KOMISJONI OTSUS (EL, Euratom) 2019/1963,

17. oktoober 2019,

millega kehtestatakse tööstusjulgeoleku rakenduseeskirjad, mida kohaldatakse salastatud hankelepingute suhtes

EUROOPA KOMISJON,

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

võttes arvesse Euroopa Aatomienergiaühenduse asutamislepingut, eriti selle artiklit 106,

võttes arvesse komisjoni 13. märtsi 2015. aasta otsust (EL, Euratom) 2015/443 komisjoni julgeoleku kohta, ([1])

võttes arvesse komisjoni 13. märtsi 2015. aasta otsust (EL, Euratom) 2015/444 ELi salastatud teabe kaitseks vajalike julgeolekunormide kohta, ([2])

võttes arvesse komisjoni 10. jaanuari 2017. aasta otsust (EL, Euratom) 2017/46 Euroopa Komisjoni side- ja infosüsteemide turvalisuse kohta, ([3])

olles konsulteerinud komisjoni julgeolekualase eksperdirühmaga vastavalt otsuse (EL, Euratom) 2015/444 artikli 41 lõikele 5

ning arvestades järgmist:

(1) Otsuse (EL, Euratom) 2015/444 artiklites 41, 42, 47 ja 48 on sätestatud, et kõnealuse otsuse 6. peatüki täiendamiseks ja toetamiseks tuleb tööstusjulgeoleku rakenduseeskirjades ette näha üksikasjalikumad sätted, millega reguleeritakse selliseid küsimusi nagu pakkumismenetlus, salastatud lepingute sõlmimine, töötlemisload, juurdepääsuload, külastused ning Euroopa Liidu salastatud teabe edastamine ja vedu.

(2) Otsuses (EL, Euratom) 2015/444 on sätestatud, et salastatud lepinguid täidetakse tihedas koostöös riikliku julgeolekuasutusega, määratud julgeolekuasutusega või asjaomase liikmesriigi muu pädeva asutusega. Liikmesriigid on kokku leppinud, et kõik nende jurisdiktsiooni kuuluvad üksused, kes võivad saada komisjonist pärit salastatud teavet või seda luua, on läbinud nõuetekohase julgeolekukontrolli ja suudavad tagada piisava kaitse, mis on võrdne sellega, mis tagatakse vastava salastusmärkega ELi salastatud teabele Euroopa Liidu Nõukogu julgeolekunormide kohaselt, nagu on sätestatud nõukogus kokku tulnud Euroopa Liidu liikmesriikide vahelises kokkuleppes, mis käsitleb Euroopa Liidu huvides vahetatava salastatud teabe kaitset (2011/C 202/05) ([4]).

(3) Nõukogu, komisjon ning liidu välisasjade ja julgeolekupoliitika kõrge esindaja on kokku leppinud, et tagavad oma spetsiifilisi institutsioonilisi ja organisatsioonilisi vajadusi arvesse võttes ELi salastatud teabe kaitset käsitlevate julgeolekueeskirjade kohaldamisel maksimaalse järjepidevuse kooskõlas deklaratsioonidega, mis on lisatud nõukogu otsuse 2013/488/EL ([5]) (ELi salastatud teabe kaitseks vajalike julgeolekueeskirjade kohta) vastuvõtmise istungi protokollile.

(4) Seepärast tuleks komisjoni tööstusjulgeoleku rakenduseeskirjades, mida kohaldatakse salastatud hankelepingute suhtes, samuti tagada maksimaalne järjepidevus ja arvesse võtta nõukogu julgeolekukomitee 13. detsembri 2016. aasta tööstusjulgeolekut käsitlevaid suuniseid ning Euroopa Parlamendi ja nõukogu direktiivi 2009/81/EÜ artikleid 7 ja 22 ([6]).

(5) 4. mail 2016 võttis komisjon vastu otsuse, ([7]) millega volitatakse julgeolekuküsimuste eest vastutavat komisjoni liiget võtma komisjoni nimel ja tema vastutusel vastu otsuse (EL, Euratom) 2015/444 artiklis 60 sätestatud rakenduseeskirjad,

([1]) ELT L 72, 17.3.2015, lk 41.
([2]) ELT L 72, 17.3.2015, lk 53.
([3]) ELT L 6, 11.1.2017, lk 40.
([4]) ELT C 202, 8.7.2011, lk 13.
([5]) Nõukogu 23. septembri 2013. aasta otsus 2013/488/EL ELi salastatud teabe kaitseks vajalike julgeolekueeskirjade kohta (ELT L 274, 15.10.2013, lk 1).
([6]) Euroopa Parlamendi ja nõukogu 13. juuli 2009. aasta direktiiv 2009/81/EÜ, millega kooskõlastatakse teatavate kaitse- ja julgeolekuvaldkonnas ostjate poolt sõlmitavate ehitustööde ning asjade ja teenuste riigihankelepingute sõlmimise kord (ELT L 216, 20.8.2009, lk 76).
([7]) Komisjoni 4. mai 2016. aasta otsus julgeolekuga seotud volituse kohta [C(2016) 2797 final].

ON VASTU VÕTNUD KÄESOLEVA OTSUSE:

1. PEATÜKK

ÜLDSÄTTED

Artikkel 1

Reguleerimisese ja kohaldamisala

1. Käesoleva otsusega kehtestatakse otsuse (EL, Euratom) 2015/444 ja eelkõige selle 6. peatüki rakendamise toetamiseks tööstusjulgeoleku rakenduseeskirjad, mida kohaldatakse salastatud hankelepingute suhtes.

2. Otsusega sätestatakse erinõuded, et tagada ELi salastatud teabe kaitsmine ettevõtjate poolt lepingueelses etapis, Euroopa Komisjoni sõlmitud salastatud lepingute kogu kehtivusaja vältel ja komisjoni lepinglaste poolt sõlmitud all-lepingutes.

3. Käesolevas otsuses käsitletakse järgmise salastatuse tasemega teavet:

a) RESTREINT UE/EU RESTRICTED;

b) CONFIDENTIEL UE/EU CONFIDENTIAL;

c) SECRET UE/EU SECRET.

Artikkel 2

Komisjoni ülesanded

1. Täites lepingu sõlmijana finantsmääruses ([8]) kirjeldatud ülesandeid, tagab komisjoni eelarvevahendite käsutaja, et salastatud leping vastab otsuse (EL, Euratom) 2015/444 6. peatükis ja käesolevates rakenduseeskirjades ning, kui see on asjakohane, hanketeates või pakkumuse esitamise ettepanekus sätestatud tööstusjulgeoleku miinimumnõuetele, ning et nendest nõuetest peetakse rakendamise käigus kinni.

2. Selleks küsib asjaomane eelarvevahendite käsutaja igas etapis nõu komisjoni julgeolekuasutuselt salastatud lepingu, programmi või projekti julgeolekuaspektide kohta ning teavitab sõlmitud lepingutest kohalikku julgeolekuametnikku. Konkreetsete teemade salastatuse taseme üle otsustab lepingu sõlmija ning võtab nõuetekohaselt arvesse salastatuse taseme määramise juhendit.

3. Rakenduseeskirjade nõuete täitmisel teeb komisjoni julgeolekuasutus tihedat koostööd asjaomaste liikmesriikide riiklike ja määratud julgeolekuasutustega, eelkõige töötlemis- ja juurdepääsulubade, külastuste korra ja veoplaanide valdkonnas.

2. PEATÜKK

SALASTATUD LEPINGU PAKKUMISMENETLUS

Artikkel 3

Aluspõhimõtted

1. Salastatud leping sõlmitakse üksnes liikmesriigis registreeritud ettevõtjaga, kolmandas riigis registreeritud ettevõtjaga või rahvusvahelise organisatsiooni poolt asutatud ettevõtjaga, kui kõnealune kolmas riik või rahvusvaheline organisatsioon on sõlminud Euroopa Liiduga salastatud teabe kaitse lepingu või komisjoniga halduskokkuleppe ([9]).

2. Enne kui algatatakse pakkumismenetlus salastatud lepingu sõlmimiseks, määrab lepingu sõlmija kindlaks pakkujatele esitatava teabe salastatuse taseme. Samuti määrab lepingu sõlmija kindlaks kõrgeima salastatuse taseme mis tahes teabe puhul, mis luuakse lepingu, programmi või projekti täitmise käigus, või vähemalt koostatava või töödeldava teabe eeldatava mahu ja liigi ning vajaduse salastatud side- ja infosüsteemi järele.

([8]) Euroopa Parlamendi ja nõukogu 18. juuli 2018. aasta määrus (EL, Euratom) 2018/1046, mis käsitleb liidu üldeelarve suhtes kohaldatavaid finantsreegleid ja millega muudetakse määrusi (EL) nr 1296/2013, (EL) nr 1301/2013, (EL) nr 1303/2013, (EL) nr 1304/2013, (EL) nr 1309/2013, (EL) nr 1316/2013, (EL) nr 223/2014 ja (EL) nr 283/2014 ja otsust nr 541/2014/EL ning tunnistatakse kehtetuks määrus (EL, Euratom) nr 966/2012 (ELT L 193, 30.7.2018, lk 1).

([9]) Loetelu ELi sõlmitud lepingutest ja Euroopa Komisjoni sõlmitud halduskokkulepetest, mille alusel võib ELi salastatud teavet vahetada kolmandate riikide ja rahvusvaheliste organisatsioonidega, leiab komisjoni veebisaidilt.

3. Lepingu sõlmija tagab, et salastatud lepingu sõlmimise teates antakse teavet salastatud teabega seotud julgeolekualaste erikohustuste kohta. I lisas on näidisvorm lepinguteates esitatava teabe jaoks.

4. Lepingu sõlmija tagab, et RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL ja SECRET UE/EU SECRET tasemel salastatud teave avaldatakse pakkujatele alles pärast seda, kui nad on alla kirjutanud konfidentsiaalsuskokkuleppele, mis kohustab neid töötlema ja kaitsma ELi salastatud teavet kooskõlas otsuse (EL, Euratom) 2015/444 ja selle rakenduseeskirjadega.

5. Kõigil lepinglastel, kellelt nõutakse CONFIDENTIEL UE/EU CONFIDENTIAL või SECRET UE/EU SECRET tasemel salastatud teabe töötlemist või säilitamist oma rajatistes kas salastatud lepingu täitmise või lepingueelsel etapil, peab olema nõutaval tasemel töötlemisluba. Allpool on esitatud kolm stsenaariumi, mis võivad esineda CONFIDENTIEL UE/EU CONFIDENTIAL või SECRET UE/EU SECRET tasemel ELi salastatud teavet sisaldava salastatud lepingu pakkumisetapis.

a) Juurdepääs CONFIDENTIEL UE/EU CONFIDENTIAL või SECRET UE/EU SECRET tasemel ELi salastatud teabele pakkumisetapis puudub.

   Kui lepinguteade või pakkumiskutse käsitleb lepingut, mis hõlmab CONFIDENTIEL UE/EU CONFIDENTIAL või SECRET UE/EU SECRET tasemel ELi salastatud teavet, kuid pakkujalt ei eeldata sellise teabe töötlemist pakkumisetapis, ei jäeta sellist pakkujat pakkumismenetlusest välja põhjusel, et tal puudub nõutaval tasemel töötlemisluba.

b) Juurdepääs CONFIDENTIEL UE/EU CONFIDENTIAL või SECRET UE/EU SECRET tasemel ELi salastatud teabele lepingu sõlmija objektil pakkumisetapis.

   Juurdepääs antakse pakkuja töötajatele, kellel on nõutaval tasemel juurdepääsuluba ja teadmisvajadus. Enne juurdepääsu andmist teeb lepingu sõlmija komisjoni julgeolekuasutuse kaudu vastava riikliku/määratud julgeolekuasutusega kindlaks, kas selles etapis on riigi õigusnormide kohaselt nõutav ka töötlemisluba.

c) CONFIDENTIEL UE/EU CONFIDENTIAL või SECRET UE/EU SECRET tasemel ELi salastatud teabe töötlemine või säilitamine pakkuja objektil pakkumisetapis.

   Kui lepinguteates või pakkumiskutses nõutakse pakkujatelt ELi salastatud teabe töötlemist või säilitamist oma objektil, peab pakkujal olema nõutaval tasemel töötlemisluba. Sellisel juhul hangib lepingu sõlmija komisjoni julgeolekuasutuse kaudu asjakohase riikliku/määratud julgeolekuasutuse kinnituse selle kohta, et pakkujal on asjakohane töötlemisluba. Juurdepääs võimaldatakse pakkuja töötajatele, kellel on nõutaval tasemel juurdepääsuluba ja teadmisvajadus.

