaalse teabe käitlemisel ja säilitamisel Euroopa Parlamendi ruumides järgivad käesolevat otsust Euroopa Parlamendi liikmed, ametnikud, fraktsioonide heaks töötavad muud Euroopa Parlamendi töötajad ning töövõtjad.

2. Julgeolekuasutuseks on peasekretär. Seoses sellega täidab peasekretär järgmisi ülesandeid:

2.1. koordineerib kõiki julgeolekuküsimusi seoses Euroopa Parlamendi tegevusega, mis on seotud konfidentsiaalse teabe kaitsega;

2.2. kiidab heaks turvaalade ja turvatud lugemissaalide loomise ning turvalise varustuse paigaldamise;

2.3. rakendab otsuseid, mis lubavad käesoleva otsuse artikli 6 kohaselt Euroopa Parlamendil edastada salastatud teavet kolmandatele osapooltele;

2.4. uurib *prima facie* Euroopa Parlamendis toimunud konfidentsiaalse teabe lekkeid või tellib vastava uurimise — koostöös Euroopa Parlamendi presidendiga, juhul kui asjaga on seotud Euroopa Parlamendi liige;

2.5. on tihedas kontaktis liidu teiste institutsioonide julgeolekuasutuste ning liikmesriikide riiklike julgeolekuasutustega, et tagada salastatud teabega seotud julgeolekupoliitika optimaalne koordineerimine;

2.6. teostab Euroopa Parlamendi julgeolekupoliitika ja -korra üle pidevalt järelevalvet ning esitab selle põhjal asjakohaseid soovitusi;

2.7. teatab riiklikule julgeolekuasutusele, mis on viinud läbi I lisa 2. osa punkti 11.3 kohase julgeolekukontrolli, kahjustavast teabest, mis võib seda asutust mõjutada.

3. Kui asjaga on seotud Euroopa Parlamendi liikmed, täidab peasekretär oma ülesandeid tihedas koostöös Euroopa Parlamendi presidendiga.

4. Punktide 2 ja 3 kohaste ülesannete täitmisel abistavad peasekretäri asepeasekretär, turvaküsimuste ja riskihindamise direktoraat, infotehnoloogia direktoraat ja salastatud teabe üksus.

4.1. Turvaküsimuste ja riskihindamise direktoraat vastutab isiklike kaitsemeetmete eest ning eelkõige julgeolekukontrolli korra eest, nagu on sätestatud I lisa 2. osas. Turvaküsimuste ja riskihindamise direktoraat teeb ka järgmist:

a) on teiste liidu institutsioonide julgeolekuasutuste ning riiklike julgeolekuasutuste kontaktpunkt küsimustes, mis on seotud Euroopa Parlamendi liikmete, ametnike ja fraktsioonides töötavate muude töötajate julgeolekukontrolli korraga;

b) annab vajalikku üldist julgeolekuteavet kohustuse kohta kaitsta salastatud teavet ning selle kohustuse täitmata jätmise tagajärgede kohta;

c) jälgib Euroopa Parlamendi hoonete turvaalade ja turvatud lugemissaalide toimimist, vajaduse korral koostöös liidu teiste institutsioonide julgeolekuasutuste ja liikmesriikide riiklike julgeolekuasutustega;

d) kontrollib koostöös liidu teiste institutsioonide julgeolekuasutuste ja liikmesriikide riiklike julgeolekuasutustega salastatud teabe haldamise ja säilitamise korda, Euroopa Parlamendi hoonete turvaalasid ja turvatud lugemissaale, kus toimub salastatud teabe käitlemine;

e) teeb peasekretärile ettepaneku asjakohase käitlemisjuhendi kohta.

4.2. Infotehnoloogia direktoraat vastutab Euroopa Parlamendis konfidentsiaalse teabe käitlemise eest läbi turvalise IT süsteemi.

4.3. Salastatud teabe üksus täidab järgmisi ülesandeid:

a) teeb tihedas koostöös turvaküsimuste ja riskihindamise direktoraadi ja infotehnoloogia direktoraadi ning liidu teiste institutsioonide julgeolekuasutustega kindlaks julgeolekuvajadused konfidentsiaalse teabe tõhusaks kaitseks;

b) teeb kindlaks Euroopa Parlamendis toimuva konfidentsiaalse teabe haldamise ja säilitamise kõik aspektid, nagu on sätestatud käitlemisjuhendis;

c) korraldab turvaala toimimist;

d) korraldab konfidentsiaalse teabe haldamist ja sellega tutvumist turvaalal või salastatud teabe üksuse turvatud lugemissaalis vastavalt käesoleva otsuse artikli 7 lõigetele 2 ja 3;

e) haldab salastatud teabe üksuse registrit;

f) annab julgeolekuasutusele aru iga tõendatud või oletatava julgeolekunõuete rikkumise ning salastatud teabe üksuses säilitatava ja turvaalal või salastatud teabe üksuse turvatud lugemissaalis hoitava konfidentsiaalse teabe kadumise või ohtusattumise juhtumi kohta.

5. Lisaks sellele määrab peasekretär julgeolekuasutusena järgmised asutused:

a) turvalisuse akrediteerimise asutus;

b) infokindluse rakendusasutus;

c) krüptomaterjalide jaotamise asutus;

d) TEMPEST-asutus;

e) infokindluse asutus;

Kõnealuste ülesannete täitmine ei nõua eraldi struktuuriüksuste moodustamist. Neil on eraldi volitused. Siiski võib kõnealuseid toiminguid ja nendega kaasnevat vastutust ühendada või integreerida samasse struktuuriüksusesse või jagada erinevatesse struktuuriüksustesse, tingimusel et välditakse huvide konflikte ja ülesannete dubleerimist.

6. Turvalisuse akrediteerimise asutus annab nõu kõikides turvaküsimustes, mis on seotud iga infotehnoloogiasüsteemi ja -võrgu akrediteerimisega Euroopa Parlamendis, ning teeb muu hulgas järgmist:

6.1. tagab, et side- ja infosüsteem vastab asjaomasele julgeolekupoliitikale ja julgeolekusuunistele; annab side- ja infosüsteemile heakskiitmise teatise kinnitamaks, et süsteemi töökeskkonnas võib käidelda kindlaksmääratud salastatuse tasemega salastatud teavet; määrab kindlaks akrediteerimise tingimused ning kriteeriumid, mille alusel nõutakse uue heakskiidu andmist;

6.2. kehtestab vastavalt asjaomastele poliitikatele turvalisuse akrediteerimise protsessi, milles on selgelt esitatud turvalisuse akrediteerimise asutuse pädevusalasse kuuluvate side- ja infosüsteemide heakskiitmise tingimused;

6.3. koostab turvalisuse akrediteerimise strateegia, milles on esitatud akrediteerimisprotsessi põhjalikkuse aste, mis on vastavuses nõutava kindluse tasemega;

6.4. vaatab läbi ja kinnitab turvadokumentatsiooni, sealhulgas riskijuhtimise ja jääkriski teatised, turvanõuete rakendamise kontrollimise dokumentatsiooni ja turvanõuete rakendamise korra, ning tagab dokumentatsiooni vastavuse Euroopa Parlamendi julgeolekueeskirjadele ja -poliitikale;

6.5. kontrollib turvameetmete rakendamist seoses side- ja infosüsteemidega, teostades või rahastades turvaanalüüse, kontrolli või ülevaateid;

6.6. määrab kindlaks julgeolekualased nõuded (nt juurdepääsu lubade tasemed) side- ja infosüsteemi suhtes tundlike ametikohtade jaoks;

6.7. kiidab heaks side- ja infosüsteemi ühendamine muu side- ja infosüsteemiga või vajaduse korral osaleb ühises heakskiitmises;

6.8. kiidab heaks salastatud teabe turvaliseks käitlemiseks ja kaitseks ette nähtud tehniliste seadmete julgeolekustandardid;

6.9. tagab, et Euroopa Parlamendis kasutatavad krüptovahendid oleksid ELi heakskiidetud vahendite nimekirjas, ning

6.10. konsulteerib süsteemi tarnija, turvalisuse eest vastutajate ning kasutajate esindajatega turvariski juhtimise küsimustes, eelkõige jääkriski ning heakskiitmise teatise tingimuste osas.

7. Infokindluse rakendusasutus täidab järgmisi ülesandeid:

7.1. töötab välja turvadokumentatsiooni kooskõlas julgeolekupoliitika ja -suunistega, eelkõige jääkriski käsitleva avalduse, turvanõuete rakendamise korra ning side- ja infosüsteemi akrediteerimise protsessi raames koostatava krüptoplaani;

7.2. osaleb süsteemispetsiifiliste tehnilise turvalisuse meetmete, seadmete ja tarkvara valimises ja katsetamises, et teostada järelevalvet nende rakendamise üle ja tagada nende turvaline paigaldamine, seadistamine ja haldamine kooskõlas asjakohase turvadokumentatsiooniga;

7.3. teostab järelevalvet turvalisusega seotud töökorra rakendamise ja kohaldamise üle ning vajaduse korral võib delegeerida turvalisusega seotud töökohustusi süsteemi omanikule, salastatud teabe üksusele;

7.4. haldab ja töötleb krüptovahendeid, tagab krüpto- ja kontrollitavate vahendite säilitamise ning vajaduse korral tagab krüpteerimismuutujate genereerimise;

7.5. teostab turvaanalüüsi läbivaatamist ja testimist, eelkõige selleks, et koostada turvalisuse akrediteerimise asutuse nõudel asjakohaseid riskiaruandeid;

7.6. pakub side- ja infosüsteemispetsiifilist infokindluse alast koolitust;

7.7. rakendab ja kasutab side- ja infosüsteemispetsiifilisi turvameetmeid.

8. Krüptomaterjalide jaotamise asutus täidab järgmisi ülesandeid:

8.1. haldab ELi krüptomaterjali ja peab selle üle arvet;

8.2. tagab asjakohaste protseduuride täitmise ja kavade loomise tihedas koostöös turvalisuse akrediteerimise asutusega ELi krüptomaterjali üle arvepidamise, turvalise käitlemise, säilitamise ja levitamise tagamiseks; ning

8.3. tagab ELi krüptomaterjalide neid kasutavatele isikutele või teenistustele edastamise või selliste materjalide neid kasutavatelt isikutelt või teenistustelt vastuvõtmise.

9. TEMPEST-asutus vastutab selle eest, et side- ja infosüsteemid oleksid kooskõlas TEMPESTi poliitika ja käitlemisjuhendiga. Asutus kiidab heaks TEMPESTi vastumeetmed seadmete ja toodete jaoks, et kaitsta kindlaksmääratud salastatuse tasemel salastatud teavet tema töökeskkonnas.

10. Infokindluse asutus vastutab Euroopa Parlamendis konfidentsiaalse teabe haldamise ja käitlemise kõikide aspektide eest ning täidab eelkõige järgmisi ülesandeid:

10.1 töötab välja infokindluse julgeolekupoliitika ja -suunised ning jälgib nende tulemuslikkust ja asjakohasust;

10.2. kaitseb ja haldab krüptovahenditega seotud tehnilist teavet;

10.3. tagab salastatud teabe kaitsmiseks valitud infokindluse meetmete vastavuse nende kõlblikkust ja valikut reguleerivale asjakohasele poliitikale;

10.4. tagab, et krüptovahendid valitakse vastavalt nende kõlblikkuse ja valiku alasele poliitikale;

10.5. konsulteerib infokindluse julgeoleku osas süsteemi tarnija, turvalisuse eest vastutajate ning kasutajate esindajatega.

