EUROOPA KONTROLLIKODA

Kontrollikoja otsus nr 041–2021 ELi salastatud teabe kaitse turbe-eeskirjade kohta

EUROOPA KONTROLLIKODA,

võttes arvesse Euroopa Liidu lepingu artiklit 13,

võttes arvesse Euroopa Liidu toimimise lepingu artiklit 287,

võttes arvesse Euroopa Parlamendi ja nõukogu 18. juuli 2018. aasta määruse (EL, Euratom) 2018/1046 (mis käsitleb liidu üldeelarve suhtes kohaldatavaid finantsreegleid) artiklit 257,

võttes arvesse kontrollikoja kodukorra rakenduseeskirjade (kontrollikoja otsus nr 21–2021) artikli 1 lõiget 6,

võttes arvesse teiste ELi institutsioonide, organite ja asutuste ELi salastatud teabe kaitsmise turvaeeskirju,

võttes arvesse kontrollikoja infoturbepoliitikat (DEC 127/15 FINAL) ja teabe salastamise poliitikat (teatis personalile 123/2020),

arvestades, et Euroopa Liidu toimimise lepingu (edaspidi „ELTL“) artikli 287 lõike 3 kohaselt on kontrollikojal õigus tutvuda kõigi asjakohaste dokumentidega ja teabega, sealhulgas ELi salastatud teabega, mis on tema arvates vajalikud oma volituste täitmiseks, mida tuleb täita institutsioonide vahelise lojaalse koostöö põhimõtte ja volituste andmise põhimõtte kohaselt; seadmata kahtluse alla Euroopa Liidu toimimise lepinguga tagatud juurdepääsuõigust ELi salastatud teabele, samas kui kontrollikojal võidakse paluda kehtestada teatavad turvameetmed ja neid järgida, nagu on siin täpsemalt kirjeldatud;

arvestades, et kontrollikoja liikmeid ning selle ametnikke ja teisi töötajaid seob isegi pärast teenistusest lahkumist konfidentsiaalsuskohustus vastavalt ELTLi artiklile 339, personalieeskirjade artiklile 17 ja nende alusel vastuvõetud aktidele;

arvestades, et kuna ELi salastatud teabe käitlemine on tundlik, peab konfidentsiaalsuskohustuse täitmine olema tagatud asjakohaste turvameetmetega, mis suudavad tagada selle teabe kõrgetasemelise kaitse ja mis on samaväärsed kaitse-eeskirjadega kehtestatud nõuetega, mis on ELi salastatud teabe osas vastu võetud teiste ELi institutsioonide, organite ja asutuste poolt, pidades silmas, et juhul kui kontrollikoda leiab, et sellised turvameetmed ei ole ELi salastatud teabe laadi ja tüüpi arvestades õigustatud, jätab kontrollikoda endale õiguse esitada mis tahes vajalikuks peetavaid tähelepanekuid, austades samal ajal ELi salastatud teabe salastatuse taset;

arvestades, et kontrollikojale edastatud teabe konfidentsiaalsuse, tervikluse ja kättesaadavuse kaitseks ette nähtud turvameetmed peavad vastama asjaomase teabe laadile ja tüübile;

arvestades, et vastavalt teadmisvajaduse põhimõttele peab kontrollikojale olema tagatud juurdepääs salastatud teabele aluslepingutega ja aluslepingute alusel vastuvõetud õigusaktidega pandud ülesannete täitmiseks;

arvestades, et teatava teabe olemuse ja tundliku sisu tõttu on asjakohane kehtestada ELi salastatud teavet sisaldavate dokumentide kontrollimiseks kontrollikoja jaoks erimenetlus;

arvestades, et institutsioon peab tagama, et käesolevat otsust rakendatakse kooskõlas kõigi kohaldatavate eeskirjadega, eelkõige sätetega, mis käsitlevad isikute turvalisust, isikute, hoonete ja IT-taristu füüsilist julgeolekut ning üldsuse juurdepääsu dokumentidele;

ON VASTU VÕTNUD JÄRGMISE OTSUSE:

Artikkel 1. Otsuse ese ja kohaldamisala

1) Käesolevas otsuses sätestatakse salastatud teabe, mida kontrollikoda käsitleb oma volituste täitmisel, kaitse aluspõhimõtted ja miinimumstandardid.

2) Käesolevas otsuses tähendab salastatud teave mis tahes või kogu alljärgnevat tüüpi teavet:

a) „ELi salastatud teave“, nagu see on määratletud teiste ELi institutsioonide, organite ja asutuste turbe-eeskirjades ja millel on üks järgmistest salastatuse taseme tähistest:

- TRÈS SECRET UE / EU TOP SECRET: teave ja materjal, mille loata avaldamine võib väga oluliselt kahjustada Euroopa Liidu või ühe või mitme liikmesriigi olulisi huve;
- SECRET UE / EU SECRET: teave ja materjal, mille loata avaldamine võib oluliselt kahjustada Euroopa Liidu või ühe või mitme liikmesriigi olulisi huve;
- CONFIDENTIEL UE / EU CONFIDENTIAL: teave ja materjal, mille loata avaldamine võib kahjustada Euroopa Liidu või ühe või mitme liikmesriigi olulisi huve;
- RESTREINT UE / EU RESTRICTED: teave ja materjal, mille loata avaldamine võib negatiivselt mõjutada Euroopa Liidu või ühe või mitme liikmesriigi huve;

b) liikmesriikide esitatud salastatud teave, millel on riigisisene salastatuse taseme tähis, mis on samaväärne punktis a loetletud ELi salastatud teabe salastatuse taseme märgistusega[1];

c) salastatud teave, mille kolmandad riigid või rahvusvahelised organisatsioonid on edastanud Euroopa Kontrollikojale ja millel on punktis a loetletud ELi salastatud teabe salastatuse taseme märgisega samaväärne turvaklassifikatsiooni tähis, nagu on sätestatud asjakohastes teabeturbe lepingutes või halduskokkulepetes.