6. Pakkumisetapis ja lepingu täitmiseks ei nõuta üldjuhul töötlemisluba RESTREINT UE/EU RESTRICTED tasemel salastatud teabele juurdepääsu saamiseks. Kui liikmesriik on oma õigusnormidega ette näinud, et RESTREINT UE/EU RESTRICTED tasemel salastatud lepingu või all-lepingu puhul on nõutav töötlemisluba, nagu on loetletud IV lisas, ei tohi see nõue tekitada täiendavaid kohustusi teistele liikmesriikidele ega välistada pakkujaid, lepinglasi ja all-lepinglasi sellistest liikmesriikidest, kus puudub töötlemisloa nõue juurdepääsu saamiseks vastavatest lepingutest/all-lepingutest saadavale UE/EU RESTRICTED tasemel salastatud teabele või konkureerimiseks sellise lepingu sõlmimiseks. Neid lepinguid täidetakse liikmesriikides kooskõlas seal kehtivate siseriiklike õigusnormidega.

7. Kui salastatud lepingu täitmiseks on nõutav töötlemisluba, esitab lepingu sõlmija komisjoni julgeolekuasutuse kaudu lepinglase riiklikule/määratud julgeolekuasutusele taotluse, kasutades selleks töötlemisloa teabelehte. III lisa D liites on esitatud töötlemisluba käsitleva teabelehe näidis ([10]). Salastatud lepingut ei sõlmita enne, kui lepinglase riiklik/määratud julgeolekuasutus on pakkuja töötlemisloa kinnitanud. Töötlemisluba käsitlevale teabelehele tuleb võimaluse korral vastata kümne tööpäeva jooksul taotluse esitamise kuupäevast.

([10]) Muud kasutatavad vormid võivad oma ülesehituse poolest erineda käesolevates rakenduseeskirjades esitatud näidisest.

Artikkel 4

All-lepingu sõlmimine salastatud lepingu korral

1. Tingimused, mille alusel komisjoniga salastatud lepingu sõlminud lepinglane võib sõlmida all-lepingu, määratakse kindlaks pakkumiskutses ja lepingudokumentides. Kui salastatud leping võimaldab teatavate selle osade täitmiseks kasutada all-lepinguid, tuleb selleks saada lepingu sõlmija eelnev kirjalik nõusolek. Enne nõusoleku andmist konsulteerib lepingu sõlmija komisjoni julgeolekuasutusega.

2. Salastatud lepingu all-leping sõlmitakse üksnes liikmesriigis registreeritud ettevõtjaga, kolmandas riigis registreeritud ettevõtjaga või rahvusvahelise organisatsiooni poolt asutatud ettevõtjaga, kui kõnealune kolmas riik või rahvusvaheline organisatsioon on sõlminud Euroopa Liiduga salastatud teabe kaitse lepingu või komisjoniga halduskokkuleppe ([11]).

3. PEATÜKK

KOMISJONI SALASTATUD LEPINGUTE SÕLMIMINE

Artikkel 5

Aluspõhimõtted

1. Salastatud lepingu sõlmimisel tagab lepingu sõlmija koos komisjoni julgeolekuasutusega, et lepinglase kohustus kaitsta ELi salastatud teavet, mis on tehtud talle kättesaadavaks või loodud lepingu täitmise käigus, on lepingu lahutamatu osa. Lepinguga seotud konkreetsed julgeolekunõuded esitatakse julgeolekuaspekte käsitlevas dokumendis. Julgeolekuaspekte käsitleva dokumendi näidisvorm on esitatud III lisas.

2. Enne salastatud lepingule allakirjutamist koostab lepingu sõlmija, olles konsulteerinud komisjoni julgeolekuasutusega, teabe salastatuse taseme määramise juhendi, milles käsitletakse ülesandeid, mida tuleb lepingu, programmi või projekti raames täita, aga ka nende ülesannete täitmise käigus loodud teavet, kui see on asjakohane. Salastatuse taseme määramise juhend on julgeolekuaspekte käsitleva dokumendi osa.

3. Programmi või projekti suhtes kohaldatavad konkreetsed julgeolekunõuded nähakse ette programmi (või projekti) julgeolekujuhistes. Programmi julgeolekujuhised võib koostada III lisas sätestatud julgeolekuaspekte käsitleva dokumendi näidise alusel. Programmi julgeolekujuhised töötab välja programmi või projekti haldav komisjoni talitus tihedas koostöös komisjoni julgeolekuasutusega ning esitab selle arvamuse saamiseks komisjoni julgeolekualasele eksperdirühmale. Kui leping on osa programmist või projektist, millel on oma julgeolekujuhised, koostatakse lepingu julgeolekuaspekte käsitlev dokument lihtsustatud kujul ja see peab sisaldama viidet programmi või projekti julgeolekujuhiste vastavatele sätetele.

4. Lepingu sõlmijat käsitatakse lepingu täitmiseks loodud ja töödeldava salastatud teabe koostajana.

5. Lepingu sõlmija teavitab komisjoni julgeolekuasutuse kaudu kõiki lepinglaste ja all-lepinglaste riiklikke/määratud julgeolekuasutusi salastatud lepingute või all-lepingute sõlmimisest ning selliste lepingute või all-lepingute pikendamistest või ennetähtaegsest lõpetamisest. Riigipõhiste nõuete loetelu on esitatud IV lisas.

6. Leping, mis sisaldab RESTREINT UE/EU RESTRICTED tasemel salastatud teavet, peab sisaldama julgeolekuklauslit, millega muudetakse lepinglasele siduvaks III lisa E liites sätestatud nõuded. Selline leping peab hõlmama julgeolekuaspekte käsitlevat dokumenti, milles nähakse vähemalt ette RESTREINT UE/EU RESTRICTED tasemel salastatud teabe töötlemise nõuded, sealhulgas infokindluse aspektid ja erinõuded, mida lepingu sõlmija volitatud lepinglane peab täitma, et saada akrediteering oma infosüsteemidele, kus töödeldakse RESTREINT UE/EU RESTRICTED salastatuse tasemega teavet.

([11]) Loetelu ELi lepingutest ja Euroopa Komisjoni halduskokkulepetest, mille alusel võib ELi salastatud teavet vahetada kolmandate riikide ja rahvusvaheliste organisatsioonidega, leiab komisjoni veebisaidilt.

7. Kui pakkujatele või võimalikele lepinglastele tehakse kättesaadavaks RESTREINT UE/EU RESTRICTED salastatuse tasemega teave, lisatakse lõikes 6 nimetatud miinimumnõuded pakkumusse või pakkumisetapis sõlmitud asjakohastesse konfidentsiaalsuskokkulepetesse.

8. Kui see on nõutav liikmesriigis kehtivate õigusnormidega, tagab riiklik/määratud julgeolekuasutus, et tema jurisdiktsiooni alla kuuluvad lepinglased või all-lepinglased järgivad RESTREINT UE/EU RESTRICTED tasemel salastatud teabe kaitseks kehtestatud julgeolekusätteid ja teeb kontrollkäike tema territooriumil asuvatesse lepinglaste rajatistesse. Kui riiklik/määratud julgeolekuasutus ei ole selleks kohustatud, tagab lepingu sõlmija, et lepinglane rakendab III lisas sätestatud julgeolekusätteid.

Artikkel 6

Lepinglase ja all-lepinglase töötajate juurdepääs ELi salastatud teabele

1. Komisjoni talitus kui lepingu sõlmija tagab, et salastatud leping sisaldab sätteid, mille kohaselt lepinglase või all-lepinglase töötajatele, kellel on salastatud lepingu või all-lepingu täitmiseks vaja juurdepääsu ELi salastatud teabele, antakse selline juurdepääs ainult siis, kui:

a) on kindlaks tehtud, et neil on teadmisvajadus;

b) asjaomane riiklik/määratud julgeolekuasutus või mis tahes muu pädev julgeolekuasutus on neile andnud nõutaval tasemel juurdepääsuloa CONFIDENTIEL UE/EU CONFIDENTIAL või SECRET UE/EU SECRET tasemel salastatud teabele;

c) neid on teavitatud ELi salastatud teabe kaitseks kohaldatavatest julgeolekunormidest ning nad on kinnitanud oma vastutust seoses kõnealuse teabe kaitsmisega.

2. Kui lepinglane või all-lepinglane soovib tööle võtta kolmanda riigi kodaniku sellisele ametikohale, kus on nõutav juurdepääs CONFIDENTIEL UE/EU CONFIDENTIAL või SECRET UE/EU SECRET tasemel ELi salastatud teabele, vastutab lepinglane või all-lepinglane sellise isiku julgeolekukontrolli menetluse algatamise eest kooskõlas siseriiklike õigusnormidega, mida kohaldatakse ELi salastatud teabele juurdepääsu andmise asukohas.

4. PEATÜKK

SALASTATUD LEPINGUTEGA SEOTUD KÜLASTUSED

Artikkel 7

Aluspõhimõtted

1. Kui komisjoni, lepinglase või all-lepinglase töötajatel on salastatud lepingu täitmiseks vaja üksteise objektidel juurdepääsu CONFIDENTIEL UE/EU CONFIDENTIAL või SECRET UE/EU SECRET tasemel salastatud teabele, tuleb külastusi korraldada koostöös riiklike/määratud julgeolekuasutuste või muude pädevate julgeolekuasutusega.

2. Lõikes 1 osutatud külastuste suhtes kehtivad järgmised nõuded:

a) külastusel peab olema ametlik eesmärk, mis on seotud komisjoni sõlmitud salastatud lepinguga;

b) igal külastajal peab olema nõutaval tasemel juurdepääsuluba ja teadmisvajadus, et saada juurdepääs ELi salastatud teabele, mis on tehtud kättesaadavaks või loodud komisjoni sõlmitud salastatud lepingu täitmise käigus.

Artikkel 8

Külastustaotlused

1. Külastus, mille lepinglane teeb teise lepinglase rajatisesse või komisjoni objektile ning millega kaasneb juurdepääs CONFIDENTIEL UE/EU CONFIDENTIAL või SECRET UE/EU SECRET tasemel salastatud teabele, korraldatakse järgmise korra kohaselt:

a) külastajat lähetava rajatise julgeolekuametnik täidab külastustaotluse vormi kõik asjakohased osad ning esitab taotluse rajatise riiklikule/määratud julgeolekuasutusele. Külastustaotluse näidisvorm on esitatud III lisa C liites;

b) lähetava rajatise riiklik/määratud julgeolekuasutus kinnitab külastaja juurdepääsuloa enne külastustaotluse esitamist vastuvõtva rajatise riiklikule/määratud julgeolekuasutusele (või komisjoni julgeolekuasutusele, kui külastatakse komisjoni objekti);

c) lähetava rajatise julgeolekuametnik hangib seejärel oma riiklikult/määratud julgeolekuasutuselt vastuvõtva rajatise riikliku/määratud julgeolekuasutuse (või komisjoni julgeolekuasutuse) vastuse, millega külastustaotlus kas rahuldatakse või lükatakse tagasi;

d) külastustaotlus loetakse heakskiidetuks, kui vastuväiteid ei ole esitatud hiljemalt viis tööpäeva enne külastuse kuupäeva.

2. Külastus, mille komisjoni ametnik teeb lepinglase rajatisesse ning millega kaasneb juurdepääs CONFIDENTIEL UE/EU CONFIDENTIAL või SECRET UE/EU SECRET tasemel salastatud teabele, korraldatakse järgmise korra kohaselt:

a) külastaja täidab külastustaotluse vormi kõik asjakohased osad ja esitab selle komisjoni julgeolekuasutusele;

b) komisjoni julgeolekuasutus kinnitab külastaja juurdepääsuloa enne külastustaotluse esitamist vastuvõtva rajatise riiklikule/määratud julgeolekuasutusele;

c) komisjoni julgeolekuasutus hangib vastuvõtva rajatise riiklikult/määratud julgeolekuasutuselt vastuse, millega külastustaotlus kas rahuldatakse või lükatakse tagasi;

d) külastustaotlus loetakse heakskiidetuks, kui viie tööpäeva jooksul enne külastuse algust ei esitata vastuväiteid.

3. Külastustaotlus võib olla ühekordne või hõlmata korduvaid külastusi. Korduvate külastuste puhul võib külastustaotluse kehtivusaeg olla kuni üks aasta alates taotletud alguskuupäevast.

4. Külastustaotluse kehtivusaeg ei tohi ületada külastaja juurdepääsuloa kehtivust.

5. Külastustaotlus tuleks üldjuhul esitada vastuvõtva rajatise pädevale julgeolekuasutusele vähemalt 15 tööpäeva enne külastuse kuupäeva.