JULGEOLEKUTEADE 2

KONFIDENTSIAALSE TEABE HALDAMINE

A. **SISSEJUHATUS**

1. Käesolev julgeolekuteade sisaldab sätteid konfidentsiaalse teabe haldamise kohta parlamendis.

2. Konfidentsiaalse teabe koostamisel hindab koostaja konfidentsiaalsuse taset ning langetab käesolevas julgeolekuteates sätestatud põhimõtete kohaselt otsuse asjaomase teabe salastamise või märgistamise kohta.

B. **ELi SALASTATUD TEABE KLASSIFIKATSIOON**

3. Otsus dokumendi salastatuse kohta tehakse enne selle koostamist. Seepärast hõlmab teabe salastamine ELi salastatud teabena selle konfidentsiaalsuse taseme eelnevat hindamist ning koostaja poolset otsust, mille kohaselt sellise teabe loata avaldamine võib eri määral kahjustada Euroopa Liidu või ühe või mitme liikmesriigi või üksikisiku huve.

4. Kui otsus teabe salastamise kohta on tehtud, viiakse läbi teine eelhindamine sobiva salastatuse taseme määramiseks. Dokumendi salastatuse tase määratakse dokumendis sisalduva teabe tundlikkuse põhjal.

5. Vastutus teabe salastamise eest lasub ainuisikuliselt koostajal. Euroopa Parlamendi ametnikud salastavad teabe peasekretäri juhtnööride kohaselt või volitusel.

6. Salastamist kasutatakse õigesti ja kaalutletult. Salastatava dokumendi koostaja väldib liiga kõrge ja liiga madala salastatuse taseme omistamist.

7. Teabele määratud salastatuse tase määrab kindlaks teabele töötajatega seotud julgeoleku, füüsilise julgeoleku, menetlusliku julgeoleku ja infokindluse valdkonnas pakutava kaitse taseme.

8. Salastamist vajav teave märgistatakse salastatud teabena ning seda käideldakse salastatud teabena selle füüsilisest vormist hoolimata. Teabe saajaid teavitatakse selgesõnaliselt teabe salastatusest, tehes seda kas salastusmärke abil (kui teave esitatakse kirjalikult, olenemata sellest, kas see esitatakse paberil või side- ja infosüsteemis) või avalduse vormis (kui teave esitatakse suuliselt, näiteks vestluse või kinnise koosoleku ajal). Salastatud materjal on füüsiliselt märgistatud viisil, mis võimaldab kergesti tuvastada selle salastatust.

9. ELi salastatud teavet elektroonilisel kujul võib koostada ainult akrediteeritud side- ja infosüsteemi abil. Salastatud teave ise ning failinimi ja andmekandja (juhul kui see on väline, nt CD-plaat või USB-mälupulk) kannavad asjaomast salastusmärget.

10. Teave salastatakse kohe selle koostamisel. Näiteks salastamist vajavat teavet sisaldavad isiklikud märkmed, kavandid või e-posti sõnumid tuleb koheselt märgistada ELi salastatud teabena ning neid tuleb koostada ja käidelda kooskõlas käesoleva otsuse ja käitlemisjuhendi nõuetega füüsiliste ja tehniliste kaitsemeetmete kohta. Selline teave võib seejärel kujuneda ametlikuks dokumendiks, mida omakorda asjakohaselt märgistatakse ja käideldakse. Ametliku dokumendi koostamise käigus võib ilmneda vajadus see ümber hinnata ning vastavalt sellele omistada kõrgem või madalam salastatuse tase.

11. Koostaja võib otsustada omistada standardse salastatuse taseme teabekategooriatele, mida ta regulaarselt koostab. Kuid koostaja peab tagama, et ta ei omista seda tehes teabele süsteemselt liiga kõrget või liiga madalat salastatuse taset.

12. ELi salastatud teave tähistatakse salastusmärkega, mis vastab tema salastatuse tasemele.

B.1. ***Salastatuse tasemed***

13. ELi salastatud teave liigitatakse ühte järgmistest tasemetest:

— TRÈS SECRET UE / EU TOP SECRET, nagu on määratletud käesoleva otsuse artikli 2 punktis d, juhul kui teabe ohtusattumine võiks tõenäoliselt:

a) seada otsesesse ohtu liidu või ühe või mitme liikmesriigi või kolmanda riigi või rahvusvahelise organisatsiooni sisemise stabiilsuse;

b) tekitada erakordselt tõsist kahju suhetele kolmandate riikide või rahvusvaheliste organisatsioonidega;

c) põhjustada otseselt hulgaliselt surmajuhtumeid;

d) tekitada erakordselt tõsist kahju liikmesriikide või muude osaliste poolt lähetatud töötajate töö tulemuslikkusele või nende julgeolekule või eriti väärtuslike julgeoleku- või luureoperatsioonide jätkuvale tulemuslikkusele; või

e) tekitada tõsist pikaajalist kahju liidu või selle liikmesriikide majandusele;

— SECRET UE / EU SECRET, nagu on määratletud käesoleva otsuse artikli 2 punktis d, juhul kui teabe ohtusattumine võiks tõenäoliselt:

a) suurendada märkimisväärselt rahvusvahelisi pingeid;

b) halvendada tõsiselt suhteid kolmandate riikide ja rahvusvaheliste organisatsioonidega;

c) seada otseselt ohtu elu või kahjustada tõsiselt avalikku korda või üksikisikute julgeolekut või vabadust;

d) kahjustada olulisi kaubanduslikke või poliitilisi läbirääkimisi, tekitades märkimisväärseid toimimisprobleeme liidule või liikmesriikidele;

e) tekitada tõsist kahju liikmesriikide operatiivsele julgeolekule või väga väärtuslike julgeoleku- või luureoperatsioonide tulemuslikkusele;

f) tekitada märkimisväärset materiaalset kahju liidu või liikmesriigi finants-, rahandus-, majandus- ja kaubandushuvidele;

g) õõnestada märkimisväärselt suurorganisatsioonide või ettevõtete rahalist elujõudu; või

h) takistada tõsiselt liidu põhimõtete väljatöötamist või toimimist, millel on rasked majanduslikud, kaubanduslikud või rahalised tagajärjed;

— CONFIDENTIEL UE / EU CONFIDENTIAL, nagu on määratletud käesoleva otsuse artikli 2 punktis d, juhul kui teabe ohtusattumine võiks tõenäoliselt:

a) kahjustada oluliselt diplomaatilisi suhteid, nt anda alust ametlikuks protestiks või muudeks sanktsioonideks;

b) seada ohtu üksikisikute julgeoleku või vabaduse;

c) seada ohtu kaubanduslike või poliitiliste läbirääkimiste tulemuse; tekitada toimimisprobleeme liidule või liikmesriikidele;

d) tekitada kahju liikmesriikide operatiivsele julgeolekule või julgeoleku- või luureoperatsioonide tulemuslikkusele;

e) õõnestada märkimisväärselt suurorganisatsioonide või ettevõtete rahalist elujõudu;

f) takistada kuritegude või terroriaktide uurimist või soodustada nende toimepanekut;

g) olla märkimisväärses vastuolus liidu või selle liikmesriikide finants-, rahandus-, majandus- ja kaubandushuvidega;

h) takistada tõsiselt liidu põhimõtete väljatöötamist või toimimist, millel on rasked majanduslikud, kaubanduslikud või rahalised tagajärjed;

— RESTREINT UE / EU RESTRICTED, nagu on määratletud käesoleva otsuse artikli 2 punktis d, juhul kui teabe ohtusattumine võiks tõenäoliselt:

a) kahjustada liidu üldisi huve;

b) kahjustada diplomaatilisi suhteid;

c) tekitada üksikisikutele või äriühingutele märkimisväärseid ebameeldivusi;

d) seada liidu või selle liikmesriigid ebasoodsasse olukorda kaubanduslikel või poliitilistel läbirääkimistel;

e) raskendada tegeliku julgeoleku säilitamist liidus või liikmesriikides;

f) takistada liidu põhimõtete tulemuslikku väljatöötamist või toimimist;

g) õõnestada liidu ja selle tegevuse nõuetekohast juhtimist;

h) rikkuda Euroopa Parlamendi poolt võetud kohustusi säilitada kolmandate isikute esitatud teabe salastatus;

i) rikkuda õiguspäraseid piiranguid teabe avaldamise kohta;

j) tekitada üksikisikutele või äriühingutele rahalist kahju või soodustada sobimatu kasu või eelise saamist;

k) piirata kuritegude uurimist või soodustada nende toimepanekut.

B.2. ***Salastatuse taseme omistamine tervikkogumitele, saatemärkustele ja väljavõtetele***

14. Lisadega kirja või teate puhul määrab selle salastatuse taseme kõige kõrgema salastatuse tasemega lisa. Kui kiri või teade lahutatakse lisadest, peab koostaja selgelt osutama kirja või teate salastatuse tasemele. Kui teadet või kirja ei ole vaja salastada, sisaldab see järgmist lauset: „Kui kiri või teade lahutatakse lisadest, ei ole see salastatud.”.

15. Erinevatel tasemetel salastatud osi sisaldavad dokumendid või failid liigendatakse võimaluse korral selliselt, et nende erinevatel tasemetel salastatud osad on kergesti tuvastatavad ja vajaduse korral eraldatavad ülejäänud dokumendist või failist. Dokumendi või faili üldine salastatuse tase on vähemalt sama kõrge kui selle kõige kõrgema salastatuse tasemega osal.

16 Ühe dokumendi eri leheküljed, lõiked, jaotised, lisad, manused ja täiendavad dokumendid võivad vajada eri salastatuse taset ning tuleb seega salastada sellele vastavalt. ELi salastatud teavet sisaldavates dokumentides võib lühemate kui ühe lehekülje pikkuste tekstilõikude salastatuse taseme märkimisel kasutada standardlühendeid.

17. Erinevatest allikatest pärineva teabe koondamisel vaadatakse lõpptulemus üle, et määrata kindlaks üldine salastatuse tase, sest vajalikuks võib osutuda dokumendi üksikosadele omistatust kõrgem salastatuse tase.

C. **MUU KONFIDENTSIAALNE TEAVE**

18. Muu konfidentsiaalne teave märgistatakse vastavalt käesoleva julgeolekuteate punktile E ja käitlemisjuhendile.

D. **KONFIDENTSIAALSE TEABE KOOSTAMINE**

19. Konfidentsiaalset teavet võivad koostada ainult käesolevas otsuses kindlaks määratud või julgeolekuasutuselt loa saanud isikud.

20. Konfidentsiaalset teavet ei tohi lisada interneti ega sisevõrgu dokumendihaldussüsteemidesse.

D.1. ***ELi salastatud teabe koostamine***

21. Selleks, et koostada ELi salastatud teavet CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE / EU SECRET või TRÈS SECRET UE / EU TOP SECRET salastatuse tasemega, peab asjaomasel isikul olema selleks käesolevast otsusest tulenev õigus või otsuse artikli 4 lõike 1 kohaselt väljastatud luba.

22. CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE / EU SECRET või TRÈS SECRET UE / EU TOP SECRET salastatuse tasemega ELi salastatud teavet koostatakse ainult turvaalal.