Artikkel 9

Külastuste kord

1. Enne kui külastajatele antakse juurdepääs ELi salastatud teabele, peab vastuvõtva rajatise julgeolekuametnik järgima külastusega seonduvat julgeolekukorda ja eeskirju, mille on kehtestanud tema riiklik/määratud julgeolekuasutus.

2. Külastaja tõendab oma isikut vastuvõtvasse rajatisse saabumisel, esitades selleks kehtiva isikutunnistuse või passi. Identifitseerimisandmed peavad vastama külastustaotluses esitatud andmetele.

3. Vastuvõttev rajatis tagab, et kõigi külastajate andmed säilitatakse, sealhulgas nende nimed, esindatav organisatsioon, juurdepääsuloa kehtivuse lõppkuupäev, külastuse kuupäev ja külastatud isikute nimed. Andmeid säilitatakse vähemalt viis aastat või kauem, kui see on nõutav vastuvõtva rajatise asukohariigi õigusnormidega.

Artikkel 10

Otse korraldatavad külastused

1. Riiklik/määratud julgeolekuasutus ja komisjoni julgeolekuasutus võivad konkreetse projekti puhul kokku leppida korra, mille alusel võivad külastaja julgeolekuametnik ja külastatava rajatise julgeolekuametnik korraldada konkreetse salastatud lepinguga seonduvaid külastusi otse. Selleks kasutatakse III lisa C liites esitatud näidisvormi. Selline erimenetlus nähakse ette projekti julgeolekujuhistes või muudes konkreetsetes kokkulepetes. Sellistel juhtudel ei kohaldata artiklis 8 ja artikli 9 lõikes 1 sätestatud korda.

2. Külastused, millega kaasneb juurdepääs RESTREINT UE/EU RESTRICTED tasemel salastatud teabele, lepitakse kokku otse lähetava ja vastuvõtva üksuse vahel, ilma et tuleks järgida artiklis 8 ja artikli 9 lõikes 1 ette nähtud korda.

5. PEATÜKK

ELI SALASTATUD TEABE EDASTAMINE JA VEDU SALASTATUD LEPINGU TÄITMISE AJAL

Artikkel 11

Aluspõhimõtted

Lepingu sõlmija tagab, et kõik ELi salastatud teabe edastamise ja veoga seotud otsused on kooskõlas otsuse (EL, Euratom) 2015/444, selle rakenduseeskirjade ning salastatud lepingu tingimustega, mille hulka kuulub ka teabe koostaja nõusolek.

Artikkel 12

Elektrooniline töötlemine

1. ELi salastatud teavet töödeldakse ja edastatakse elektrooniliselt kooskõlas otsuse (EL, Euratom) 2015/444 5. ja 6. peatüki ning selle rakenduseeskirjade sätetega.

Lepinglasele kuuluvad side- ja infosüsteemid, mida kasutatakse ELi salastatud teabe töötlemiseks lepingu täitmise eesmärgil („lepinglase side- ja infosüsteemid“), peavad olema vastutava turvalisuse akrediteerimise asutuse poolt akrediteeritud. ELi salastatud teabe elektrooniline edastamine peab olema kaitstud otsuse (EL, Euratom) 2015/444 artikli 36 lõike 4 kohaselt heakskiidetud krüptovahenditega. TEMPEST-turvameetmeid rakendatakse kooskõlas kõnealuse otsuse artikli 36 lõikega 6.

2. RESTREINT UE/EU RESTRICTED tasemel ELi salastatud teavet töötleva lepinglase side- ja infosüsteemide ning teiste süsteemide nendega sidumise turvalisuse akrediteerimise võib delegeerida lepinglase julgeolekuametnikule juhul, kui see on riigi õigusnormidega lubatud. Selle ülesande delegeerimise korral vastutab lepinglane julgeolekuaspekte käsitlevas dokumendis kirjeldatud julgeolekualaste miinimumnõuete rakendamise eest, kui tema side- ja infosüsteemides töödeldakse RESTREINT UE/EU RESTRICTED tasemel salastatud teavet. Riiklikule/määratud julgeolekuasutusele ja turvalisuse akrediteerimise asutusele jääb siiski vastutus lepinglase töödeldava RESTREINT UE/EU RESTRICTED tasemel salastatud teabe kaitsmise eest ja õigus kontrollida lepinglase võetud turvameetmeid. Lisaks peab lepinglane esitama lepingu sõlmijale ning, kui see on riigi õigusnormidega ette nähtud, pädevale riiklikule turvalisuse akrediteerimise asutusele kinnituse nõuetele vastavuse kohta, mis tõendab, et lepinglase side- ja infosüsteem ning teiste süsteemide sidumine sellega on akrediteeritud RESTREINT UE/EU RESTRICTED tasemel ELi salastatud teabe töötlemiseks ([12]).

Artikkel 13

Vedu kommertskulleriga

ELi salastatud teabe vedu kommertskulleriga toimub kooskõlas komisjoni nende otsuste asjakohaste sätetega, milles nähakse ette RESTREINT UE/EU RESTRICTED ja CONFIDENTIEL UE/EU CONFIDENTIAL salastatuse tasemega teabe töötlemise rakenduseeskirjad.

Artikkel 14

Vedu käsipostiga

1. Salastatud teabe käsipostiga veo suhtes kehtivad ranged julgeolekunõuded.

2. Lepinglase töötaja võib RESTREINT UE/EU RESTRICTED tasemel salastatud teavet ELi piires käsipostiga vedada, kui on täidetud järgmised nõuded:

a) kasutatav ümbrik või pakend on läbipaistmatu ega osuta selle sisu salastatusele;

([12]) Miinimumnõuded side- ja infosüsteemidele, milles töödeldakse RESTREINT UE/EU RESTRICTED tasemel ELi salastatud teavet, on sätestatud III lisa E liites.

b) salastatud teave on kogu aeg valdaja valduses;

c) ümbrikku ega pakendit ei avata teeloleku ajal.

3. Lähetav ja vastuvõttev üksus lepivad eelnevalt kokku, et lepinglase töötaja veab CONFIDENTIEL UE/EU CONFIDENTIAL ja SECRET UE/EU SECRET tasemel salastatud teavet ELi liikmesriigi piires käsipostiga. Lähetav asutus või rajatis teatab vastuvõtvale asutusele või rajatisele saadetise üksikasjad, sealhulgas viited, salastatuse taseme, eeldatava saabumisaja ja kulleri nime. Selline vedu käsipostiga on lubatud, kui on täidetud järgmised tingimused:

a) salastatud teavet veetakse kahekordses ümbrikus või pakendis;

b) välimine ümbrik või pakend on kaitstud ja sellel ei ole märget selle sisu salastatuse kohta, kuid sisemisele ümbrikule on märgitud salastatuse tase;

c) salastatud teave on kogu aeg valdaja valduses;

d) ümbrikku ega pakendit ei avata teeloleku ajal;

e) ümbrikku või pakendit veetakse lukustatavas portfellis või samaväärses heakskiidetud pakendis, mis on sellise suuruse ja kaaluga, et seda saab igal ajal selle valdaja valduses hoida; pagasiruumi ei tohi seda anda;

f) kulleril on tema pädeva julgeolekuasutuse välja antud kulleri sertifikaat, mille alusel tohib kuller salastatud saadetist vedada.

4. Kui lepinglase töötaja veab käsipostiga CONFIDENTIEL UE/EU CONFIDENTIAL ja SECRET UE/EU SECRET tasemel salastatud teavet ühest ELi liikmesriigist teise, kohaldatakse järgmisi täiendavaid nõudeid:

a) kuller vastutab salastatud materjali turvalise hoidmise eest kuni selle üleandmiseni saajale;

b) julgeolekunõuete rikkumise korral võib saatja riiklik/määratud julgeolekuasutus taotleda, et selle riigi ametiasutused, kus rikkumine toimus, viiksid läbi uurimise, esitaksid oma järeldused ja võtaksid vajaduse korral õiguslikke või muid meetmeid;

c) kullerit on teavitatud kõigist julgeolekualastest kohustustest, millest tuleb veo ajal kinni pidada, ja ta on seda kirjalikult kinnitanud;

d) juhised kullerile peavad olema lisatud kulleri sertifikaadile;

e) kullerile on esitatud saadetise kirjeldus ja teekond;

f) dokumendid tagastatakse riiklikule/määratud julgeolekuasutusele teekonna lõppemisel või hoitakse saaja jaoks järelevalve eesmärgil kättesaadavana;

g) kui toll, immigratsiooniasutus või piiripolitsei soovib saadetise läbi vaadata ja seda kontrollida, on neil lubatud saadetist piisavalt avada ja vaadelda, et oleks võimalik kinnitada, et saadetis ei sisalda muud kui deklareeritud materjali;

h) tollil tuleks austada ametlikke veodokumente ja kulleriga kaasas olevaid lubasid.

Kui toll avab saadetise, tuleb seda teha väljaspool kõrvaliste isikute nägemisulatust ja võimaluse korral kulleri juuresolekul. Kuller palub kontrolli teostavalt ametiasutuselt, et nad pakiksid saadetise ümber ja sulgeksid selle uuesti ning kinnitaksid kirjalikult, et saadetis avati nende poolt.

5. Kui lepinglase töötaja veab RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL ja SECRET UE/EU SECRET tasemel salastatud teavet kolmandasse riiki või rahvusvahelisele organisatsioonile, kohaldatakse vastavalt Euroopa Liidu või komisjoni ning asjaomase kolmanda riigi või rahvusvahelise organisatsiooni vahel sõlmitud salastatud teabe kaitse lepingu või halduskokkuleppe sätteid.

6. PEATÜKK

TALITLUSPIDEVUSE PLANEERIMINE

Artikkel 15

Talitluspidevuse plaanid ja taastamismeetmed

Komisjoni talitus kui lepingu sõlmija tagab, et salastatud lepingus on nõue, et lepinglane koostab erakorraliste olukordade jaoks talitluspidevuse plaanid, et kaitsta salastatud lepingu täitmisel töödeldavat ELi salastatud teavet, ning näeb nendes ette ennetus- ja taastamismeetmed, et minimeerida intsidentide mõju ELi salastatud teabe töötlemisele ja säilitamisele. Lepinglane teavitab lepingu sõlmijat oma talitluspidevuse plaanist.

Artikkel 16

Jõustumine

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

Brüssel, 17. oktoober 2019

Komisjoni nimel

presidendi eest

komisjoni liige

Günther OETTINGER

I LISA

HANKELEPINGU TEATES ESITATAV STANDARDTEAVE

(kohandatakse vastavalt kasutatud hanketeatele)

Lepingu puhul, mis sisaldab CONFIDENTIEL UE/EU CONFIDENTIAL või SECRET UE/EU SECRET tasemel salastatud teavet

Muud eritingimused (*kui neid kohaldatakse*)

Lepingu täitmisel kohaldatakse eritingimusi ● Jah ○ Ei

(*kui „Jah"*) Eritingimuste kirjeldus:

Leping hõlmab juurdepääsu CONFIDENTIEL UE/EU CONFIDENTIAL või SECRET UE/EU SECRET tasemel salastatud teabele, selle töötlemist ja/või säilitamist, mille suhtes kohaldatakse otsuses (EL, Euratom) 2015/444 ja selle rakenduseeskirjades [1] sätestatud julgeolekunorme, mis on vajalikud ELi salastatud teabe kaitseks.

Salastatud teavet töötleval lepinglase töötajal peab olema töötlemisluba ja juurdepääsuload.

Julgeolekualased erikohustused on lepingu osa (lepingule lisatud julgeolekuaspekte käsitlev dokument). All-lepingud on lubatud lepingu sõlmija eelneval kirjalikul nõusolekul; lisaks tuleb all-lepinglasel ja selle töötajatel järgida kõiki julgeolekueeskirju.

Lepingu puhul, mis sisaldab RESTREINT UE/EU RESTRICTED tasemel salastatud teavet

Muud eritingimused (*kui neid kohaldatakse*)

Lepingu täitmisel kohaldatakse eritingimusi ● Jah ○ Ei

(*kui „Jah"*) Eritingimuste kirjeldus:

Leping hõlmab või sisaldab juurdepääsu RESTREINT UE/EU RESTRICTED salastatuse tasemega teabele, selle töötlemist ja/või säilitamist, mille suhtes kohaldatakse otsuses (EL, Euratom) 2015/444 ja selle rakenduseeskirjades [2] sätestatud ELi salastatud teabe kaitseks vajalikke julgeolekunorme.

Julgeolekualased erikohustused on lepingu osa (lepingule lisatud julgeolekuaspekte käsitlev dokument). All-lepingud on lubatud lepingu sõlmija eelneval kirjalikul nõusolekul; lisaks tuleb all-lepinglasel ja selle töötajatel järgida kõiki julgeolekueeskirju.

[1] Lepingu sõlmija lisab viited pärast seda, kui rakenduseeskirjad on vastu võetud.
[2] Lepingu sõlmija lisab viited pärast seda, kui rakenduseeskirjad on vastu võetud.

II LISA

HANKELEPINGU TÜÜPTINGIMUSED

(kohandatakse vastavalt kasutatud lepingule)

ARTIKKEL XX

JULGEOLEKUALASED KOHUSTUSED

XX.1 ELi salastatud teave

Kui lepingu täitmine hõlmab ELi salastatud teabe kasutamist või loomist, tuleb seda teavet kuni selle salastatuse kustutamiseni käsitleda kooskõlas 1. lisas sätestatud julgeolekuaspekte käsitleva dokumendi ja salastatuse taseme määramise juhendiga ning otsuse (EL, Euratom) 2015/444 ja selle rakenduseeskirjadega ([1]).

Kõik salastatud teavet sisaldavad tulemid esitatakse vastavalt lepingu sõlmijaga kokku lepitud erimenetlusele.

Salastatud teavet hõlmavate ülesannete täitmiseks ei tohi sõlmida all-lepinguid ilma lepingu sõlmija eelneva sõnaselge kirjaliku nõusolekuta.

ELi salastatud teavet ei tohi avaldada ühelegi kolmandale isikule (sealhulgas all-lepinglasele) ilma lepingu sõlmija eelneva sõnaselge kirjaliku nõusolekuta.

([1]) Lepingu sõlmija lisab viited pärast seda, kui rakenduseeskirjad on vastu võetud.

III LISA

[(Raamlepingu) IV lisa]

JULGEOLEKUASPEKTE KÄSITLEV DOKUMENT

[Näidis]

A Liide

JULGEOLEKUNÕUDED

Lepingu sõlmija lisab julgeolekuaspekte käsitlevasse dokumenti järgmised julgeolekunõuded. Mõned sätted ei pruugi olla lepingu suhtes kohaldatavad. Need on esitatud nurksulgudes.

Sätete loetelu ei ole ammendav. Sõltuvalt salastatud lepingu laadist võib lisada täiendavaid sätteid.

ÜLDTINGIMUSED

[*N.B.: kohaldatakse kõigi salastatud lepingute suhtes*]

1. Käesolev julgeolekuaspekte käsitlev dokument on salastatud lepingu [või all-lepingu] lahutamatu osa ning selles kirjeldatakse lepinguga seonduvaid julgeolekunõudeid. Nende nõuete täitmata jätmine võib olla piisav alus lepingu lõpetamiseks.

2. Lepinglaste suhtes kehtivad kõik otsuses (EL, Euratom) 2015/444 ja selle rakenduseeskirjades [1] sätestatud kohustused.

3. Lepingu täitmisel loodud salastatud teabe salastatuse tasemeks tuleb märkida ELi salastatud teave, nagu on ette nähtud käesoleva dokumendi B liites esitatud salastatuse taseme määramise juhendis. Kõrvalekaldumine salastatuse taseme määramise juhendis sätestatud salastatuse tasemest on lubatud üksnes lepingu sõlmija kirjalikul loal.

4. Komisjonil kui lepingu sõlmijal on salastatud lepingu täitmiseks loodud ja töödeldud ELi salastatud teabe koostaja õigused.

5. Lepinglane või all-lepinglane ei tohi ilma lepingu sõlmija kirjaliku nõusolekuta kasutada lepingu sõlmija esitatud või tema nimel koosatud teavet või materjale ühelgi muul eesmärgil kui lepingu eesmärk.

6. Lepinglane uurib kõiki ELi salastatud teabega seotud julgeolekunõuete rikkumisi ja teavitab lepingu sõlmijat neist nii kiiresti kui võimalik. Lepinglane või all-lepinglane teatab viivitamata oma riiklikule julgeolekuasutusele või määratud julgeolekuasutusele, ning juhul, kui riigi õigusnormid seda võimaldavad, komisjoni julgeolekuasutusele kõigist juhtumitest, mille puhul on teada või alust kahtlustada, et lepingu kohaselt esitatud või loodud ELi salastatud teave on kadunud või avalikustatud volitamata isikutele.

7. Pärast lepingu lõppemist tagastab lepinglane või all-lepinglane lepingu sõlmijale kogu tema valduses oleva ELi salastatud teabe nii kiiresti kui võimalik. Kui see on otstarbekas, võib lepinglane või all-lepinglane ELi salastatud teabe selle tagastamise asemel hävitada. Seda tuleb teha kooskõlas selles riigis kehtivate õigusnormidega, kus lepinglane asub, komisjoni julgeolekuasutuse eelneval nõusolekul ja viimase juhiste kohaselt. ELi salastatud teave tuleb hävitada viisil, mis teeb võimatuks selle tervikliku või osalise taastamise.

8. Kui lepinglasel või all-lepinglasel on lubatud säilitada ELi salastatud teavet pärast lepingu lõpetamist või lõppemist, tuleb ELi salastatud teavet jätkuvalt kaitsta kooskõlas otsusega (EL, Euratom) 2015/444 (edaspidi „otsus 2015/444“) ja selle rakenduseeskirjadega [2].

9. ELi salastatud teabe elektrooniline töötlemine, käitlemine ja edastamine peab toimuma kooskõlas otsuse 2015/444 5. ja 6. peatüki sätetega. Need sisaldavad muu hulgas nõuet, et lepinglasele kuuluvad side- ja infosüsteemid, mida kasutatakse lepingu eesmärgil ELi salastatud teabe töötlemiseks (edaspidi „lepinglase side- ja infosüsteemid“), peavad olema akrediteeritud [3]; aga ka nõuet, et ELi salastatud teabe elektrooniline edastamine peab olema kaitstud krüptovahenditega, mis on heaks kiidetud vastavalt otsuse 2015/444 artikli 36 lõikele 4, ning et TEMPEST-turvameetmeid tuleb rakendada kooskõlas otsuse 2015/444 artikli 36 lõikega 6.

[1] Lepingu sõlmija lisab viited pärast seda, kui rakenduseeskirjad on vastu võetud.
[2] Lepingu sõlmija lisab viited pärast seda, kui rakenduseeskirjad on vastu võetud.
[3] Akrediteerimist korraldav asutus peab esitama lepingu sõlmijale komisjoni julgeolekuasutuse kaudu kinnituse nõuetele vastavuse kohta, kooskõlastades selle asjaomase riikliku turvalisuse akrediteerimise asutusega.

10. Lepinglane või all-lepinglane koostab talitluspidevuse plaani, et kaitsta salastatud lepingu täitmisel töödeldavat ELi salastatud teavet erakorralistes olukordades, ning kehtestab ennetus- ja taastamismeetmed, et minimeerida ELi salastatud teabe töötlemise ja säilitamisega seonduvate intsidentide mõju. Lepinglane või all-lepinglane teavitab lepingu sõlmijat oma talitluspidevuse plaanist.

LEPINGUD, MILLE PUHUL ON NÕUTAV JUURDEPÄÄS UE/EU RESTRICTED TASEMEL SALASTATUD TEABELE

11. Lepingu täitmiseks ei ole vaja juurdepääsuluba. RESTREINT UE/EU RESTRICTED tasemel salastatud teave või materjal peab olema kättesaadav üksnes lepinglase töötajatele, kellel on seda teavet vaja lepingu täitmiseks (*teadmisvajaduse põhimõte*) ja keda lepinglase julgeolekuametnik on teavitanud ülesannetest ja sellise teabe salajasuse kahjustamise või rikkumise tagajärgedest ning kes on kirjalikult kinnitanud, et on teadlikud ELi salastatud teabe kaitsmata jätmisega kaasnevatest tagajärgedest.

12. Välja arvatud juhul, kui lepingu sõlmija on andnud oma kirjaliku nõusoleku, ei tohi lepinglane ega all-lepinglane anda RESTREINT UE/EU RESTRICTED tasemel salastatud teabele ja materjalile juurdepääsu ühelegi muule üksusele või isikule kui tema töötaja, kellel on teadmisvajadus.

13. Lepinglane või all-lepinglane säilitab lepingu täitmise käigus loodud või esitatud salastatud teabe salastusmärked ega tohi salastatust ilma lepingu sõlmija kirjaliku nõusolekuta kustutada.

14. RESTREINT UE/EU RESTRICTED tasemel salastatud teavet või materjali, mis ei ole kasutusel, säilitatakse lukustatud kontorimööblis. Dokumendid toimetatakse kohale läbipaistmatus ümbrikus. Dokumendid on kogu aeg vedaja valduses ja neid ei tohi teeloleku ajal avada.

15. Lepinglane või all-lepinglane võib komisjonile edastada RESTREINT UE/EU RESTRICTED tasemel salastatud dokumente, kasutades kommertskullerteenust, postiteenust, käsiposti või elektroonilisi vahendeid. Selle käigus järgib lepinglane või all-lepinglane komisjonis välja antud programmi (projekti) julgeolekujuhiseid ja/või komisjoni töötusjulgeoleku rakenduseeskirju, mida kohaldatakse salastatud hankelepingute suhtes ([4]).

16. Kui RESTREINT UE/EU RESTRICTED salastatuse tasemega dokumente ei ole enam vaja, tuleb need hävitada viisil, mis teeb võimatuks nende tervikliku või osalise taastamise.

17. RESTREINT UE/EU RESTRICTED tasemel ELi salastatud teavet töötlevate lepinglase side- ja infosüsteemide ning teiste süsteemide nendega sidumise turvalisuse akrediteerimise võib lepinglase julgeolekuametnikule delegeerida juhul, kui riigi õigusnormid seda võimaldavad. Kui akrediteerimine delegeeritakse, vastutavad riiklikud/määratud julgeolekuasutused/turvalisuse akrediteerimise asutused jätkuvalt lepinglase töödeldava RESTREINT UE/EU RESTRICTED tasemel salastatud teabe eest ja neile jääb õigus kontrollida lepinglase võetud turvameetmeid. Lepinglane esitab lepingu sõlmijale ning, kui see on riiklike õigusnormidega ette nähtud, pädevale riiklikule turvalisuse akrediteerimise asutusele kinnituse nõuetele vastavuse kohta, mis tõendab, et lepinglase side- ja infosüsteem ning teiste süsteemide sidumine sellega on akrediteeritud RESTREINT UE/EU RESTRICTED tasemel salastatud teabe töötlemiseks.

RESTREINT UE/EU RESTRICTED TASEMEL SALASTATUD TEABE TÖÖTLEMINE SIDE- JA INFOSÜSTEEMIDES

18. Miinimumnõuded side- ja infosüsteemidele RESTREINT UE/EU RESTRICTED tasemel salastatud teabe töötlemiseks on sätestatud käesoleva julgeolekuaspekte käsitleva dokumendi E liites.

TINGIMUSED, MILLE KOHASELT VÕIB LEPINGLANE SÕLMIDA ALL-LEPINGU

19. Enne kui lepinglane sõlmib salastatud lepingu osa kohta all-lepingu, tuleb tal selleks saada komisjoni (lepingu sõlmija) asjaomase talituse luba.

([4]) Lepingu sõlmija lisab viited pärast seda, kui rakenduseeskirjad on vastu võetud.

20. All-lepingut ei sõlmita äriühinguga, mis on registreeritud väljaspool ELi asuvas riigis, ega üksusega, mis kuulub rahvusvahelisse organisatsiooni, kui kõnealune väljaspool ELi asuv riik või rahvusvaheline organisatsioon ei ole sõlminud ELiga salastatud teabe kaitse lepingut või komisjoniga halduskokkulepet.

21. Kui lepinglane on sõlminud all-lepingu, kohaldatakse lepingu julgeolekusätteid *mutatis mutandis* lepinglas(t)e ja tema (nende) töötajate suhtes. Sellisel juhul on lepinglase kohustus tagada, et kõik all-lepinglased kohaldavad neid põhimõtteid oma all-lepingute suhtes. Nõuetekohase julgeolekualase järelevalve tagamiseks teavitatakse lepinglase ja all-lepinglase riiklikke/määratud julgeolekuasutusi kõigist seonduvatest salastatud all-lepingutest, mis on sõlmitud CONFIDENTIEL UE/EU CONFIDENTIAL ja SECRET UE/EU SECRET salastatuse tasemel. Vajaduse korral esitatakse lepinglase ja all-lepinglase riiklikele/määratud julgeolekuasutustele koopia all-lepinguga seotud konkreetsetest julgeolekusätetest. Riiklikud/määratud julgeolekuasutused, keda tuleb RESTREINT UE/EU RESTRICTED tasemel salastatud lepingutega seotud julgeolekusätetest teavitada, on loetletud komisjoni tööstusjulgeoleku rakenduseeskirjades, mida kohaldatakse salastatud hankelepingute suhtes ([1]).