23. ELi salastatud teabe koostamise suhtes kohaldatakse järgmisi nõudeid:

a) igale leheküljele märgitakse selgelt kehtiv salastatuse tase;

b) igale leheküljele märgitakse lehekülgenumber ja lehekülgede koguarv;

c) dokumendi esimesel leheküljel peab olema kirjas viitenumber ja teema, mis iseenesest ei ole salastatud teave, välja arvatud juhul, kui see on sellisena tähistatud;

d) dokumendi esimesel leheküljel peab olema kuupäev;

e) CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE / EU SECRET või TRÈS SECRET UE / EU TOP SECRET salastatuse tasemega dokumendi esimesel leheküljel peab olema lisade ja manuste nimekiri;

f) CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE / EU SECRET või TRÈS SECRET UE / EU TOP SECRET salastatuse tasemega dokumendi igal leheküljel peab olema koopia number, kui antakse välja mitu koopiat. Iga koopia esimesel leheküljel peab olema koopiate ja lehekülgede koguarv ning

g) kui dokument sisaldab viiteid liidu teistest institutsioonidest saadud dokumentidele, mis sisaldavad salastatud teavet, või kui dokument sisaldab nendest dokumentidest tulenevat salastatud teavet, peab dokument olema sama salastatuse tasemega nagu need dokumendid ning dokumenti ei tohi ilma koostaja kirjaliku nõusolekuta edastada teistele isikutele peale nende, kelle nimed on algse dokumendi või salastatud teavet sisaldavate dokumentide saajate nimekirjas.

24. Koostaja säilitab kontrolli enda koostatud ELi salastatud teabe üle. Tema eelnev kirjalik nõusolek on nõutav, enne kui:

a) ELi salastatud teabe salastatuse taset alandatakse või salastatus kustutatakse;

b) ELi salastatud teave leiab kasutamist muudel kui koostaja määratud eesmärkidel;

c) ELi salastatud teave avalikustatakse kolmandale riigile või rahvusvahelisele organisatsioonile;

d) ELi salastatud teave avaldatakse mis tahes isikule, institutsioonile, riigile või rahvusvahelisele organisatsioonile peale adressaatide, kellele koostaja on algselt andnud loa kõnealuse teabega tutvuda;

e) ELi salastatud teave avalikustatakse kolmandas riigis asuvale töövõtjale või võimalikule töövõtjale;

f) ELi salastatud teavet kopeeritakse või tõlgitakse, kui teave on TRÈS SECRET UE / EU TOP SECRET salastatuse tasemega;

g) ELi salastatud teave hävitatakse.

D.2. ***Muu konfidentsiaalse teabe koostamine***

25. Peasekretär võib julgeolekuasutusena otsustada, kas lubada üksusel, teenistusel ja/või isikul muu konfidentsiaalse teabe koostamist.

26. Muu konfidentsiaalne teave on tähistatud ühe käitlemisjuhendis määratletud märkega.

27. Muu konfidentsiaalse teabe koostamise suhtes kohaldatakse järgmisi nõudeid:

a) märge peab olema dokumendi esimese lehekülje ülaservas;

b) igale leheküljele märgitakse leheküljenumber ja lehekülgede koguarv;

c) dokumendi esimesel leheküljel peab kirjas olema viitenumber ja teema;

d) dokumendi esimesel leheküljel peab olema kuupäev ning

e) dokumendi viimasel leheküljel peab olema kõikide lisade ja manuste nimekiri.

28. Muu konfidentsiaalse teabe koostamise suhtes kohaldatakse käitlemisjuhendis sätestatud eeskirju ja menetlusi.

E. **JULGEOLEKUTÄHISED JA -MÄRKED**

29. Dokumentidel olevate julgeolekutähiste ja -märgete eesmärk on kontrollida teabevoogu ning piirata juurdepääsu konfidentsiaalsele teabele teadmisvajaduse põhimõttest lähtudes.

30. Julgeolekutähiste ja/või -märgete kasutamisel või lisamisel tuleb vältida segiajamist ELi salastatud teabe salastatuse tasemetega: RESTREINT UE / EU RESTRICTED, CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE / EU SECRET, TRÈS SECRET UE / EU TOP SECRET.

31. Julgeolekutähiste ja -märgete kasutamist reguleerivad eeskirjad koos Euroopa Parlamendi heakskiidetud julgeolekumärgetega kehtestatakse käitlemisjuhendis.

E.1. ***Julgeolekutähised***

32. Julgeolekutähiseid võib kasutada ainult koos salastatuse tasemetega ning neid ei lisata dokumentidele eraldi. Julgeolekutähise võib lisada ELi salastatud teabele:

a) salastatuse taseme kehtivuse piiramiseks (salastatud teabe puhul tähendab see automaatset salastatuse taseme alandamist või salastatuse kustutamist);

b) asjaomase ELi salastatud teabe levitamise piiramiseks;

c) eraldi käitlemiskorra kehtestamiseks lisaks vastava salastatuse taseme käitlemiskorrale.

33. ELi salastatud teavet sisaldavate dokumentide käitlemise ja hoidmise suhtes kohaldatav erikontroll toob kõigile asjaosalistele kaasa lisakoormuse. Sellega seotud töö minimeerimiseks näeb hea tava sellise dokumendi koostamise puhul ette kehtestada salastatusele tähtaeg, pärast mida dokumendi salastatuse taset automaatselt alandatakse või salastatus kustutatakse.

34. Kui dokumendis käsitletakse konkreetset töövaldkonda ning selle levikut on vaja piirata ja/või selle suhtes tuleb kohaldada erilist käitlemiskorda, võib dokumendi salastatuse tasemele lisada vastava avalduse, mis aitab tuvastada dokumendi sihtrühma.

E.2. ***Märked***

35. Märked ei kujuta endast salastatuse taset. Nende eesmärk on anda üksnes konkreetsed juhised dokumendi käitlemiseks ning neid ei kasutata dokumendi sisu kirjeldamiseks.

36. Märkeid võib kasutada dokumendil eraldi või koos salastatuse tasemega.

37. Üldreeglina kasutatakse märkeid teabe puhul, mis on hõlmatud ametisaladusega (osutatud Euroopa Liidu toimimise lepingu artiklis 339 ja personalieeskirjade artiklis 17) või mida Euroopa Parlament peab õiguslikel põhjustel kaitsma, kuid mida ei ole vaja või mida ei saa salastada.

E.3. ***Märgete kasutamine side- ja infosüsteemides***

38. Märgete kasutamise eeskirju kohaldatakse ka akrediteeritud side- ja infosüsteemide suhtes.

39. Turvalisuse akrediteerimise asutus kehtestab erieeskirjad märgete kasutamiseks akrediteeritud side- ja infosüsteemides.

F. **TEABE VASTUVÕTMINE**

40. CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE / EU SECRET või TRÈS SECRET UE / EU TOP SECRET salastatuse tasemega või samaväärset teavet võib Euroopa Parlamendis kolmandatelt isikutelt vastu võtta ainult salastatud teabe üksus.

41. RESTREINT UE / EU RESTRICTED salastatuse tasemega või samaväärset teavet ning muud konfidentsiaalset teavet võivad kolmandatelt isikutelt vastu võtta ja käesolevas julgeolekuteates sätestatud põhimõtteid kohaldada nii salastatud teabe üksus kui ka pädev parlamendi organ või ametikandja.

G. **REGISTREERIMINE**

42. Registreerimine on niisuguse menetluste kohaldamine, mille abil talletatakse andmed konfidentsiaalse teabe kogu kasutusaja iga etapi, sealhulgas selle levitamise, sellega tutvumise ja selle hävitamise kohta.

43. Käesolevas julgeolekuteates tähendab registreerimisraamat registrit, kuhu talletatakse eelkõige kuupäevad ja kellaajad, millal:

a) konfidentsiaalne teave saabub Euroopa Parlamendi asjaomase organi või ametikandja sekretariaati või salastatud teabe üksusse või väljastatakse sealt;

b) julgeolekukontrolli läbinud isik konfidentsiaalse teabega tutvub või see talle edastatakse ning

c) konfidentsiaalne teave hävitatakse.

44. Salastatud teabe koostaja ülesanne on märkida esialgne avaldus sellist teavet sisaldava dokumendi koostamisel. Selline avaldus edastatakse salastatud teabe üksusele dokumendi koostamisel.

45. CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE / EU SECRET või TRÈS SECRET UE / EU TOP SECRET salastatuse tasemega või samaväärset teavet võib julgeolekukaalutulustel registreerida ainult salastatud teabe üksus. Kolmandatelt isikutelt saadud RESTREINT UE / EU RESTRICTED salastatuse tasemega teabe, samaväärse teabe ja muu konfidentsiaalse teabe registreerib halduseesmärgil dokumendi ametliku vastuvõtmise eest vastutav teenistus, olgu selleks salastatud teabe üksus või Euroopa Parlamendi organi või ametikandja sekretariaat. Euroopa Parlamendis koostatud muu konfidentsiaalse teabe registreerib halduseesmärgil koostaja.

46. CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE / EU SECRET või TRÈS SECRET UE / EU TOP SECRET salastatuse tasemega või samaväärne teave registreeritakse eelkõige siis:

a) kui see koostatakse;

b) kui see saabub salastatud teabe üksusesse või kui see sealt väljastatakse ning

c) kui see saabub side- ja infosüsteemi või kui see sealt väljastatakse.

47. RESTREINT UE / EU RESTRICTED salastatuse tasemega või samaväärne teave registreeritakse eelkõige siis,

a) kui see koostatakse;

b) kui see saabub Euroopa Parlamendi asjaomase organi või ametikandja sekretariaati või salastatud teabe üksusse või väljastatakse sealt ning

c) kui see saabub side- ja infosüsteemi või kui see sealt väljastatakse.

48. Konfidentsiaalset teavet võib registreerida paberkandjal olevasse või elektroonilisse registreerimisraamatusse / side- ja infosüsteemi.

49. RESTREINT UE / EU RESTRICTED salastatuse tasemega või samaväärse teabe ning muu konfidentsiaalse teabe puhul talletatakse vähemalt:

a) kuupäev ja kellaaeg, millal teave saabub Euroopa Parlamendi asjaomase organi või ametikandja sekretariaati või salastatud teabe üksusse või väljastatakse sealt;

b) dokumendi pealkiri, salastatuse tase või märge, salastatuse taseme või märke aegumise kuupäev ning kõik dokumendiga seotud viitenumbrid;

50. CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE / EU SECRET või TRÈS SECRET UE / EU TOP SECRET salastatuse tasemega või samaväärse teabe puhul talletatakse vähemalt:

a) teabe salastatud teabe üksusesse saabumise või sealt väljastamise kuupäev ja kellaaeg;

b) dokumendi pealkiri, salastatuse tase või märge, kõik dokumendiga seotud viitenumbrid ning salastatuse/märke aegumise kuupäev;

c) koostaja andmed;

d) märge isiku andmete kohta, kellele on antud dokumendile juurdepääs, ning kuupäeva kohta, millal see isik seda juurdepääsu kasutas;

e) märge dokumendist tehtud koopiate ja tõlgete kohta;

f) kuupäev ja kellaaeg, millal dokumendi koopiad või tõlked salastatud teabe üksusest väljastatakse või sinna tagastatakse, ning üksikasjad selle kohta, kuhu need saadeti ja kes need tagastas;

g) kuupäev ja kellaeg, millal dokument hävitatakse, ning kelle poolt, vastavalt hävitamist käsitlevatele Euroopa Parlamendi julgeolekueeskirjadele ning

h) dokumendi salastatuse kustutamine või salastatuse taseme alandamine.

51. Registreerimisraamatud salastatakse või märgistatakse vastavalt vajadusele. Registreerimisraamatud, milles registreeritakse TRÈS SECRET UE / EU TOP SECRET salastatuse tasemega või samaväärne teave, salastatakse samal tasemel.