22. Lepinglane ei avalda ELi salastatud teavet all-lepinglasele ilma lepingu sõlmija eelneva sõnaselge kirjaliku nõusolekuta. Kui all-lepinglasele tuleb ELi salastatud teavet saata sageli või regulaarselt, võib lepingu sõlmija anda oma nõusoleku kindlaksmääratud ajaks (nt 12 kuud) või all-lepingu kestuse ajaks.

KÜLASTUSED

Kui CONFIDENTIEL UE/EU CONFIDENTIAL või SECRET UE/EU SECRET tasemel salastatud teavet hõlmava külastuse suhtes kohaldatakse tavapärast külastuse taotlemise korda, tuleb lepingu sõlmijal lisada lõiked 23, 24 ja 25 ning välja jätta lõige 26. Kui CONFIDENTIEL UE/EU CONFIDENTIAL või SECRET UE/EU SECRET tasemel salastatud teavet hõlmav külastus lepitakse kokku otse lähetava ja vastuvõtva asutuse vahel, tuleb lepingu sõlmijal välja jätta punktid 24 ja 25 ning lisada ainult punkt 26.

23. Külastused, mis hõlmavad juurdepääsu või võimalikku juurdepääsu RESTREINT UE/EU RESTRICTED tasemel salastatud teabele, lepitakse kokku otse lähetava ja vastuvõtva asutuse vahel, ilma et tuleks järgida punktides 24–26 kirjeldatud korda.

[24. Külastuste suhtes, mis hõlmavad juurdepääsu või võimalikku juurdepääsu CONFIDENTIEL UE/EU CONFIDENTIAL või SECRET UE/EU SECRET tasemel salastatud teabele, kohaldatakse järgmist korda:

a) külastajat lähetava rajatise julgeolekuametnik täidab kõik külastustaotluse vormi asjakohased osad (C liide) ning esitab taotluse rajatise riiklikule/määratud julgeolekuasutusele;

b) lähetava rajatise riiklik/määratud julgeolekuasutus kinnitab külastaja juurdepääsuloa enne külastustaotluse esitamist vastuvõtva rajatise riiklikule/määratud julgeolekuasutusele (või komisjoni julgeolekuasutusele, kui külastatakse komisjoni objekti);

c) lähetava rajatise julgeolekuametnik hangib seejärel oma riiklikult/määratud julgeolekuasutuselt vastuvõtva rajatise riikliku/määratud julgeolekuasutuse (või komisjoni julgeolekuasutuse) vastuse, millega külastustaotlus kas rahuldatakse või lükatakse tagasi;

d) külastustaotlus loetakse heakskiidetuks, kui vastuväiteid ei ole esitatud hiljemalt viis tööpäeva enne külastuse kuupäeva.]

[25. Enne kui külastaja(te)le antakse juurdepääs CONFIDENTIEL UE/EU CONFIDENTIAL või SECRET UE/EU SECRET tasemel salastatud teabele, peab vastuvõtval rajatisel olema selleks oma riikliku/määratud julgeolekuasutuse luba.]

[26. Külastused, mis hõlmavad juurdepääsu või võimalikku juurdepääsu CONFIDENTIEL UE/EU CONFIDENTIAL või SECRET UE/EU SECRET tasemel salastatud teabele, lepitakse kokku otse lähetava ja vastuvõtva asutuse vahel (vormi näidis, mida võib sel eesmärgil kasutada, on esitatud C liites).]

([1]) Lepingu sõlmija lisab viited pärast seda, kui rakenduseeskirjad on vastu võetud.

27. Külastaja peab oma isikut tõendama vastuvõtvasse rajatisse saabumisel, esitades selleks kehtiva isikutunnistuse või passi.

28. Vastuvõttev rajatis tagab kõigi külastajate andmete registreerimise. Külastaja andmed peavad sisaldama külastaja nime, tema esindatavat organisatsiooni, juurdepääsuloa kehtivuse lõppkuupäeva (kui see on asjakohane), külastuse kuupäeva ja külastatud isiku(te) nime(sid). Ilma et see piiraks Euroopa andmekaitsenormide kohaldamist, säilitatakse selliseid andmeid vähemalt viis aastat või vastavalt riigi õigusnormidele, kui see on asjakohane.

HINDAMISKÜLASTUSED

29. Komisjoni julgeolekuasutus võib teha koostöös asjaomase riikliku/määratud julgeolekuasutusega külastusi lepinglaste või all-lepinglaste rajatistesse, et kontrollida, kas ELi salastatud teabe töötlemisel täidetakse julgeolekunõudeid.

SALASTATUSE TASEME MÄÄRAMISE JUHEND

30. Loetelu lepingu kõigist elementidest, mis on salastatud või mis salastatakse lepingu täitmise käigus, sellist tegevust käsitlevad reeglid ning kohaldatavad salastatuse tasemed esitatakse salastatuse taseme määramise juhendis. Salastatuse taseme määramise juhend on käesoleva lepingu lahutamatu osa ja see on esitatud käesoleva lisa B liites.

B Liide

SALASTATUSE TASEME MÄÄRAMISE JUHEND

[teksti kohandatakse sõltuvalt lepingu esemest]

C Liide

KÜLASTUSTAOTLUS

(NÄIDIS)

Külastustaotluse täitmise üksikasjalik juhend

(Taotlus esitatakse ainult inglise keeles)

HEADING	Märkige lahtris külastuse liik, teabe liik, külastatavate kohtade arv ja külastajate arv.
4. **ADMINISTRATIVE DATA**	Täidab taotlev riiklik/määratud julgeolekuasutus.
5. **REQUESTING ORGANISATION OR INDUSTRIAL FACILITY**	Märkida täielik nimi ja postiaadress. Märkida linn, riik ja sihtnumber, kui see on asjakohane.
6. **ORGANISATION OR INDUSTRIAL FACILITY TO BE VISITED**	Märkida täielik nimi ja postiaadress. Lisada linn, riik, sihtnumber, teleksi või faksi number (kui see on asjakohane), telefoninumber ja e-posti aadress. Esitage oma peamise kontaktpunkti või selle isiku nimi, telefoni- ja faksinumber ning e-posti aadress, kellega te külastuse kokku leppisite. Märkused: 1) Õige sihtnumber on oluline, sest ettevõttel võib olla erinevaid rajatisi. 2) Kui taotlus esitatakse käsitsi, võib kasutada 1. lisa, kui sama teemaga seoses tuleb külastada kahte või enamat rajatist. Kui kasutatakse lisa, peaks punkt 3 sisaldama järgmist teavet: „SEE ANNEX 1, NUMBER OF FAC: …“ (märkida rajatiste arv)
7. **DATES OF VISIT**	Märkige külastuse tegelik kuupäev või ajavahemik (kuupäevast kuupäevani) vormingus „päev – kuu – aasta“. Vajaduse korral märkige sulgudes muu võimalik kuupäev või ajavahemik.
8. **TYPE OF INITIATIVE**	Märkige, kas külastus toimub taotleva organisatsiooni või asutuse initsiatiivil või selle rajatise kutsel, mida külastatakse.
9. **THE VISIT RELATES TO:**	Esitage projekti, lepingu või pakkumismenetluse täisnimetus, kasutades üksnes üldkasutatavaid lühendeid.

10. **SUBJECT TO BE DISCUSSED/ JUSTIFICATION**	Kirjeldage lühidalt külastuse põhjust (põhjuseid). Ärge kasutage selgitamata lühendeid. Märkused: Korduvkülastuse puhul peaks selle andmeelemendi esimesed sõnad olema „Recurring visits“ (nt Recurring visits to discuss _____).
11. **ANTICIPATED LEVEL OF CLASSIFIED INFORMATION TO BE INVOLVED**	Märkige, kas SECRET UE/EU SECRET (S-UE/EU-S) või CONFIDENTIEL UE/EU CONFIDENTIAL (C-UE/EU-C).
12. **PARTICULARS OF VISITOR**	Märkus: kui osaleb rohkem kui kaks külastajat, tuleks kasutada 2. lisa.
13. **THE SECURITY OFFICER OF THE REQUESTING ENTITY**	Siin tuleb esitada taotleva rajatise julgeolekuametniku nimi, telefoninumber, faksinumber ja e-posti aadress.
14. **CERTIFICATION OF SECURITY CLEARANCE**	Selle välja täidab tõendit väljastav asutus. Märkused tõendit väljastava asutuse jaoks: a) Märkida nimi, aadress, telefoninumber, faksinumber ja e-posti aadress (võib olla valmistrükitud). b) See punkt tuleb allkirjastada ja tembeldada (kui see on asjakohane).
15. **REQUESTING SECURITY AUTHORITY**	Selle välja täidab riiklik/määratud julgeolekuasutus. Märkus riiklikule/määratud julgeolekuasutusele: a) Märkida nimi, aadress, telefoninumber, faksinumber ja e-posti aadress (võib olla valmistrükitud). b) See punkt tuleb allkirjastada ja tembeldada (kui see on asjakohane).

Kõik väljad tuleb täita ja vorm edastada valitsustevaheliste kanalite kaudu ([2]).

([2]) Kui on kokku lepitud, et selliseid külastusi, millega kaasneb juurdepääs või võimalik juurdepääs CONFIDENTIEL UE/EU CONFIDENTIAL või SECRET UE/EU SECRET tasemel ELi salastatud teabele, võib korraldada otse, võib täidetud vormi esitada otse külastatava asutuse julgeolekuametnikule.

REQUEST FOR VISIT

(MODEL)

TO: _____

1. **TYPE OF VISIT REQUEST**	2. **TYPE OF INFORMATION**	3. **SUMMARY**
☐ Single ☐ Recurring ☐ Emergency ☐ Amendment ☐ Dates ☐ Visitors ☐ Facility For an amendment, insert the NSA/DSA original RFV Reference No_____	☐ C-UE/EU-C ☐ S-UE/EU-S	No of sites: _____ No of visitors: _____

4. **ADMINISTRATIVE DATA:**

Requester:	NSA/DSA RFV Reference No_____
To:	Date *(dd/mm/yyyy)*: _____/_____/_____

5. **REQUESTING ORGANISATION OR INDUSTRIAL FACILITY:**

NAME:

POSTAL ADDRESS:

E-MAIL ADDRESS:

FAX NO: TELEPHONE NO:

6. **ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED** *(Annex 1 to be completed)*

7. **DATE OF VISIT** *(dd/mm/yyyy)*: FROM _____/_____/_____ TO _____/_____/_____

8. **TYPE OF INITIATIVE:**

☐ Initiated by requesting organisation or facility

☐ By invitation of the facility to be visited

9. **THE VISIT RELATES TO CONTRACT:**

10. **SUBJECT TO BE DISCUSSED/REASONS/PURPOSE** *(Include details of host entity and any other relevant information. Abbreviations should be avoided):*

11. **ANTICIPATED HIGHEST CLASSIFICATION LEVEL OF INFORMATION/MATERIAL OR SITE ACCESS TO BE INVOLVED:**

12. **PARTICULARS OF VISITOR(S)** *(Annex 2 to be completed)*

13. **THE SECURITY OFFICER OF THE REQUESTING ORGANISATION OR INDUSTRIAL FACILITY:**

NAME:

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE:

14. **CERTIFICATION OF SECURITY CLEARANCE LEVEL:**

NAME:

ADDRESS:

TELEPHONE NO:

E-MAIL ADDRESS:

STAMP

SIGNATURE: DATE *(dd/mm/yyyy)*: _____/_____/_____

15. **REQUESTING NATIONAL SECURITY AUTHORITY/DESIGNATED SECURITY AUTHORITY:**

NAME:

ADDRESS:

TELEPHONE NO:

E-MAIL ADDRESS:

STAMP

SIGNATURE: DATE *(dd/mm/yyyy)*: _____/_____/_____

16. **REMARKS** *(Mandatory justification required in the case of an emergency visit)*:

<Täidetakse hiljem: viide kohaldatavatele isikuandmeid käsitlevatele õigusaktidele ja link andmesubjektile kohustusliku teabe juurde, nt kuidas rakendatakse isikuandmete kaitse üldmääruse ([3]) artiklit 13. >

([3]) Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) (ELT L 119, 4.5.2016, lk 1).