52. Salastatud teabe võib registreerida:

a) ühes registreerimisraamatus või

b) eri registreerimisraamatutes, lähtudes salastatuse tasemest, sellest, kas teave saabub või väljub, ning teabe päritolust või saajast.

53. Kui teavet töödeldakse elektrooniliselt side- ja infosüsteemi sees, võib registreerimismenetlus toimuda side- ja infosüsteemi enda vahendite abil, kui need vastavad nõuetele, mis on samaväärsed eespool nimetatutega. Kui ELi salastatud teave väljub side- ja infosüsteemi piirest, kohaldatakse eespool kirjeldatud registreerimismenetlust.

54. Salastatud teabe üksus registreerib kogu salastatud teabe, mida Euroopa Parlament on kolmandatele isikutele väljastanud, ja salastatud teabe, mida Euroopa Parlament on kolmandatelt isikutelt saanud.

55. Kui CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE / EU SECRET või TRÈS SECRET UE / EU TOP SECRET salastatuse tasemega või samaväärse teabe registreerimine on lõpule viidud, kontrollib salastatud teabe üksus, kas adressaadil on kehtiv juurdepääsuluba. Kui juurdepääsuluba on olemas, teavitab salastatud teabe üksus adressaati. Salastatud teabega tutvumine saab toimuda ainult siis, kui salastatud teavet sisaldav dokument on registreeritud.

H. **EDASTAMINE**

56. Koostaja määrab esialgselt kindlaks isikud, kellele tema koostatud ELi salastatud teave edastatakse.

57. Euroopa Parlamendi koostatud RESTREINT UE / EU RESTRICTED salastatuse tasemega ja muud konfidentsiaalset teavet edastab Euroopa Parlamendis koostaja kooskõlas asjaomase käitlemisjuhendiga ning teadmisvajaduse põhimõttest lähtudes. Euroopa Parlamendi poolt turvaalal koostatud CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE / EU SECRET või TRÈS SECRET UE / EU TOP SECRET salastatuse tasemega teabe osas tuleb teabe saajate nimekiri (ja mis tahes täiendavad suunised edastamiseks) esitada salastatud teabe üksusele, mis vastutab selle haldamise eest.

58. Euroopa Parlamendi poolt koostatud ELi salastatud teavet võib kolmandatele isikutele edastada ainult salastatud teabe üksus teadmisvajaduse põhimõttest lähtudes.

59. Salastatud teabe üksuse või taotluse esitanud Euroopa Parlamendi organi või ametikandja saadud konfidentsiaalset teavet edastatakse vastavalt teabe koostajalt saadud juhistele.

I. **KÄITLEMINE, SÄILITAMINE JA TUTVUMINE**

60. Konfidentsiaalse teabe käitlemine, säilitamine ja sellega tutvumine toimub vastavalt julgeolekuteatele 4 ja käitlemisjuhendile.

J. **SALASTATUD TEABE KOPEERIMINE JA TÕLKIMINE**

61. TRÈS SECRET UE / EU TOP SECRET salastatuse tasemega või samaväärset teavet sisaldavaid dokumente ei tohi kopeerida ega tõlkida ilma selle koostaja eelneva kirjaliku nõusolekuta. SECRET UE / EU SECRET salastatuse tasemega või samaväärset teavet või CONFIDENTIEL UE / EU CONFIDENTIAL salastatuse tasemega või samaväärset teavet sisaldavaid dokumente võib kopeerida või tõlkida valdaja ülesandel, tingimusel et koostaja ei ole seda keelustanud.

62. TRÈS SECRET UE / EU TOP SECRET, SECRET UE / EU SECRET või CONFIDENTIEL UE / EU CONFIDENTIAL salastatuse tasemega või samaväärset teavet sisaldava dokumendi iga koopia tuleb julgeoleku huvides registreerida.

63. Salastatud teavet sisaldava originaaldokumendi suhtes kohaldatavaid turvameetmeid rakendatakse ka selle dokumendi koopiate ja tõlgete suhtes.

64. Nõukogult saadud dokumendid peaksid olema kõikides ametlikes keeltes.

65. Salastatud teavet sisaldavate dokumentide koopiaid ja/või tõlkeid võib nõuda koostaja või koopia valdaja. CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE / EU SECRET või TRÈS SECRET UE / EU TOP SECRET salastatuse tasemega või samaväärset teavet sisaldavate dokumentide koopiaid võib teha üksnes turvaalal ning koopiamasinatel, mis kuuluvad akrediteeritud side- ja infosüsteemi. RESTREINT UE / EU RESTRICTED salastatuse tasemega või sellega samaväärset teavet sisaldavate dokumentide koopiaid võib teha akrediteeritud koopiamasinatel Euroopa Parlamendi hoonetes.

66. Kõikide konfidentsiaalset teavet sisaldavate dokumentide või nende osade koopiad ja tõlked tuleb asjakohaselt märgistada, nummerdada ja registreerida.

67. Koopiaid ei tehta rohkem kui tingimata vajalik. Kõik koopiad hävitatakse vastavalt käitlemisjuhendile nendega tutvumise perioodi lõppedes.

68. Ainult Euroopa Parlamendi ametnikest tõlkidele ja tõlkijatele antakse juurdepääs salastatud teabele.

69. Tõlkidel ja tõlkijatel, kellel on juurdepääs CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE / EU SECRET või TRÈS SECRET UE / EU TOP SECRET salastatuse tasemega või samaväärset teavet sisaldavatele dokumentidele, peab olema vastav juurdepääsuluba.

70. CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE / EU SECRET või TRÈS SECRET UE / EU TOP SECRET salastatuse tasemega või samaväärset teavet sisaldavate dokumentidega töötades peavad tõlgid ja tõlkijad viibima turvaalal.

K. **KONFIDENTSIAALSE TEABE SALASTATUSE TASEME ALANDAMINE, SALASTATUSE KUSTUTAMINE JA MÄRKE KUSTUTAMINE**

K.1. ***Üldpõhimõtted***

71. Konfidentsiaalse teabe salastatuse taset alandatakse, salastatus kustutatakse või märge kustutatakse, kui kaitset ei ole enam vaja või seda ei ole enam vaja algsel tasemel.

72. Euroopa Parlamendis koostatud dokumentides sisalduva teabe salastatuse taseme alandamise, salastatuse kustutamise ja märke kustutamise otsuseid võib teha ka juhtumipõhiselt, nt vastuseks juurdepääsutaotlusele üldsuse või liidu muu institutsiooni poolt, või salastatud teabe üksuse või Euroopa Parlamendi organi või ametikandja algatusel.

73. ELi salastatud teabe koostamise ajal märgib koostaja võimaluse korral, kas asjaomase ELi salastatud teabe salastatuse taset võib teataval kuupäeval või konkreetse sündmuse järel alandada või võib selle salastatuse kustutada. Kui sellise teabe edastamine ei ole otstarbekas, vaatab koostaja, salastatud teabe üksus või teavet valdav Euroopa Parlamendi organ või ametikandja ELi salastatud teabe salastatuse taseme vähemalt iga viie aasta järel läbi. ELi salastatud teabe salastatuse taset alandada või salastatuse kustutada võib igal juhul üksnes koostaja eelneval kirjalikul nõusolekul.

74. Kui ELi salastatud teabe koostajat ei ole võimalik Euroopa Parlamendis koostatud dokumentide puhul kindlaks teha või leida, vaatab ELi salastatud teabe salastatuse taseme läbi julgeolekuasutus teavet valdava Euroopa Parlamendi organi või ametikandja ettepanekul. Organ või ametikandja võib konsulteerida salastatud teabe üksusega.

75. Salastatud teabe üksus või teavet valdav Euroopa Parlamendi organ või ametikandja vastutab selle eest, et dokumendi adressaate teavitatakse teabe salastatuse kustutamisest või salastatuse taseme alandamisest, ning adressaadid omakorda vastutavad selle eest, et muudatustest teavitatakse järgmisi adressaate, kellele nad on saatnud kõnealuse dokumendi või selle koopia.

76. Dokumendis sisalduva teabe salastatuse kustutamine, salastatuse taseme alandamine ja märke kustutamine registreeritakse.

K.2. ***Salastatuse kustutamine***

77. ELi salastatud teabe salastatuse võib kustutada täielikult või osaliselt. Selle salastatuse võib kustutada osaliselt, kui kaitset ei peeta enam vajalikuks salastatud teavet sisaldava dokumendi konkreetse osa puhul, kuid seda peetakse vajalikuks ülejäänud dokumendi puhul.

78. Kui Euroopa Parlamendis koostatud dokumendis sisalduva ELi salastatud teabe läbivaatamisel jõutakse otsusele salastatus kustutada, kaalutakse, kas teha asjaomane dokument avalikuks või kanda sellele edastamismärge (s.t dokumenti ei tehta avalikuks).

79. Kui ELi salastatud teabe salastatus kustutatakse, tuleb salastatuse kustutamine registreerimisraamatusse talletada koos järgmiste andmetega: salastatuse kustutamise kuupäev, salastatuse kustutamist taotlenud ja selleks loa andnud isikute nimed, kustutatud salastatuse tasemega dokumendi viitenumber ja selle lõplik sihtkoht.

80. Endised salastusmärked kustutatud salastusega dokumendis ja selle kõigis koopiates tuleb läbi kriipsutada. Dokument ja selle kõik koopiad tuleb asjakohaselt talletada.

81. Salastatud teabe salastatuse osalisel kustutamisel tehakse kustutatud salastatusega osast väljavõte ja see talletatakse asjakohaselt. Pädev teenistus peab registreerima järgmised andmed:

a) salastatuse osalise kustutamise kuupäev;

b) salastatuse kustutamist taotlenud ja selleks loa andnud isikute nimed ning

c) kustutatud salastatusega väljavõtte viitenumber.

K.3. ***Salastatuse taseme alandamine***

82. Pärast salastatud teabe salastatuse taseme alandamist tuleb seda sisaldav dokument registreerida nii endisele kui ka uuele salastatuse tasemele vastavas registreerimisraamatus. Üles tuleb märkida salastatuse taseme alandamise kuupäev ning selleks loa andnud isiku nimi.

83. Alandatud salastatuse tasemega teavet sisaldav dokument ja selle kõik koopiad peavad saama uue salastatuse taseme ning need tuleb asjakohaselt talletada.

L. **KONFIDENTSIAALSE TEABE HÄVITAMINE**

84. Konfidentsiaalne teave (kas paberkandjal või elektroonilisel kujul), mida ei ole enam vaja, hävitatakse või kustutatakse vastavalt käitlemisjuhendile ja asjaomastele arhiveerimiseeskirjadele.

85. TRÈS SECRET UE / EU TOP SECRET või SECRET UE / EU SECRET salastatuse tasemega või samaväärse teabe hävitab salastatud teabe üksus. Teabe hävitamise juures viibib isik, kellel on vähemalt hävitatava teabe salastatuse tasemele vastav juurdepääsuluba.

86. TRÈS SECRET UE / EU TOP SECRET salastatuse tasemega või samaväärset teavet võib hävitada üksnes teabe koostaja eelneval kirjalikul nõusolekul.

87. CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE / EU SECRET või TRÈS SECRET UE / EU TOP SECRET salastatuse tasemega või samaväärset teavet võib hävitada ja sellest vabaneda salastatud teabe üksus koostaja või pädeva asutuse ülesandel. Registreerimisraamatud ja muud registrid ajakohastatakse vastavalt. RESTREINT UE / EU RESTRICTED salastatuse tasemega või samaväärset teavet võib hävitada ja sellest vabaneda salastatud teabe üksus või asjaomane Euroopa Parlamendi organ või ametikandja.

88. Hävitamise eest vastutav ametnik ja hävitamise tunnistaja kirjutavad alla hävitamisaktile, mis antakse hoiule salastatud teabe üksusesse. Salastatud teabe üksuses säilitatakse koos edastamisvormidega TRÈS SECRET UE / EU TOP SECRET salastatuse tasemega või samaväärse teabe hävitamisakte vähemalt kümme aastat ning SECRET UE / EU SECRET salastatuse tasemega või samaväärse teabe ja CONFIDENTIEL UE / EU CONFIDENTIAL salastatuse tasemega või samaväärse teabe hävitamisakte vähemalt viis aastat.

89. Salastatud teavet sisaldavad dokumendid hävitatakse viisil, mis vastab asjakohastele liidu või samaväärsetele standarditele, et vältida nende täielikku või osalist taastamist.

90. Salastatud teabe salvestamiseks kasutatud elektrooniliste andmekandjate hävitamine toimub vastavalt käitlemisjuhendile.

91. Salastatud teabe hävitamine tuleb talletada vastavasse registreerimisraamatusse koos järgmiste andmetega:

a) hävitamise kuupäev ja kellaaeg;

b) hävitamise eest vastutava ametniku nimi;

c) hävitatud dokumendi või koopiate märked;

d) hävitatud ELi salastatud teabe säilitamise algne füüsiline vorm;

e) hävitamise vahendid ning

f) hävitamise koht.

M. **ARHIVEERIMINE**

92. Salastatud teave, sh lisatud teade või kiri, lisad, vastuvõtukviitung ja/või dokumendi muud osad, viiakse üle turvala turvatud arhiivi kuus kuud pärast seda, kui sellega viimati tutvuti, ning kõige hiljem üks aasta pärast seda, kui see hoiule anti. Salastatud teabe arhiveerimise üksikasjalikud eeskirjad kehtestatakse käitlemisjuhendis.

93. Muu konfidentsiaalse teabe puhul kohaldatakse dokumentide haldamise üldisi eeskirju, ilma et see piiraks muid erisätteid nende käitlemise kohta.

JULGEOLEKUTEADE 3

KONFIDENTSIAALSE TEABE TÖÖTLEMINE AUTOMATISEERITUD SIDE- JA INFOSÜSTEEMIDE ABIL

A. **INFOSÜSTEEMIDES KÄIDELDAVA SALASTATUD TEABE INFOKINDLUS**

1. Infokindlus infosüsteemide valdkonnas tähendab kindlust, et sellised süsteemid kaitsevad neis käideldavat salastatud teavet ning toimivad ettenähtud korras, ettenähtud ajal ja õiguspäraste kasutajate kontrolli all. Tulemuslik infokindlus tagab asjakohasel tasemel konfidentsiaalsuse, tervikluse, kättesaadavuse, salgamise vääramise ja autentsuse. Infokindluse aluseks on riskijuhtimisprotsess.

2. Side- ja infosüsteem, mis on ette nähtud salastatud teabe käitlemiseks, tähendab süsteemi, mis võimaldab elektroonilises vormis oleva teabe käitlemist. Niisugune infosüsteem hõlmab kõiki selle toimimiseks vajalikke vahendeid, sealhulgas infrastruktuuri, töökorralduse, töötajate ja teabega seotud ressursse.

3. Side- ja infosüsteemides käideldakse salastatud teavet kooskõlas infokindluse kontseptsiooniga.

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

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

a) autentsus: tagatis, et teave on ehtne ja et see pärineb heausksest allikast;

b) kättesaadavus: teave on vastavat luba omava üksuse taotluse alusel kättesaadav ja kasutatav;

c) konfidentsiaalsus: teavet ei avalikustata vastava loata isikutele või üksustele või vastava loata töötlemiseks;

d) terviklus: teabe ja süsteemi osade täpsuse ja terviklikkuse kaitse;

e) salgamise vääramine: võime tõestada tegevuse või sündmuse toimumist selliselt, et välistada võimalus kõnealuse sündmuse või tegevuse toimumise hilisemaks eitamiseks.

B. **INFOKINDLUSE PÕHIMÕTTED**

6. Allpool toodud sätted on iga side- ja infosüsteemi, milles käideldakse salastatud teavet, turvalisuse aluseks. Kõnealuste sätete rakendamise üksikasjalikud nõuded määratakse kindlaks infokindluse julgeolekupoliitikas ja julgeolekusuunistes.

B.1. ***Turvariski juhtimine***

7. Turvariski juhtimine on side- ja infosüsteemi määratlemise, arendamise, kasutamise ja haldamise lahutamatu osa. Riskijuhtimist (hindamine, käsitlemine, aktsepteerimine ja teavitamine) viiakse läbi julgeolekuteates 1 esitatud süsteemiomanike, projekteerimisasutuste, töötlejate ja julgeolekualase heakskiidu andmise asutuste esindajate poolt ühiselt järkjärgulise protsessina, kasutades tõestatud, läbipaistvat ja arusaadavat riskihindamise protsessi. Side- ja infosüsteemi ulatus ja selle osad määratakse selgelt kindlaks riskijuhtimisprotsessi alguses.

8. Julgeolekuteates 1 nimetatud pädevad asutused käsitlevad side- ja infosüsteeme ähvardavaid võimalikke ohtusid ning koostavad ajakohased ja täpsed ohuhinnangud, mis kajastavad olemasolevat töökeskkonda. Nad ajakohastavad pidevalt oma teadmisi süsteemi haavatavuse küsimustes ning vaatavad korrapäraselt läbi haavatavust käsitlevad hinnangud, et ajakohastada neid vastavalt muutustele infotehnoloogia valdkonnas.

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

10. Side- ja infosüsteemi akrediteerimine hõlmab jääkriski käsitleva ametliku avalduse koostamist ja jääkriski aktsepteerimist vastutava asutuse poolt. Konkreetsed nõuded, nende ulatus ja üksikasjalikkuse aste, mille määrab kindlaks side- ja infosüsteemi akrediteerimise eest vastutav asjaomane turvalisuse akrediteerimise asutus, on vastavuses hinnatud riskiga, mille puhul on arvesse võetud kõiki asjaomaseid tegureid, sealhulgas side- ja infosüsteemis käideldava salastatud teabe salastatuse taset.

B.2. ***Turvalisus side- ja infosüsteemi kogu kasutusaja jooksul***

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

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

13. Side- ja infosüsteemide, sealhulgas nende tehniliste ja mittetehniliste turvameetmete suhtes viiakse akrediteerimisprotsessi käigus läbi turvatestid, et tagada, et on saavutatud sobiv kindluse tase, ning teha kindlaks, et side- ja infosüsteemid, sealhulgas nende tehnilised ja mittetehnilised turvameetmed, on nõuetekohaselt rakendatud, integreeritud ja seadistatud.

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

15. Side- ja infosüsteemi turvaalane dokumentatsioon kujuneb süsteemi kasutusaja jooksul muudatuste haldamise protsessi lahutamatu osana.

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

B.3. ***Parim tava***

17. Infokindluse asutus töötab välja parima tava side- ja infosüsteemis käideldava salastatud teabe kaitseks. Parimat tava käsitlevates suunistes kirjeldatakse side- ja infosüsteemi tehnilisi, füüsilisi, organisatsioonilisi ja menetluslikke turvameetmeid, mille tulemuslikkus teadaolevate ohtude tõrjumisel ja haavatavuse kõrvaldamisel on tõendatud.

18. Side- ja infosüsteemis käideldava salastatud teabe kaitsel tuginetakse infokindlusega tegelevate üksuste kogemustele.

19. Parima tava levitamine ja edasine rakendamine aitab saavutada ühtse infokindluse taseme Euroopa Parlamendi peasekretariaadi kasutatavate side- ja infosüsteemide puhul, milles käideldakse salastatud teavet.

B.4. ***Süvakaitse***

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

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

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

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

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

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

Selliste turvameetmete tugevusaste määratakse kindlaks vastavalt riskihinnangule.

21. Julgeolekuteates 1 nimetatud pädevad asutused tagavad, et nad on suutelised reageerima intsidentidele, mis võivad ületada organisatsiooni piire selliselt, et kooskõlastada reageeringuid ning jagada teavet nende intsidentide ja nendega seotud riskide kohta (infotehnoloogilise hädaolukorrale reageerimise võime).

B.5. ***Privileegide minimaalsuse ja piiratuse põhimõte***

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

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

B.6. ***Infokindlusalane teadlikkus***

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

a) turvanõuete rikkumine võib oluliselt kahjustada side- ja infosüsteeme, milles käideldakse salastatud teavet;

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

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

25. Turvalisusega seotud vastutuse mõistmise tagamiseks on infokindlusalane koolitus ja teadlikkust tõstev koolitus kohustuslik kõigile asjaomastele töötajatele, sealhulgas kõrgema astme juhtkonnale, Euroopa Parlamendi liikmetele ning side- ja infosüsteemi kasutajatele.

B.7. ***Infotehnoloogia turvatoodete hindamine ja heakskiitmine***

26. CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE / EU SECRET või TRÈS SECRET UE / EU TOP SECRET salastatuse tasemega või samaväärset teavet käitlevaid side- ja infosüsteeme kaitstakse viisil, mis välistab teabe ohtusattumise tahtmatu elektromagnetkiirguse kaudu („TEMPEST-turvameetmed”).

27. Kui salastatud teavet kaitstakse krüptovahenditega, sertifitseerib turvalisuse akrediteerimise asutus sellised vahendid ELi poolt heakskiidetud krüptovahenditena.

28. Salastatud teabe elektroonilise edastamise ajal kasutatakse ELi poolt heakskiidetud krüptovahendeid. Sellest nõudest olenemata võib erakorraliste asjaolude korral kohaldada erimenetlusi või spetsiifilisi tehnilisi tingimusi, nagu on täpsustatud punktides 41–44.

29. Turvameetmete usaldatavus, mida väljendatakse infokindluse taseme kaudu, määratakse kindlaks riskijuhtimisprotsessi tulemuste põhjal ning kooskõlas asjaomase julgeolekupoliitika ja julgeolekusuunistega.

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

31. Turvalisuse akrediteerimise asutus kiidab heaks julgeolekusuunised mittekrüpteerivate infotehnoloogia turvatoodete kvalifitseerimise ja heakskiitmise kohta.

B.8. ***Edastamine turvaala piires***

32. Salastatud teabe edastamisel turvaala piires võib kasutada riskijuhtimisprotsessi tulemuste alusel ja turvalisuse akrediteerimise asutuse loal teabe krüpteerimata levitamist või madalamal tasemel krüpteerimist.

B.9. ***Side- ja infosüsteemide turvaline ühendamine***

33. Omavaheline ühendus tähendab kahe või enama infotehnoloogia süsteemi vahelist otseühendust, mille eesmärk on andmete ja muude teaberessursside ühesuunaline või mitmesuunaline jagamine.

34. Side- ja infosüsteem käsitab igat temaga ühendatud infotehnoloogia süsteemi esialgu ebausaldusväärsena ning rakendab mis tahes muu side- ja infosüsteemiga toimuva salastatud teabe vahetuse kontrollimiseks kaitsemeetmeid.

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

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

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

c) side- ja infosüsteemide ühenduspunktides rakendatakse kaitseteenuseid.