KÜLASTUSTAOTLUSE VORMI 1. LISA

ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED

1.

NAME:

ADDRESS:

TELEPHONE NO:

FAX NO:

NAME OF POINT OF CONTACT:

E-MAIL:

TELEPHONE NO:

NAME OF SECURITY OFFICER OR

SECONDARY POINT OF CONTACT:

E-MAIL:

TELEPHONE NO:

2.

NAME:

ADDRESS:

TELEPHONE NO

FAX NO:

NAME OF POINT OF CONTACT:

E-MAIL:

TELEPHONE NO:

NAME OF SECURITY OFFICER OR

SECONDARY POINT OF CONTACT:

E-MAIL:

TELEPHONE NO:

(Continue as required)

<Täidetakse hiljem: viide kohaldatavatele isikuandmeid käsitlevatele õigusaktidele ja link andmesubjektile kohustusliku teabe juurde, nt kuidas rakendatakse isikuandmete kaitse üldmääruse ([1]) artiklit 13. >

([1]) Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) (ELT L 119, 4.5.2016, lk 1).

KÜLASTUSTAOTLUSE VORMI 2. LISA

PARTICULARS OF VISITOR(S)

1.

SURNAME:

FIRST NAMES *(as per passport)*:

DATE OF BIRTH *(dd/mm/yyyy)*: ____/____/____

PLACE OF BIRTH:

NATIONALITY:

SECURITY CLEARANCE LEVEL:

PP/ID NUMBER:

POSITION:

COMPANY/ORGANISATION:

2.

SURNAME:

FIRST NAMES *(as per passport)*:

DATE OF BIRTH *(dd/mm/yyyy)*: ____/____/____

PLACE OF BIRTH:

NATIONALITY:

SECURITY CLEARANCE LEVEL:

PP/ID NUMBER:

POSITION:

COMPANY/ORGANISATION:

(Continue as required)

<Täidetakse hiljem: viide kohaldatavatele isikuandmeid käsitlevatele õigusaktidele ja link andmesubjektile kohustusliku teabe juurde, nt kuidas rakendatakse isikuandmete kaitse üldmääruse ([1]) artiklit 13. >

([1]) Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) (ELT L 119, 4.5.2016, lk 1).

D Liide

TÖÖTLEMISLOA TEABELEHT

(NÄIDIS)

1. **Sissejuhatus**

1.1. Lisatud on töötlemisloa teabeleht, mis võimaldab kiiret teabevahetust riikliku julgeolekuasutuse või määratud julgeolekuasutuse, muude pädevate riiklike julgeolekuasutuste ja komisjoni (kui lepingu sõlmija) vahel seoses salastatud pakkumuses, lepingus või all-lepingus osaleva rajatise töötlemisloaga.

1.2. Töötlemisloa teabeleht on kehtiv ainult juhul, kui see kannab asjaomase riikliku/määratud julgeolekuasutuse või muu pädeva asutuse templit.

1.3. Töötlemisloa teabelehel on taotluse ja vastuste osa ning seda võib kasutada eespool nimetatud või muudel eesmärkidel, mille puhul on nõutav töötlemisluba. Taotlev riiklik/määratud julgeolekuasutus esitab päringu põhjuse taotluse osa väljal 7.

1.4. Töötlemisloa teabelehel esitatud üksikasjad ei ole üldjuhul salastatud. Seega, kui töötlemisloa teabelehte saadetakse asjaomastele riiklikele/määratud/komisjoni julgeolekuasutustele, tehakse seda eelistatavalt elektrooniliselt.

1.5. Riiklik/määratud julgeolekuasutus teeb kõik endast oleneva, et vastata töötlemisloaga seonduvale teabenõudele kümne tööpäeva jooksul.

1.6. Kui sellega seoses edastatakse salastatud teavet või sõlmitakse leping, teavitatakse sellest riiklikku/määratud julgeolekuasutust.

Menetlus ja juhised töötlemisloa teabelehe kasutamiseks

Need üksikasjalikud juhised on mõeldud teabelehte täitvale riiklikule/määratud julgeolekuasutusele või komisjonile kui lepingu sõlmijale. Taotlus tuleb eelistatavalt täita trükitähtedes.

PÄIS	Taotleja sisestab täieliku riikliku/määratud julgeolekuasutuse ja riigi nime.
1. **TAOTLUSE LIIK**	Taotlev lepingu sõlmija valib taotluse liigi jaoks sobiva märkeruudu. Lisada taotletava juurdepääsu tase. Kasutatakse järgmisi lühendeid: SECRET UE/EU SECRET = S-UE/EU-S CONFIDENTIEL UE/EU CONFIDENTIAL = C-UE/EU-C CIS = salastatud teabe töötlemiseks kasutatavad side- ja infosüsteemid

2. **TEEMA ÜKSIKASJAD**	Väljad 1–6 ei vaja selgitust. Väljal 4 tuleb kasutada standardset kahetähelist riigikoodi. Väli 5 on vabatahtlik.
3. **TAOTLUSE PÕHJUS**	Taotluse konkreetne põhjus, aga ka projektinäitajad, lepingu või pakkumiskutse number. Täpsustada andmemahu vajadus, side- ja infosüsteemi salastatuse tase jne. Lisada tuleks kõik tähtajad/aegumistähtajad/lepingu sõlmimise kuupäevad, mis võivad töötlemisloa menetlemist mõjutada.
4. **TAOTLEV RIIKLIK/MÄÄRATUD JULGEOLEKUASUTUS**	Märkida tegeliku taotleja nimi (riikliku/määratud julgeolekuasutuse nimel) ja taotluse kuupäev vormingus (pp/kk/aaaa).
5. **VASTUSTE OSA**	Väljad 1–5: valige sobivad väljad. Väli 2: kui töötlemisloa menetlemine on pooleli, on soovitav teavitada taotlejat menetluseks vajalikust ajast (kui see on teada). Väli 6: a) Kuigi valideerimine on riikide ja isegi rajatiste lõikes erinev, soovitatakse esitada töötlemisloa kehtivusaja lõppkuupäev. b) Kui töötlemisluba on tähtajatu, võib selle välja läbi kriipsutada. c) Riigi eeskirjade ja normide kohaselt vastutab töötlemisloa pikendamise eest taotleja, lepinglane või all-lepinglane.
6. **MÄRKUSED**	Kasutada täiendava teabe esitamiseks töötlemisloa, rajatise või eespool nimetatud küsimuste kohta.
7. **VÄLJAANDEV RIIKLIK/MÄÄRATUD JULGEOLEKUASUTUS**	Märkida väljaandva asutuse nimi (riikliku/määratud julgeolekuasutuse nimel) ja vastuse kuupäev vormingus (pp/kk/aaaa).

TÖÖTLEMISLOA TEABELEHT

(NÄIDIS)

Kõik väljad tuleb täita ja vorm edastada kas valitsustevaheliste või valitsuse ja rahvusvahelise organisatsiooni vaheliste kanalite kaudu.

TAOTLUS TÖÖTLEMISLOA KINNITAMISEKS

KELLELE: _____

(Riiklik/määratud julgeolekuasutus Riigi nimi)

Vajaduse korral täitke vastavad lahtrid:

[] Anda kinnitus töötlemisloa kohta järgmisel tasemel: [] S-UE/EU-S [] C-UE/EU-C

allpool esitatud rajatise puhul

[] Sealhulgas salastatud materjali/teabe kaitsmine

[] Sealhulgas salastatud teabe töötlemiseks kasutatavad side- ja infosüsteemid

[] Algatada otse või lepinglase või all-lepinglase vastava taotluse alusel menetlus töötlemisloa saamiseks (kuni ja kaasa arvatud) tasemel ....., aga ka tasemel ..... kaitse ja tasemel ..... side- ja infosüsteemide jaoks, kui sellised tasemed rajatises praegu puuduvad.

Kinnitada allpool esitatud rajatise andmete õigsust ning esitada vajaduse korral parandusi ja täiendusi.

1. Rajatise täielik nimi:	Parandused/täiendused:
.....	.....
2. Rajatise täielik aadress:	
.....	.....
3. Postiaadress (kui erineb 2. punktis esitatud aadressist)	
.....	.....
4. Sihtnumber/linn/riik	
.....	.....
5. Julgeolekuametniku nimi	
.....	.....
6. Julgeolekuametniku telefon/faks/e-post	
.....	.....

7. Käesolev taotlus on esitatud järgmis(t)el põhjus(t)el: (esitada lepingueelse etapi (taotluste väljavalimine), lepingu või all-lepingu, programmi/projekti jne üksikasjad)

.....

Taotlev riiklik/määratud julgeolekuasutus/komisjoni lepingu sõlmija: Nimi: ..... Kuupäev: (pp/kk/aaaa) .....

VASTUS (kümne tööpäeva jooksul)

Käesolevaga tõendatakse, et:

1. [] eespool nimetatud rajatisel on töötlemisluba kuni salastatuse tasemeni [] S-UE/EU-S

   [] C-UE/EU-C (kaasa arvatud).

2. Eespool nimetatud rajatis on võimeline kaitsma salastatud teavet/materjale:

   [] jah, tase: ..... [] ei.

3. eespool nimetatud rajatisel on akrediteeritud/heaks kiidetud side- ja infosüsteem:

   [] jah, tase: ..... [] ei.

4. [] seoses eespool nimetatud taotlusega on algatatud menetlus töötlemisloa saamiseks. Teid teavitatakse, kui töötlemisluba kinnitatakse või selle andmisest keeldutakse.

5. [] eespool nimetatud rajatisel töötlemisluba puudub.

6. Käesolev töötlemisloa kinnitus kaotab kehtivuse: ..... (*pp/kk/aaaa*) või muul ajal, mille määrab riiklik/määratud julgeolekuasutus. Teid teavitatakse, kui töötlemisluba kaotab kehtivuse varem või kui eespool esitatud teave muutub.

7. Märkused:

   .....

VÄLJAANDEV RIIKLIK/MÄÄRATUD JULGEOLEKUASUTUS Nimi: ..... Kuupäev: (pp/kk/aaaa) .....

<Täidetakse hiljem: viide kohaldatavatele isikuandmeid käsitlevatele õigusaktidele ja link andmesubjektile kohustusliku teabe juurde, nt kuidas rakendatakse isikuandmete kaitse üldmääruse ([2]) artiklit 13. >

([2]) Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) (ELT L 119, 4.5.2016, lk 1).

E Liide

Miinimumnõuded elektroonilise RESTREINT UE/EU RESTRICTED tasemel ELi salastatud teabe kaitsmiseks selle töötlemise korral lepinglase side- ja infosüsteemis

Üldine teave

1. Lepinglane vastutab selle eest, et RESTREINT UE/EU RESTRICTED tasemel teabe kaitse vastaks käesolevas julgeolekuklauslis sätestatud miinimumnõuetele ja muudele lepingu sõlmija või, kui see on kohaldatav, riikliku või määratud julgeolekuasutuse esitatud täiendavatele nõuetele.

2. Lepinglane vastutab käesolevas dokumendis kirjeldatud julgeolekunõuete rakendamise eest.

3. Käesolevas dokumendis hõlmab side- ja infosüsteem kõiki seadmeid, mida kasutatakse ELi salastatud teabe töötlemiseks, salvestamiseks ja edastamiseks, sealhulgas tööjaamad, printerid, koopiamasinad, faksid, serverid, võrguhaldussüsteemid, võrgukontrollerid ja sidekontrollerid, sülearvutid, elektronmärkmikud, tahvelarvutid, nutitelefonid ja eemaldatavad salvestusseadmed, nagu USB-pulgad, CD-d, SD-kaardid jne.

4. Erivarustus (nt krüptovahendid) peab olema kaitstud vastavalt kindlaks määratud julgeolekunõuete rakendamise korrale.

5. Lepinglased loovad struktuuri, mis vastutab RESTREINT UE/EU RESTRICTED tasemel salastatud teabe töötlemisel kasutatava side- ja infosüsteemi turbehalduse eest, ning määravad asjaomase rajatise eest vastutava julgeolekuametniku.

6. Lepinglase töötajatele kuuluvate IT-lahenduste (riistvara, tarkvara ja teenused) kasutamine RESTREINT UE/EU RESTRICTED tasemel salastatud teabe säilitamise või töötlemise eesmärgil ei ole lubatud.