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

37. Kui kaitsmata või avalikku võrku kasutatakse üksnes ülekandeks ja andmed on krüpteeritud sellise ELi krüptovahendiga, mis on sertifitseeritud punkti 27 kohaselt, ei loeta sellist ühendust omavaheliseks ühenduseks.

38. TRÈS SECRET UE / EU TOP SECRET salastatuse tasemega või samaväärse teabe või SECRET UE / EU SECRET salastatuse tasemega või samaväärse teabe käitlemiseks akrediteeritud side- ja infosüsteemi vahetu või astmeline ühendamine kaitsmata või avaliku võrguga on keelatud.

B.10. ***Elektroonilised salvestuskandjad***

39. Elektroonilised andmekandjad hävitatakse pädeva julgeolekuasutuse poolt heaks kiidetud korra kohaselt.

40. Elektrooniliste andmekandjate taaskasutamine, nende salastatuse taseme alandamine või salastatuse kustutamine toimub vastavalt käitlemisjuhendile.

B.11. ***Erakorralised asjaolud***

41. Erakorraliste asjaolude, nagu ähvardava või reaalse kriisi, konflikti, sõjaolukorra või operatiivsete erakorraliste asjaolude korral võib kohaldada allpool kirjeldatud erimenetlusi.

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

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

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

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

44. Kui kohaldatakse punkte 41 või 42, esitatakse vastav aruanne pädevale asutusele.

JULGEOLEKUTEADE 4

FÜÜSILINE JULGEOLEK

A. **SISSEJUHATUS**

Käesolevas julgeolekuteates kehtestatakse julgeolekupõhimõtted, mille eesmärk on luua turvaline keskkond Euroopa Parlamendis konfidentsiaalse teabe korrektse käsitlemise tagamiseks. Neid põhimõtteid, sealhulgas neid mis on seotud tehnilise turvalisusega, täiendab käitlemisjuhend.

B. **TURVARISKI JUHTIMINE**

1. Salastatud teabe turvariski juhitakse protsessina. Nimetatud protsessi eesmärk on teha kindlaks teadaolevad turvariskid, määratleda vastavalt käesolevas julgeolekuteates sätestatud aluspõhimõtetele ja miinimumstandarditele selliste riskide vastuvõetava tasemeni vähendamise turvameetmed ning kohaldada neid meetmeid kooskõlas julgeolekuteates 3 määratletud süvakaitse põhimõttega. Selliste meetmete tulemuslikkust hinnatakse pidevalt.

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

3. Hädaolukorra lahendamise plaanides võetakse arvesse vajadust kaitsta salastatud teavet hädaolukordades, et vältida loata juurdepääsu teabele, teabe loata avaldamist või teabe tervikluse või kättesaadavuse kadumist.

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

C. **ÜLDPÕHIMÕTTED**

5. Teabele määratud salastatuse või märgete tase määrab kindlaks füüsilise julgeoleku osas teabele pakutava kaitse taseme.

6. Salastamist vajav teave märgistatakse salastatud teabena ning seda käideldakse salastatud teabena olenemata selle füüsilisest vormist. Teabe saajaid teavitatakse selgesõnaliselt teabe salastatusest, tehes seda kas salastusmärke abil (kui teave esitatakse kirjalikult, olenemata sellest, kas see esitatakse paberil või side- ja infosüsteemis) või avalduse vormis (kui teave esitatakse suuliselt, näiteks vestluse või ettekande ajal). Salastatud materjal on füüsiliselt märgistatud viisil, mis võimaldab kergesti tuvastada selle salastatust.

7. Konfidentsiaalset teavet ei loeta mingil juhul avalikes kohtades, kus seda võivad näha teadmisvajaduseta isikud, näiteks rongides, õhusõidukites, kohvikutes, baarides jne. Seda ei jäeta hotelli seifidesse ega tubadesse ega avalikes kohtades järelevalveta.

D. **VASTUTUS**

8. Salastatud teabe üksus vastutab füüsilise julgeoleku tagamise eest oma turvatud rajatistes hoitava konfidentsiaalse teabe haldamisel. Salastatud teabe üksus vastutab ka oma turvatud rajatiste haldamise eest.

9. Füüsilise julgeoleku tagamise eest RESTREINT UE / EU RESTRICTED salastatuse tasemega või samaväärse teabe ning muu konfidentsiaalse teabe haldamisel vastutab vastav Euroopa Parlamendi organ või ametikandja.

10. Turvaküsimuste ja riskihindamise direktoraat tagab töötajatega seotud julgeoleku ja julgeolekukontrolli, mis on vajalikud konfidentsiaalse teabe turvaliseks käitlemiseks Euroopa Parlamendis.

11. Infotehnoloogia direktoraat annab nõu ning tagab, et mis tahes loodav või kasutatav side- ja infosüsteem vastaks täielikult julgeolekuteatele 3 ning vastavale käitlemisjuhendile.

E. **TURVATUD RAJATISED**

12. Tehniliste turvastandardite alusel ja vastavalt konfidentsiaalsele teabele määratud tasemele on lubatud luua turvatud rajatisi, mis on määratletud artiklis 7.

13. Turvatud rajatised sertifitseeritakse turvalisuse akrediteerimise asutuse ja valideeritakse julgeolekuasutuse poolt.

F. **KONFIDENTSIAALSE TEABEGA TUTVUMINE**

14. Kui salastatud teabe üksusesse hoiule antud RESTREINT UE / EU RESTRICTED salastatuse tasemega või samaväärse teabe ning muu konfidentsiaalse teabega tuleb tutvuda väljaspool turvaala, edastab salastatud teabe üksus selle koopia asjaomasele juurdepääsuluba omavale teenistusele, kes tagab, et niisuguse teabega tutvumine ja selle käitlemine on kooskõlas käesoleva otsuse artikli 8 lõikega 2 ja artikliga 10 ning asjaomase käitlemisjuhendiga.

15. Kui RESTREINT UE / EU RESTRICTED salastatuse tasemega või samaväärne teave ning muu konfidentsiaalne teave on antud hoiule Euroopa Parlamendi organile või ametikandjale, kes ei ole salastatud teabe üksus, tagab selle Euroopa Parlamendi organi või ametikandja sekretariaat, et niisuguse teabega tutvumine ja selle käitlemine on kooskõlas käesoleva otsuse artikli 7 lõikega 3, artikli 8 lõigetega 1, 2 ja 4, artikli 9 lõigetega 3, 4 ja 5, artikli 10 lõigetega 2–6 ja artikliga 11 ning asjaomase käitlemisjuhendiga.

16. Kui CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE / EU SECRET või TRÈS SECRET UE / EU TOP SECRET salastatuse tasemega või samaväärse teabega tuleb tutvuda turvaalal, tagab salastatud teabe üksus, et niisuguse teabega tutvumine ja selle käitlemine on kooskõlas käesoleva otsuse artiklitega 9 ja 10 ning asjaomase käitlemisjuhendiga.

G. **TEHNILINE TURVALISUS**

17. Tehniliste turvameetmete eest vastutab turvalisuse akrediteerimise asutus, kes määrab vastavas käitlemisjuhendis kindlaks kohaldatavad spetsiifilised tehnilised turvameetmed.

18. Turvatud lugemissaalide puhul, mis on ette nähtud RESTREINT UE / EU RESTRICTED salastatuse tasemega või samaväärse teabe ning muu konfidentsiaalse teabega tutvumiseks, järgitakse spetsiifilisi tehnilisi turvameetmeid, mis on kehtestatud käitlemisjuhendis.

19. Turvaala hõlmab järgmisi rajatisi:

a) juurdepääsualase julgeolekukontrolli ruum, mis seatakse sisse vastavalt käitlemisjuhendis kehtestatud tehnilistele turvameetmetele. Sisenemine sellesse rajatisse registreeritakse. Juurdepääsualane julgeolekukontroll vastab kõrgetele standarditele, mis on seotud juurdepääsu omavate isikute tuvastamisega, videosalvestamisega ja turvaliste kohtadega, mis on ette nähtud niisuguste isiklike asjade hoiuleandmiseks, mille kasutamine ei ole turvatud ruumides lubatud (telefonid, kirjutusvahendid jne);

b) sideruum salastatud teabe, sealhulgas krüpteeritud salastatud teabe edastamiseks ja vastuvõtmiseks vastavalt julgeolekuteatele 3 ning vastavale käitlemisjuhendile;

c) turvatud arhiiv, kus RESTREINT UE / EU RESTRICTED, CONFIDENTIEL UE / EU CONFIDENTIAL ja/või SECRET UE / EU SECRET salastatuse tasemega või samaväärse teabe puhul kasutatakse heakskiidetud ja sertifitseeritud eraldi konteinereid. TRÈS SECRET UE / EU TOP SECRET salastatuse tasemega või samaväärne teave paigutatakse spetsiifilises sertifitseeritud konteineris eraldi ruumi. Ainuke selles eraldi ruumis olev täiendav materjal on abilaud arhiivi käitlemiseks salastatud teabe üksuse poolt;

d) registriruum, kus on vajalikud vahendid registreerimise paberkandjal või elektroonilise teostamise võimaldamiseks ning mis on varustatud turvatud rajatistega, mis on vajalikud asjakohase side- ja infosüsteemi paigaldamiseks. Üksnes registriruumis võivad olla heakskiidetud ja akrediteeritud paljundamisseadmed (paberkandjal või elektrooniliste koopiate tegemiseks). See, millised paljundamisseadmed on heakskiidetud ja akrediteeritud, täpsustatakse käitlemisjuhendis. Registriruumis on tagatud ka ruum, mis on vajalik akrediteeritud materjali hoidmiseks ja käitlemiseks, et võimaldada füüsilises vormis salastatud teabe märgistamist, kopeerimist ja edastamist salastatuse taseme kaupa. Kogu akrediteeritud materjali määratleb salastatud teabe üksus ning akrediteerib turvalisuse akrediteerimise asutus infokindluse rakendusasutuse nõuande alusel. Registriruum on varustatud ka akrediteeritud hävitusseadmega, mis on heaks kiidetud kõige kõrgema salastatuse taseme jaoks, nagu on kirjeldatud käitlemisjuhendis. CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE / EU SECRET või TRÈS SECRET UE / EU TOP SECRET salastatuse tasemega või samaväärne teave tõlgitakse registriruumis asjakohases akrediteeritud süsteemis. Registriruumis on töökohad kuni kahele tõlkijale, kes saavad töötada samal ajal ja sama dokumendiga. Kohal viibib üks salastatud teabe üksuse töötaja;

e) lugemissaal individuaalseks salastatud teabega tutvumiseks selleks nõuetekohast luba omavate isikute poolt. Lugemissaalis on piisavalt ruumi kahele isikule, sealhulgas salastatud teabe üksuse töötajale, kes viibib iga teabega tutvumise ajal kogu aeg saalis. Selle saali turvatase on piisav CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE / EU SECRET või TRÈS SECRET UE / EU TOP SECRET salastatuse tasemega või samaväärse teabega tutvumiseks. Lugemissaal võib olla varustatud TEMPEST-seadmetega, et võimaldada vajaduse korral elektroonilist teabega tutvumist vastavalt asjaomase teabe salastatuse tasemele;

f) koosolekuruum, mis mahutab kuni 25 isikut, et arutada CONFIDENTIEL UE / EU CONFIDENTIAL ja SECRET UE / EU SECRET salastatuse tasemega või samaväärset teavet. Koosolekuruum on varustatud vajalike turvaliste ja sertifitseeritud tehniliste seadmetega, mis võimaldavad suulist tõlget kuni kahte keelde ja kuni kahest keelest. Kui koosolekuruumi ei kasutata koosolekute pidamiseks, võib seda kasutada ka täiendava lugemissaalina individuaalsete teabega tutvumiste tarbeks. Erandkorras võib salastatud teabe üksus lubada salastatud teabega tutvuda rohkem kui ühel vastavat luba omaval isikul, kui juurdepääsuloa ja teadmisvajaduse tase on kõikidel ruumis viibivatel isikutel ühesugune. Salastatud teabega võib samaaegselt tutvuda kuni neli isikut. Niisugusel juhul suurendatakse ruumis viibivate salastatud teabe üksuse töötajate arvu;

g) turvatud tehnikaruumid kõikide kogu turvaala turvalisusega seotud tehniliste seadmete ja turvatud infotehnoloogia serverite mahutamiseks.

20. Turvaala vastab kohaldatavatele rahvusvahelistele turvastandarditele ning on turvaküsimuste ja riskihindamise direktoraadi poolt sertifitseeritud. Turvaalal on tagatud vähemalt järgmised tehnilised turvanõuded:

a) häire- ja järelevalvesüsteemid;

b) ohutusvahendid ja avariisüsteemid (kahesuunaline hoiatussüsteem);

c) videovalve süsteem;

d) sissetungimise avastamise süsteem;

e) juurdepääsu kontroll (sealhulgas biomeetriline turvasüsteem);

f) konteinerid;

g) lukustatavad kapid;

h) elektromagnetkiirgusvastane kaitse.

21. Täiendavaid tehnilisi turvameetmeid võib vajadusel lisada turvalisuse akrediteerimise asutus tihedas koostöös salastatud teabe üksusega ja julgeolekuasutuse heakskiidul.

22. Infrastruktuuriseadmed võib ühendada selle hoone üldjuhtimissüsteemidega, kus turvaala asub. Juurdepääsu kontrolli ning side- ja infosüsteemi alased turvaseadmed on aga mis tahes muust niisugusest Euroopa Parlamendis olemasolevast süsteemist sõltumatud.

H. **TURVAALA KONTROLL**

23. Turvalisuse akrediteerimise asutus viib salastatud teabe üksuse taotluse alusel korrapäraselt läbi turvaala kontrolle.

24. Turvalisuse akrediteerimise asutus koostab kontrolli käigus kontrollitavate objektide kontrollakti ja ajakohastab seda kooskõlas käitlemisjuhendiga.

I. **KONFIDENTSIAALSE TEABE TRANSPORTIMINE**

25. Konfidentsiaalset teavet veetakse vastavalt käitlemisjuhendile varjatult ilma mingi viiteta sisu konfidentsiaalsusele.

26. Üksnes kullerid või töötajad, kellel on vastava taseme juurdepääsuluba, võivad vedada CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE / EU SECRET või TRÈS SECRET UE / EU TOP SECRET salastatuse tasemega või samaväärset teavet.

27. Konfidentsiaalset teavet võib saata välisposti või käsipostiga väljaspool hoonet üksnes vastavalt käitlemisjuhendis sätestatud tingimustele.

28. CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE / EU SECRET või TRÈS SECRET UE / EU TOP SECRET salastatuse tasemega või samaväärset teavet ei saadeta kunagi e-posti ega faksi teel, isegi mitte turvalise e-posti süsteemi või krüptofaksi teel. RESTREINT UE / EU RESTRICTED salastatuse tasemega või samaväärset teavet ning muud konfidentsiaalset teavet võib saata e-posti teel, kasutades selleks akrediteeritud krüpteerimissüsteemi.

J. **KONFIDENTSIAALSE TEABE SÄILITAMINE**

29. Konfidentsiaalsele teabele määratud salastatuse või märgete tase määrab kindlaks teabele pakutava kaitse taseme selle säilitamisel. Seda säilitatakse seadmetes, mis on selleks sertifitseeritud vastavalt käitlemisjuhendile.

30. RESTREINT UE / EU RESTRICTED salastatuse tasemega või samaväärset teavet ning muud konfidentsiaalset teavet:

a) säilitatakse standardses lukustatud teraskapis, kas büroos või tööruumides, kui neid tegelikult ei kasutata;

b) ei jäeta järelevalveta, välja arvatud juhul, kui see on nõuetekohaselt luku taha pandud ja säilitatud;

c) ei jäeta kirjutuslauale ega muule lauale nii, et seda võivad lugeda või selle võivad eemaldada juurdepääsuloata isikud, näiteks külastajad, koristajad, hooldustöötajad jne;

d) ei näidata ühelegi juurdepääsuloata isikule ning seda ei arutata ühegi juurdepääsuloata isikuga.

31. RESTREINT UE / EU RESTRICTED salastatuse tasemega või samaväärset teavet ning muud konfidentsiaalset teavet säilitatakse üksnes Euroopa Parlamendi organi või ametikandja sekretariaatides või salastatud teabe üksuses vastavalt käitlemisjuhendile.

32. CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE / EU SECRET või TRÈS SECRET UE / EU TOP SECRET salastatuse tasemega või samaväärset teavet:

a) säilitatakse turvaalal turvakonteineris või turvakambris. Erandkorras, näiteks juhul kui salastatud teabe üksus on suletud, võib seda säilitada julgeolekuteenistuste juures asuvas heakskiidetud ja sertifitseeritud seifis;

b) ei jäeta turvaalal kunagi järelevalveta, ilma et see oleks eelnevalt lukustatud heakskiidetud seifi (isegi kui eemalviibimise aeg on väga lühike);

c) ei jäeta kirjutuslauale ega muule lauale nii, et seda võib lugeda või selle võib eemaldada juurdepääsuloata isik, isegi kui salastatud teabe üksuse vastutav töötaja jääb ruumi.

Kui salastatud teavet sisaldav dokument koostatakse turvaalal elektrooniliselt, lukustatakse arvuti ja muudetakse kuvari pilt juurdepääsmatuks, kui dokumendi koostaja või salastatud teabe üksuse vastutav töötaja lahkub ruumist (isegi kui eemalviibimise aeg on väga lühike). Automaatset turvalukustust, mis aktiveerub mõne minuti möödudes, ei peeta piisavaks meetmeks.

JULGEOLEKUTEADE 5

TÖÖSTUSJULGEOLEK

A. **SISSEJUHATUS**

1. Käesolev julgeolekuteade käsitleb üksnes salastatud teavet.

2. Selles on esitatud käesoleva otsuse I lisa 1. osa ühiste miinimumstandardite rakendamise sätted.

3. Tööstusjulgeolek tähendab meetmete kohaldamist selleks, et tagada salastatud teabe kaitsmine töövõtjate ja alltöövõtjate poolt lepingueelsetel läbirääkimistel ja salastatud lepingute kogu kehtivusaja jooksul. Selliste lepingutega ei kaasne juurdepääsu TRÈS SECRET UE / EU TOP SECRET salastatuse tasemega teabele.

4. Euroopa Parlament kui avaliku sektori hankija tagab, et salastatud lepingute sõlmimisel tööstus- või muude üksustega järgitakse käesolevas otsuses sätestatud ja lepingus viidatud tööstusjulgeoleku miinimumstandardeid.

B. **SALASTATUD LEPINGUTE TURVAELEMENDID**

B.1. ***Salastatuse taseme määramise juhend***

5. Enne salastatud lepingu pakkumismenetluse algatamist või sellise lepingu sõlmimist määrab Euroopa Parlament kui avaliku sektori hankija kindlaks pakkujatele ja töövõtjatele edastatava teabe salastatuse taseme ning samuti töövõtjate poolt koostatava teabe salastatuse taseme. Selleks koostab Euroopa Parlament lepingu täitmiseks kasutatava salastatuse taseme määramise juhendi.

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

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

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

B.2. ***Julgeolekuaspekte käsitlev dokument***

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

8. Julgeolekuaspekte käsitlev dokument sisaldab sätteid, milles nõutakse, et töövõtja ja/või alltöövõtja järgiks käesolevas otsuses sätestatud miinimumstandardeid. Kõnealuste miinimumstandardite eiramine võib olla alus lepingu lõpetamiseks.

B.3. ***Programmi/projekti julgeolekujuhised***

9. Sõltuvalt ELi salastatud teabele juurdepääsu või selle käitlemist või säilitamist hõlmavate programmide või projektide ulatusest võib asjaomase programmi või projekti juhtimiseks määratud avaliku sektori hankija koostada konkreetsed programmi/projekti julgeolekujuhised.

C. **TÖÖTLEMISLUBA**

10. Töötlemisloa väljastab riiklik julgeolekuasutus või liikmesriigi muu pädev julgeolekuasutus tõendamaks vastavalt riigisisestele õigusaktidele, et tööstus- või muu üksus suudab oma rajatistes kaitsta (CONFIDENTIEL UE / EU CONFIDENTIAL või SECRET UE / EU SECRET) salastatuse tasemel või samaväärset ELi salastatud teavet. Töötlemisloa väljastamise kinnitus esitatakse Euroopa Parlamendile kui avaliku sektori hankijale enne, kui töövõtjale või alltöövõtjale või potentsiaalsele töövõtjale või alltöövõtjale edastatakse ELi salastatud teavet või võimaldatakse sellele juurdepääs.

11. Töötlemisloa väljastamisel:

a) hinnatakse tööstus- või muu üksuse usaldusväärsust;

b) hinnatakse omandiõigust, kontrolli ja/või lubamatu mõju võimalikkust, mida saaks turvariskiks pidada;

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

d) kontrollitakse, et CONFIDENTIEL UE / EU CONFIDENTIAL või SECRET UE / EU SECRET salastatuse tasemega teabele juurdepääsu vajavate juhtkonna liikmete, omanike ja töötajate julgeolekustaatus on kindlaks määratud käesolevas otsuses sätestatud nõuete kohaselt; ja

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

12. Kui see on asjakohane, teavitab Euroopa Parlament avaliku sektori hankijana asjaomast riiklikku julgeolekuasutust või muud pädevat julgeolekuasutust sellest, et lepingueelses etapis või lepingu täitmiseks on vaja töötlemisluba. Töötlemis- või juurdepääsuluba on lepingueelses etapis nõutav, kui pakkumismenetluse käigus on vaja väljastada CONFIDENTIEL UE / EU CONFIDENTIAL või SECRET UE / EU SECRET salastatuse tasemega teavet.

13. Kui nõutakse töötlemisluba, ei anna avaliku sektori hankija salastatud lepingut eelistatud pakkujale täitmiseks enne, kui on saadud kinnitus selle liikmesriigi riiklikult julgeolekuasutuselt või muult pädevalt julgeolekuasutuselt, kus on asjaomase töövõtja või alltöövõtja asukoht, et on väljastatud nõuetekohane töötlemisluba.

14. Töötlemisloa väljastanud mis tahes pädev julgeolekuasutus teavitab Euroopa Parlamenti kui avaliku sektori hankijat kõigist töötlemisloaga seotud muudatustest. All-lepingust teavitatakse vastavalt pädevat julgeolekuasutust.

15. Töötlemisloa tühistamine asjaomase riikliku julgeolekuasutuse või muu pädeva julgeolekuasutuse poolt on Euroopa Parlamendile piisav alus avaliku sektori hankijana salastatud lepingu lõpetamiseks või pakkuja hankekonkursilt kõrvaldamiseks.