7. RESTREINT UE/EU RESTRICTED tasemel salastatud teavet töötleva lepinglase side- ja infosüsteemi akrediteerimise peab heaks kiitma asjaomase liikmesriigi turvalisuse akrediteerimise asutus või see ülesanne delegeeritakse lepinglase julgeolekuametnikule vastavalt sellele, kuidas on riigi õigusnormidega ette nähtud.

8. Ainult RESTREINT UE/EU RESTRICTED tasemel salastatud teavet, mis on krüpteeritud heakskiidetud krüptovahenditega, võib töödelda, säilitada või edastada (traadiga või traadita tehnoloogia abil) nagu muud lepingu raames edastatavat salastamata teavet. Krüptovahendid peavad olema heaks kiidetud ELi või liikmesriigi poolt.

9. Hooldus-/remonditöödega tegelevad välisrajatised peavad olema lepinguga kohustatud järgima RESTREINT UE/EU RESTRICTED tasemel salastatud teabe töötlemise suhtes kohaldatavaid sätteid, nagu on ette nähtud käesolevas dokumendis.

10. Lepingu sõlmija või asjaomase riikliku/määratud julgeolekuasutuse/turvalisuse akrediteerimise asutuse taotlusel peab lepinglane tõendama, et ta täidab lepingu julgeolekuklauslit. Kui nende nõuete täitmise tagamiseks taotletakse ka lepinglase protsesside ja rajatiste auditit ja kontrolli, peab lepinglane võimaldama lepingu sõlmija, riikliku/määratud julgeolekuasutuse/turvalisuse akrediteerimise asutuse või ELi asjaomase julgeolekuasutuse esindajatel auditit ja kontrolli läbi viia.

Füüsiline turvalisus

11. Alad, kus side- ja infosüsteeme kasutatakse RESTREINT UE/EU RESTRICTED teabe kuvamiseks, säilitamiseks, töötlemiseks või edastamiseks, aga ka selliste side- ja infosüsteemide serverite, võrguhaldussüsteemide, võrgukontrollerite ja sidekontrollerite paiknemise alad peaksid olema eraldi kontrollitud alad, millel on nõuetekohane juurdepääsukontrolli süsteem. Juurdepääs nendele eraldi kontrollitud aladele peaks piirduma isikutega, kellel on selleks eriluba. Ilma et see piiraks lõike 8 kohaldamist, tuleb lõikes 3 kirjeldatud seadmeid hoida sellistel eraldi kontrollitud aladel.

12. Tuleb rakendada turvamehhanisme ja/või -menetlusi, et reguleerida teisaldatavate mäluseadmete (nagu USBd, massmälu seadmed või CD-RWd) kasutamist side- ja infosüsteemi komponentides ja nende ühendamist kõnealuse süsteemi komponentidega.

Juurdepääs side- ja infosüsteemile

13. Juurdepääs lepinglase side- ja infosüsteemile, milles töödeldakse ELi salastatud teavet, on lubatud ainult teadmisvajaduse ja töötajate vastavate volituste alusel.

14. Kõik side- ja infosüsteemid peavad olema varustatud volitatud kasutajate ajakohastatud loeteludega. Kõik kasutajad tuleb iga töötlemisseansi alguses autentida.

15. Salasõnad, mis kuuluvad enamiku identimise ja autentimisega seonduvate turvameetmete juurde, peavad koosnema vähemalt üheksast tähemärgist ning sisaldama nii numbreid kui ka erimärke (kui süsteem seda võimaldab) ning samuti tähti. Salasõna tuleb muuta vähemalt iga 180 päeva tagant. Salasõna tuleb muuta niipea kui võimalik, kui selle salajasus on kahjustatud või see on avalikustatud volitamata isikule, aga ka siis, kui kahtlustatakse selle salajasuse kahjustamist või salasõna avalikustamist.

16. Kõik side- ja infosüsteemid peavad olema varustatud sisemiste juurdepääsu kontrollidega, et volitamata kasutajatel puuduks juurdepääs RESTREINT UE/EU RESTRICTED tasemel salastatud teabele ning et nad ei saaks süsteemi ega turvakontrolle muuta. Kui kasutaja terminal on olnud teatava aja jooksul mitteaktiivne, tuleb ta side- ja infosüsteemidest automaatselt välja logida või seadistada side- ja infosüsteem nõnda, et see aktiveeriks salasõnaga kaitstud ekraani, kui mitteaktiivsus on kestnud 15 minutit.

17. Igale side- ja infosüsteemi kasutajale antakse kordumatu kasutajakonto ja kasutajanimi. Kasutajakontod tuleb automaatselt lukustada pärast seda, kui on tehtud vähemalt viis järjestikust ebaõnnestunud sisselogimiskatset.

18. Kõik side- ja infosüsteemi kasutajad peavad olema teadlikud oma ülesannetest ja menetlustest, mida tuleb järgida, et kaitsta side- ja infosüsteemis RESTREINT UE/EU RESTRICTED tasemel salastatud teavet. Need ülesanded ja menetlused peavad olema dokumenteeritud ning kasutajad peavad kirjalikult kinnitama, et on nendega tutvunud.

19. Turvanõuete rakendamise kord peab olema kasutajatele ja administraatoritele kättesaadav ja sisaldama turvarollide kirjeldusi ning nendega seotud ülesannete, juhiste ja kavade loetelu.

Raamatupidamisarvestus, auditeerimine ja intsidentidele reageerimine

20. Igasugune juurdepääs side- ja infosüsteemile tuleb registreerida.

21. Registreerida tuleb järgmised sündmused:

    a) kõik edukad ja ebaõnnestunud sisselogimiskatsed;

    b) väljalogimine (sealhulgas aegumine, kui see on asjakohane);

    c) juurdepääsuõiguste ja -privileegide loomine, kustutamine või muutmine;

    d) salasõnade loomine, kustutamine või muutmine.

22. Kõigi eespool loetletud sündmuste puhul tuleb esitada vähemalt järgmine teave:

    a) sündmuse liik;

    b) kasutaja ID;

    c) kuupäev ja kellaaeg;

    d) seadme ID.

23. Raamatupidamisarvestus peaks turbeametnikku võimalike turvaintsidentide uurimisel aitama. Samuti saab raamatupidamisarvestust kasutada õigusliku uurimise toetamiseks turvaintsidendi korral. Kõiki turbeandmeid tuleks regulaarselt kontrollida, et teha kindlaks võimalikud turvaintsidendid. Raamatupidamisdokumente tuleb kaitsta loata kustutamise või muutmise eest.

24. Lepinglane peab turvaintsidentidega toimetulekuks koostama reageerimisstrateegia. Kasutajatele ja administraatoritele tuleb anda juhised, kuidas intsidentidele reageerida, kuidas nendest teatada ja mida teha erakorralises olukorras.

25. RESTREINT UE/EU RESTRICTED tasemel salastatud teabe salajasuse kahjustamisest või selle võimalikust kahjustamisest tuleb teavitada lepingu sõlmijat. Teavitus peab sisaldama nii asjaomase teabe kirjeldust kui ka salajasuse kahjustamise või selle võimaliku kahjustamise asjaolude kirjeldust. Kõigile side- ja infosüsteemi kasutajatele peab olema selgitatud, kuidas julgeolekuametnikku igast tegelikust või kahtlustatavast turvaintsidendist teavitada.

Võrgud ja võrkude sidumine

26. Kui RESTREINT UE/EU RESTRICTED tasemel salastatud teavet töötleva lepinglase side- ja infosüsteem seotakse sellise side- ja infosüsteemiga, mis ei ole akrediteeritud, suurendab see märkimisväärselt ohtu nii side- ja infosüsteemi enda kui ka selles töödeldava RESTREINT UE/EU RESTRICTED teabe turvalisusele. See hõlmab internetti ja muid avaliku või erasektori side- ja infosüsteeme, näiteks lepinglasele või all-lepinglasele kuuluvaid muid side- ja infosüsteeme. Sellisel juhul peab lepinglane tegema riskihindamise, et välja selgitada täiendavad julgeolekunõuded, mida tuleb turvalisuse akrediteerimise osana rakendada. Lepinglane esitab lepingu sõlmijale ning, kui see on riigi õigusnormidega ette nähtud, pädevale turvalisuse akrediteerimise asutusele kinnituse nõuetele vastavuse kohta, mis tõendab, et lepinglase side- ja infosüsteem ning selle sidumine teise süsteemiga on akrediteeritud ELi salastatud teabe töötlemiseks RESTREINT UE/EU RESTRICTED tasemel.

27. Kaugjuurdepääs LANi teenustele (nt kaugjuurdepääs e-postile ja süsteemitoele) muude süsteemide kaudu on keelatud, välja arvatud juhul, kui lepingu sõlmija rakendab spetsiaalseid turvameetmeid ja on nendes kokku leppinud, ning kui see on nõutav riigi õigusnormidega ja selleks on pädeva turvalisuse akrediteerimise asutuse heakskiit.

Konfiguratsiooni haldamine

28. Üksikasjalik riist- ja tarkvara konfiguratsioon, mis vastab akrediteerimise/heakskiitmise dokumentidele (sealhulgas süsteemi- ja võrguskeemid), peab olema kättesaadav ja seda tuleb korrapäraselt hooldada.

29. Lepinglase julgeolekuametnik teeb riist- ja tarkvara konfiguratsioonikontrolli, et välistada loata riist- või tarkvara kasutuselevõtt.

30. Lepinglase side- ja infosüsteemi konfiguratsiooni muudatusi tuleb hinnata seoses nende mõjuga turvalisusele ning muudatused peab heaks kiitma julgeolekuametnik ja pädev turvalisuse akrediteerimise asutus, kui see on nõutav riigi õigusnormidega.

31. Süsteemi tuleb vähemalt kord kvartalis turvaaukude väljaselgitamiseks kontrollida. Pahavara tuvastamise tarkvara tuleb installeerida ja ajakohastada. Võimaluse korral peaks selline tarkvara olema riiklikult või rahvusvaheliselt tunnustatud või valdkondliku standardina üldtunnustatud.

32. Lepinglane peab välja töötama talitluspidevuse plaani. Tuleb kehtestada andmete varundamise kord, pöörates tähelepanu järgmistele küsimustele:

a) varukoopiate tegemise sagedus;

b) hoiustamisnõuded kohapeal (tulekindlad hoidlad) või väljaspool;

c) varukoopiatele volitatud juurdepääsu kontroll.

Andmekandjate saniteerimine ja hävitamine

33. Iga side- ja infosüsteemi või andmekandja puhul, kus on kunagi hoitud RESTREINT UE/EU RESTRICTED tasemel salastatud teavet, tuleb kogu süsteemis või enne andmekandja kõrvaldamist teha järgmised saniteerimistööd:

a) välkmälu (nt USB-mälupulgad, SD-kaardid, pooljuhtkettad, hübriidkettad) tuleb vähemalt kolm korda üle kirjutada ning seejärel kontrollida, et originaalsisu taastamine ei oleks võimalik, või sellele salvestatud andmed kustutada heakskiidetud kustutamistarkvara abil;

b) magnetkandjad (nt kõvakettad) tuleb üle kirjutada või demagneetida;

c) optilised andmekandjad (nt CDd ja DVDd) tuleb purustada või tükeldada;

d) muude andmekandjate puhul tuleb kohaldatavate turvanõuete osas konsulteerida lepingu sõlmija või vajaduse korral riikliku/määratud julgeolekuasutuse/turvalisuse akrediteerimise asutusega.

34. RESTREINT UE/EU RESTRICTED tasemel salastatud teave tuleb saniteerida mis tahes andmekandjal enne selle andmist üksusele, millel puuduvad juurdepääsuõigused RESTREINT UE/EU RESTRICTED tasemel salastatud teabele (nt hooldustööde tegemiseks).

IV LISA

RESTREINT UE/EU RESTRICTED tasemel salastatud teabe töötlemis- ja juurdepääsuluba ning riiklikud/määratud julgeolekuasutused, keda tuleb RESTREINT UE/EU RESTRICTED tasemel salastatud teavet sisaldavatest lepingutest teavitada ([1])

Liikmesriik	Töötlemisluba		Riikliku/määratud julgeolekuasutuse teavitamine lepingutest või all-lepingutest, mis sisaldavad R-UE/EU-R tasemel salastatud teavet		Juurdepääsuluba	
	JAH	EI	JAH	EI	JAH	EI
Belgia		X		X		X
Bulgaaria		X		X		X
Tšehhi		X		X		X
Taani	X		X		X	
Saksamaa		X		X		X
Eesti	X		X			X
Iirimaa		X		X		X
Kreeka	X			X	X	
Hispaania		X	X			X
Prantsusmaa		X		X		X
Horvaatia		X	X			X
Itaalia		X	X			X
Küpros		X	X			X
Läti		X		X		X

([1]) Töötlemisluba ja juurdepääsuluba käsitlevad siseriiklikud nõuded ja RESTREINT UE/EU RESTRICTED tasemel salastatud teavet sisaldavatest lepingutest teavitamise nõuded ei tohi tekitada täiendavaid kohustusi teistele liikmesriikidele ega nende jurisdiktsiooni kuuluvatele lepinglastele.
NB! CONFIDENTIEL UE/EU CONFIDENTIAL ja SECRET UE/EU SECRET tasemel salastatud teavet sisaldavatest lepingutest teavitamine on kohustuslik.

Liikmesriik	Töötlemisluba		Riikliku/määratud julgeolekuasutuse teavitamine lepingutest või all-lepingutest, mis sisaldavad R-UE/EU-R tasemel salastatud teavet		Juurdepääsuluba	
	JAH	EI	JAH	EI	JAH	EI
Leedu	X		X			X
Luksemburg	X		X		X	
Ungari		X		X		X
Malta		X		X		X
Madalmaad	X (ainult kaitseotstarbeliste lepingute puhul)		X (ainult kaitseotstarbeliste lepingute puhul)			X
Austria		X		X		X
Poola		X		X		X
Portugal		X		X		X
Rumeenia		X		X		X
Sloveenia	X		X			X
Slovakkia	X		X			X
Soome		X		X		X
Rootsi	X (ainult kaitseotstarbeliste lepingute puhul)		X (ainult kaitseotstarbeliste lepingute puhul)		X (ainult kaitseotstarbeliste lepingute puhul)	
Ühendkuningriik		X		X		X

V LISA

TÖÖSTUSJULGEOLEKUGA SEOTUD MENETLUSTE EEST VASTUTAVATE RIIKLIKU/MÄÄRATUD JULGEOLEKUASUTUSE OSAKONDADE LOETELU

BELGIA

National Security Authority
FPS Foreign Affairs
Rue des Petits Carmes 15
1000 Brussels
Tel: +32 25014542 (sekretariaat)
Faks: +32 25014596
E-post: nvo-ans@diplobel.fed.be

BULGAARIA

1. State Commission on Information Security - National Security Authority
   4 Kozloduy Street
   1202 Sofia
   Tel: +359 29835775
   Faks: +359 29873750
   E-post: dksi@government.bg

2. Defence Information Service at the Ministry of Defence (security service)
   3 Dyakon Ignatiy Street
   1092 Sofia
   Tel: +359 29227002
   Faks: +359 29885211
   E-post: office@iksbg.org

3. State Intelligence Agency (security service)
   12 Hajdushka Polyana Street
   1612 Sofia
   Tel: +359 29813221
   Faks: +359 29862706
   E-post: office@dar.bg

4. State Agency for Technical Operations (security service)
   29 Shesti Septemvri Street
   1000 Sofia
   Tel: +359 29824971
   Faks: +359 29461339
   E-post: dato@dato.bg

   (Eespool loetletud pädevad asutused teevad julgeolekukontrolli töötlemisloa andmiseks salastatud lepingu sõlmimist taotlevatele juriidilistele isikutele ja juurdepääsuloa andmiseks isikutele, kes täidavad salastatud lepingut nende ametiasutuste vajaduste huvides).

5. State Agency National Security (security service)
   45 Cherni Vrah Blvd.
   1407 Sofia
   Tel: +359 28147109
   Faks: +359 29632188, +359 28147441
   E-post: dans@dans.bg

   (Eespool nimetatud julgeolekuteenistus viib läbi julgeolekukontrolli töötlemislubade ja juurdepääsulubade andmiseks kõigile muudele riigis asuvatele juriidilistele isikutele ja üksikisikutele, kes taotlevad salastatud lepingu sõlmimist või täitmist.)

TŠEHHI VABARIIK

National Security Authority
Industrial Security Department
PO BOX 49
150 06 Praha 56
Tel: +420 257283129
E-post: sbr@nbu.cz

TAANI

1. Politiets Efterretningstjeneste
(Danish Security Intelligence Service)
Klausdalsbrovej 1
2860 Søborg
Tel: +45 33148888
Faks: +45 33430190

2. Forsvarets Efterretningstjeneste
(Danish Defence Intelligence Service)
Kastellet 30
2100 Copenhagen Ø
Tel: +45 33325566
Faks: +45 33931320

SAKSAMAA

1. Tööstusjulgeoleku poliitika, töötlemislubade ja transpordikavadega (välja arvatud krüpto- ja konfidentsiaalne äriteave) seotud küsimused:
Federal Ministry of Economic Affairs and Energy
Industrial Security Division - ZB3
Villemombler Str. 76
53123 Bonn
Tel: +49 228996154028
Faks: +49 228996152676
E-post: dsagermany-zb3@bmwi.bund.de (office email address)

2. Tavapärased külastustaotlused Saksamaa äriühingutelt/Saksamaa äriühingutesse:
Federal Ministry of Economic Affairs and Energy
Industrial Security Division – ZB2
Villemombler Str. 76
53123 Bonn
Tel: +49 228996152401
Faks: +49 228996152603
E-post: zb2-international@bmwi.bund.de (office email address)

3. Krüptomaterjali transpordikavad:
Federal Office for Information Security (BSI)
National Distribution Agency/NDA-EU DEU
Mainzer Str. 84
53179 Bonn
Tel: +49 2289995826052
Faks: +49 228991095826052
E-post: NDAEU@bsi.bund.de

EESTI

National Security Authority Department
Estonian Foreign Intelligence Service
Rahumäe tee 4b
11316 Tallinn
Tel: +372 6939211
Faks: +372 6935001
E-post: nsa@fis.gov.ee

IIRIMAA

National Security Authority Ireland
Department of Foreign Affairs and Trade
76–78 Harcourt Street
Dublin 2
D02 DX45
Tel: +353 14082724
E-post: nsa@dfa.ie

KREEKA

Hellenic National Defence General Staff
E' Division (Security INTEL, CI BRANCH)
E3 Directorate
Industrial Security Office
227–231 Mesogeion Avenue
15561 Holargos, Athens
Tel: +30 2106572022, +30 2106572178
Faks: +30 2106527612
E-post: daa.industrial@hndgs.mil.gr

HISPAANIA

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Calle Argentona 30
28023 Madrid
Tel: +34 913725000
Faks: +34 913725808
E-post: nsa-sp@areatec.com
Personali töötlemislubadega seotud küsimuste puhul: asip@areatec.com
Transpordikavade ja rahvusvaheliste külastuste puhul: sp-ivtco@areatec.com

PRANTSUSMAA

Riiklik julgeolekuasutus (poliitika ja rakendamine muudes valdkondades kui kaitsetööstus)
Secrétariat général de la défense et de la sécurité nationale
Sous-direction Protection du secret (SGDSN/PSD)
51 boulevard de la Tour-Maubourg
75700 Paris 07 SP
Tel: +33 171758193
Faks: +33 171758200
E-post: ANSFrance@sgdsn.gouv.fr

Määratud julgeolekuasutus (rakendamine kaitsetööstuses)
Direction Générale de l'Armement
Service de la Sécurité de Défense et des systèmes d'Information (DGA/SSDI)
60 boulevard du général Martial Valin
CS 21623
75509 Paris Cedex 15
Tel: +33 988670421
E-post: vormid ja väljaminevad külastustaotlused: dga-ssdi.ai.fct@intradef.gouv.fr
Sissetulevad külastustaotlused: dga-ssdi.visit.fct@intradef.gouv.fr

HORVAATIA

Office of the National Security Council
Croatian NSA
Jurjevska 34
10000 Zagreb
Tel: +385 14681222
Faks: +385 14686049
E-post: NSACroatia@uvns.hr

ITAALIA

Presidenza del Consiglio dei Ministri
D.I.S. - U.C.Se.
Via di Santa Susanna 15
00187 Roma
Tel: +39 0661174266
Faks: +39 064885273

KÜPROS

ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Λεωφόρος Στροβόλου, 172–174
Στρόβολος, 2048, Λευκωσία
Τηλέφωνα: +357 22807569, +357 22807764
Τηλεομοιότυπο: +357 22302351
E-post: cynsa@mod.gov.cy

Ministry of Defence
National Security Authority (NSA)
172–174, Strovolos Avenue
2048 Strovolos, Nicosia
Tel: +357 22807569, +357 22807764
Faks: +357 22302351
E-post: cynsa@mod.gov.cy

LÄTI

National Security Authority
Constitution Protection Bureau of the Republic of Latvia
P.O. Box 286
Riga LV-1001
Tel: +371 67025418, +371 67025463
Faks: +371 67025454
E-post: ndi@sab.gov.lt, ndi@zd.gov.lv

LEEDU

Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija
(The Commission for Secrets Protection Coordination of the Republic of Lithuania)
National Security Authority
Gedimino 40/1
LT-01110 Vilnius
Tel: +370 70666703, +370 70666701
Faks: +370 70666700
E-post: nsa@vsd.lt

LUKSEMBURG

Autorité Nationale de Sécurité
207, route d'Esch
L-1471 Luxembourg
Tel: +352 24782210
E-post: ans@me.etat.lu

UNGARI

National Security Authority of Hungary
H-1399 Budapest P.O. Box 710/50
H-1024 Budapest, Szilágyi Erzsébet fasor 11/B
Tel: +36 13911862
Faks: +36 13911889
E-post: nbf@nbf.hu

MALTA

Director of Standardisation
Designated Security Authority for Industrial Security
Standards & Metrology Institute
Malta Competition and ConsumerAffairs Authority
Mizzi House
National Road
Blata I-Bajda HMR9010
Tel.: +356 23952000
Faks: +356 21242406
E-post: certification@mccaa.org.mt

MADALMAAD

1. Ministry of the Interior and Kingdom Relations
PO Box 20010
2500 EA The Hague
Tel: +31 703204400
Faks: +31 703200733
E-post: nsa-nl-industry@minbzk.nl

2. Ministry of Defence
Industrial Security Department
PO Box 20701
2500 ES The Hague
Tel: +31 704419407
Faks: +31 703459189
E-post: indussec@mindef.nl

AUSTRIA

1. Federal Chancellery of Austria
Department I/12, Office for Information Security
Ballhausplatz 2
1014 Vienna
Tel: +43 153115202594
E-post: isk@bka.gv.at

2. Määratud julgeolekuasutus sõjanduse valdkonnas:
BMLVS/Abwehramt
Postfach 2000
1030 Vienna
E-post: abwa@bmlvs.gv.at

POOLA

Internal Security Agency
Department for the Protection of Classified Information
Rakowiecka 2A
00–993 Warsaw
Tel: +48 225857944
Faks: +48 225857443
E-post: nsa@abw.gov.pl

PORTUGAL

Gabinete Nacional de Segurança
Serviço de Segurança Industrial
Rua da Junqueira nº 69
1300-342 Lisbon
Tel: +351 213031710
Faks: +351 213031711
E-post: sind@gns.gov.pt, franco@gns.gov.pt

RUMEENIA

Oficiul Registrului Național al Informațiilor Secrete de Stat - ORNISS
Romanian NSA - ORNISS - National Registry Office for Classified Information
4th Mures Street
012275 Bucharest
Tel: +40 212075115
Faks: +40 212245830
E-post: relatii.publice@orniss.ro, nsa.romania@nsa.ro

SLOVEENIA

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

SLOVAKKIA

Národný bezpečnostný úrad
(National Security Authority)
Security Clearance Department
Budatínska 30
851 06 Bratislava
Tel: +421 268691111
Faks: +421 268691700
E-post: podatelna@nbu.gov.sk

SOOME

National Security Authority
Ministry for Foreign Affairs
P.O. Box 453
FI-00023 Government
E-post: NSA@formin.fi

ROOTSI

1. National Security Authority
   Utrikesdepartementet (Ministry for Foreign Affairs)
   UD SÄK/NSA
   SE-103 39 Stockholm
   Tel: +46 84051000
   Faks: +46 87231176
   E-post: ud-nsa@gov.se

2. DSA
   Försvarets Materielverk (Swedish Defence Materiel Administration)
   FMV Säkerhetsskydd
   SE-115 88 Stockholm
   Tel: +46 87824000
   Faks: +46 87826900
   E-post: security@fmv.se

Ühendkuningriik

UK National Security Authority
Room 335, 3rd Floor
70 Whitehall
London
SW1A 2AS
Tel: +44 2072765497, +44 2072765645
E-post: UK-NSA@cabinet-office.x.gsi.gov.uk