D. **SALASTATUD LEPINGUD JA ALL-LEPINGUD**

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

17. Salastatud lepingu või all-lepingu sõlmimise järel teavitab Euroopa Parlament avaliku sektori hankijana töövõtja või alltöövõtja riiklikku julgeolekuasutust ja/või muud pädevat julgeolekuasutust salastatud lepinguga seotud julgeolekusätetest.

18. Salastatud lepingute lõpetamisel teatab Euroopa Parlament avaliku sektori hankijana (ja/või all-lepingu puhul vajaduse korral pädev julgeolekuasutus) sellest viivitamata selle liikmesriigi riiklikule julgeolekuasutusele või muule pädevale julgeolekuasutusele, kus töövõtja või alltöövõtja on registreeritud.

19. Üldiselt nõutakse, et töövõtja või alltöövõtja tagastab salastatud lepingu või all-lepingu lõpetamisel tema valduses oleva salastatud teabe avaliku sektori hankijale.

20. Erisätted salastatud teabe hävitamiseks lepingu täitmise jooksul või lõpetamisel kehtestatakse julgeolekuaspekte käsitlevas dokumendis.

21. Kui töövõtjal või alltöövõtjal lubatakse salastatud teavet säilitada pärast lepingu lõppemist, järgib kõnealune töövõtja või alltöövõtja jätkuvalt käesolevas otsuses sisalduvaid miinimumstandardeid ning kaitseb ELi salastatud teabe konfidentsiaalsust.

22. Tingimused, mille alusel töövõtja võib sõlmida all-lepinguid, on määratletud nii pakkumiskutses kui ka lepingus.

23. Enne all-lepingu sõlmimist salastatud lepingu mis tahes osa täitmiseks taotleb töövõtja Euroopa Parlamendilt kui avaliku sektori hankijalt luba. All-lepinguid ei tohi sõlmida tööstus- või muude üksustega, mis on registreeritud kolmandas riigis, mis ei ole sõlminud liiduga teabeturbe lepingut.

24. Töövõtja vastutab selle eest, et oleks tagatud kõigi all-lepinguga seotud tegevuste teostamine kooskõlas käesolevas otsuses sätestatud miinimumnõuetega, ning ei anna ELi salastatud teavet alltöövõtjale ilma avaliku sektori hankija eelneva kirjaliku nõusolekuta.

25. Töövõtja või alltöövõtja koostatud või käideldava salastatud teabe suhtes teostab teabe koostaja õigusi avaliku sektori hankija.

E. **SALASTATUD LEPINGUTEGA SEOTUD KÜLASTUSED**

26. Kui Euroopa Parlamendil, töövõtjal või alltöövõtjal on salastatud lepingu täitmiseks vaja juurdepääsu CONFIDENTIEL UE / EU CONFIDENTIAL või SECRET UE / EU SECRET salastatuse tasemega teabele üksteise ruumides, korraldatakse külastused koostöös riiklike julgeolekuasutuste või muude asjaomaste pädevate julgeolekuasutusega. Riiklikud julgeolekuasutused võivad siiski seoses konkreetsete projektidega leppida kokku ka korra, mille kohaselt selliseid külastusi võib korraldada otse.

27. Kõigil külastajatel peab olema asjakohane juurdepääsuluba Euroopa Parlamendi lepinguga seotud salastatud teabele juurdepääsuks ja teadmisvajadus sellise teabe suhtes.

28. Külastajatele võimaldatakse juurdepääs vaid külastuse eesmärgiga seotud salastatud teabele.

F. **SALASTATUD TEABE EDASTAMINE JA VEDU**

29. Salastatud teabe elektroonilise edastamise suhtes kohaldatakse julgeolekuteate 3 asjakohaseid sätteid.

30. Salastatud teabe transpordi suhtes kohaldatakse julgeolekuteate 4 asjakohaseid sätteid ja asjakohast käitlemisjuhendit.

31. Salastatud materjali transportimise suhtes veosena kohaldatakse julgeolekukorra kindlaksmääramisel järgmisi põhimõtteid:

a) julgeolek kindlustatakse lähtekohast lõppsihtkohta transportimise kõigil etappidel;

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

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

d) enne CONFIDENTIEL UE / EU CONFIDENTIAL või SECRET UE / EU SECRET salastatuse tasemega või samaväärse materjali piiriülest vedu koostab saatja veoplaani ning peasekretär kiidab selle heaks;

e) veod toimuvad võimalikult täpselt väljumispunktist sihtpunkti ja need lõpetatakse nii kiiresti kui asjaolud seda võimaldavad;

f) võimaluse korral kulgeb teekond läbi liikmesriikide territooriumi.

G. **SALASTATUD TEABE EDASTAMINE KOLMANDATES RIIKIDES PAIKNEVATELE TÖÖVÕTJATELE**

32. Salastatud teave edastatakse kolmandates riikides paiknevatele töövõtjatele ja alltöövõtjatele vastavalt turvameetmetele, mis on kokku lepitud Euroopa Parlamendi kui avaliku sektori hankija ning selle asjaomase kolmanda riigi vahel, kus töövõtja on registreeritud.

H. **RESTREINT UE / EU RESTRICTED SALASTATUSE TASEMEGA TEABE KÄITLEMINE JA SÄILITAMINE**

33. Euroopa Parlamendil kui avaliku sektori hankijal on vastavalt vajadusele koostöös asjaomase liikmesriigi riikliku julgeolekuasutusega õigus korraldada lepingu tingimuste alusel külastusi töövõtjate / alltöövõtjate valdustesse, et kontrollida, kas lepingus nõutud asjakohased turvameetmed RESTREINT UE / EU RESTRICTED tasemel ELi salastatud teabe kaitsmiseks on kasutusele võetud.

34. Euroopa Parlament teavitab avaliku sektori hankijana riiklikke julgeolekuasutusi või muid pädevaid julgeolekuasutusi RESTREINT UE / EU RESTRICTED salastatuse tasemega teavet sisaldavatest lepingutest või all-lepingutest niivõrd, kuivõrd seda nõutakse riigisiseste õigusaktide kohaselt.

35. Töövõtjatelt või alltöövõtjatelt ja nende töötajatelt ei nõuta töötlemis- või juurdepääsuluba Euroopa Parlamendi poolt sõlmitud lepingute puhul, mis sisaldavad RESTREINT UE / EU RESTRICTED salastatuse tasemega teavet.

36. Avaliku sektori hankijana vaatab Euroopa Parlament läbi RESTREINT UE / EU RESTRICTED salastatuse tasemega teabele juurdepääsu eeldavate lepingute pakkumiskutsetele laekunud vastused, ilma et see piiraks töötlemis- või juurdepääsulubade suhtes riigisiseste õigusaktide kohaselt kehtestatud võimalike nõuete kohaldamist.

37. Tingimused, mille alusel töövõtja võib sõlmida all-lepinguid, on määratletud nii pakkumiskutses kui ka lepingus.

38. Kui leping hõlmab RESTREINT UE / EU RESTRICTED salastatuse tasemega teabe käitlemist töövõtja side- ja infosüsteemis, tagab Euroopa Parlament avaliku sektori hankijana, et lepingus või mis tahes all-lepingus täpsustatakse side- ja infosüsteemide akrediteerimiseks vajalikud tehnilised ja haldusnõuded, mis on vastavuses hinnatud riskiga ning milles on arvesse võetud kõik asjaomased tegurid. Selliste side- ja infosüsteemide akrediteerimise ulatus lepitakse kokku avaliku sektori hankija ja asjaomase riikliku julgeolekuasutuse vahel.

JULGEOLEKUTEADE 6

JULGEOLEKUNÕUETE RIKKUMINE NING KONFIDENTSIAALSE TEABE KADUMINE VÕI OHTUSATTUMINE

1. Julgeolekunõuete rikkumine toimub sellise tegevuse või tegevusetuse tagajärjel, mis on vastuolus käesoleva otsusega ning mis võib konfidentsiaalset teavet ohustada või selle ohtu seada.

2. Konfidentsiaalne teave satub ohtu siis, kui see on tervikuna või osaliselt sattunud vastavat luba mitteomavate isikute kätte, st niisuguste isikute kätte, kes ei ole läbinud vastava taseme julgeolekukontrolli või kellel ei ole vajalikku teadmisvajadust, või kui kõnealuse teabe sattumine selliste isikute kätte on tõenäoline.

3. Konfidentsiaalne teave võib sattuda ohtu hooletuse, ettevaatamatuse või ebadiskreetsuse tagajärjel, samuti liidu vastu suunatud teenistuste tegevuse või õõnestusorganisatsioonide tõttu.

4. Kui peasekretär avastab tõendatud või oletatava julgeolekunõuete rikkumise, konfidentsiaalse teabe kadumise või ohtusattumise või teda teavitatakse sellest, teeb ta järgmist:

a) teeb kindlaks asjaolud;

b) hindab ja minimeerib tekitatud kahju;

c) võtab meetmeid kordumise ennetamiseks;

d) teavitab konfidentsiaalse teabe koostanud või edastanud kolmanda osapoole või liikmesriigi pädevat asutust.

Kui asi puudutab Euroopa Parlamendi liiget, tegutseb peasekretär koostöös Euroopa Parlamendi presidendiga.

Kui teave on saadud muult liidu institutsioonilt, tegutseb peasekretär kooskõlas salastatud teabe suhtes kehtivate asjakohaste turvameetmetega ning korraga, mis on kehtestatud komisjoniga sõlmitud raamkokkuleppe või nõukoguga sõlmitud institutsioonidevahelise kokkuleppe kohaselt.

5. Kõiki isikuid, kes peavad käitlema konfidentsiaalset teavet, teavitatakse põhjalikult julgeolekumenetlustest, ebadiskreetsete vestluste ohtlikkusest ning sellest, millised peaksid olema nende suhted meediaga, ning vajaduse korral kirjutavad nad alla deklaratsioonile, et nad ei avalda konfidentsiaalse teabe sisu kolmandatele isikutele, et nad järgivad salastatud teabe kaitsmise kohustust ja et nad on teadlikud tagajärgedest, mis kaasnevad selle tegemata jätmisega. Salastatud teabele juurdepääsu saamist või selle kasutamist isiku poolt, keda ei ole vastavalt teavitatud ja kes ei ole vastavale deklaratsioonile alla kirjutanud, peetakse julgeolekunõuete rikkumiseks.

6. Euroopa Parlamendi liikmed, Euroopa Parlamendi ametnikud ja fraktsioonides töötavad muud Euroopa Parlamendi töötajad ning töövõtjad teavitavad viivitamata peasekretäri igast märgatud julgeolekunõuete rikkumise, konfidentsiaalse teabe kadumise või ohtusattumise juhtumist.

7. Iga isiku suhtes, kes on vastutav konfidentsiaalse teabe ohtusattumise eest, kohaldatakse distsiplinaarmeetmeid vastavalt asjaomastele õigusnormidele. Niisugused meetmed ei piira mis tahes õiguslike meetmete võtmist vastavalt kohaldatavale õigusele.

8. Piiramata muude õiguslike meetmete võtmist, toovad Euroopa Parlamendi ametnike ja fraktsioonides töötavate Euroopa Parlamendi muude töötajate poolt toime pandud rikkumised kaasa personalieeskirjade VI peatükis sätestatud menetluste ja karistuste kohaldamise.

9. Piiramata muude õiguslike meetmete võtmist, kohaldatakse Euroopa Parlamendi liikmete poolt toime pandud rikkumiste suhtes Euroopa Parlamendi kodukorra artikli 9 lõikes 2 ning artiklites 152, 153 ja 154 sätestatud menetlusi.