3) Kontrollikoda käitleb RESTREINT UE / EU RESTRICTED tasemel salastatud teavet oma ruumides ja võtab selleks kõik vajalikud kaitsemeetmed. Kontrollikoja töötajatele, kes vajavad juurdepääsu ELi salastatud teabe kõrgemale tasemele, korraldatakse osalemine nii, et seda saaks teha teistes ELi institutsioonide, organite ja asutuste sobivates ruumides.

4) Seda otsust kohaldatakse kõigi kontrollikoja osakondade ja ruumide suhtes.

[1] Vt nõukogus kokku tulnud Euroopa Liidu liikmesriikide vaheline 4. mail 2011. aastal sõlmitud kokkulepe, mis käsitleb Euroopa Liidu huvides vahetatava salastatud teabe kaitset, ja selle lisa (ELT 2011/C 202/13).

5) Välja arvatud juhul, kui see otsus puudutab konkreetseid töötajate rühmi, kohaldatakse käesolevat otsust kontrollikoja liikmete ja kontrollikoja töötajate suhtes, kellele kehtivad Euroopa Liidu personalieeskirjad ja teiste teenistujate teenistustingimused[2], samuti liikmesriikide kontrollikoja juurde lähetatud riiklikke ekspertide, teenuseosutajate, nende töötajate, praktikantide ja kõikide isikute, kellel on juurdepääs kontrollikoja hoonetele ja muudele kinnistutele või kontrollikoja poolt hallatavale teabele, suhtes.

6) Kui ei ole sätestatud teisiti, kohaldatakse ELi salastatud teabe sätteid samaväärsel viisil selle artikli lõike 2 punktides b ja c osutatud salastatud teabe suhtes.

Artikkel 2. **Mõisted**

Käesolevas otsuses kasutatakse järgmisi mõisteid:

a) „luba juurdepääsuks ELi salastatud teabele“ tähendab kontrollikoja personali, finantsküsimuste ja üldteenuste direktori otsust liikmesriigi pädeva asutuse poolt antud kinnituse põhjal, et kontrollikoja ametnikule, muule töötajale või lähetatud riiklikule eksperdile võib anda loa juurdepääsuks ELi salastatud teabele eeldusel, et sellekohane vajadus on kindlaks tehtud ja neid on nende vastutusest asjakohaselt teavitatud, ning lubada kindlaksmääratud kuupäevani juurdepääsu teatava salastatuse tasemega teabele (CONFIDENTIEL UE / EU CONFIDENTIAL või kõrgem tase); sellist isikut loetakse „turvakontrolli läbinuks“;

b) „salastatus“ tähendab salastatuse taseme määramist teabele, lähtudes tõsisest kahjust, mida selle loata avalikustamine võib põhjustada;

c) „krüptomaterjal“ tähendab krüptoalgoritme, krüptoriistvara ja -tarkvara mooduleid ning tooteid, sealhulgas rakendamise üksikasju ja seotud dokumentatsiooni ning kodeerimisandmed;

d) „salastatuse kustutamine“ tähendab salastatuse tühistamist;

e) „dokument“ tähendab mis tahes talletatud teavet selle füüsilisest kujust ja omadustest olenemata;

f) „taseme alandamine“ tähendab salastatuse taseme alandamist;

g) „töötlemisluba“ tähendab pädeva julgeolekuasutuse haldusotsust selle kohta, et lähtudes turvalisuse seisukohast peab asjaomastes ruumides olema tagatud piisaval tasemel kaitse vastavalt ELi salastatud teabe salastatuse tasemele;

h) „käitlemine“: ELi salastatud teabe käitlemine tähendab kõiki võimalikke toiminguid, mida ELi salastatud teabega võidakse selle eluaja jooksul teha: loomine, registreerimine, töötlemine, transportimine, taseme alandamine, salastatuse kustutamine ja teabe hävitamine. Side- ja infosüsteemide puhul hõlmab see ka teabe kogumist, kuvamist, edastamist ja säilitamist;

i) „valdaja“ tähendab kontrollitud teadmisvajadusega nõuetekohaselt volitatud isikut, kelle valduses on salastatud teave ja kes seetõttu vastutab selle kaitsmise eest;

j) „infoturbeametnik“ tähendab kontrollikoja infoturbeametnikku, kes võib täielikult või osaliselt delegeerida käesolevas otsuses sätestatud ülesandeid;

k) „teave“ tähendab kirjalikku või suulist teavet selle kandjast või autorist olenemata;

[2] Määrus nr 31 (EMÜ), millega kehtestatakse ametnike personalieeskirjad ja muude teenistujate teenistustingimused, muudetud, EÜT 01 962R0031–1.1.2020–019.003–1 (https://eur-lex.europa.eu/eli/reg/1962/31 (1)/2020–01-01).

l) „materjal“ tähendab mis tahes meediumit, andmekandjat, masinat või seadet;

m) „teabe koostaja“ tähendab ELi institutsiooni, organit või asutust, liikmesriiki, kolmandat riiki või rahvusvahelist organisatsiooni, kelle volitusel on salastatud teave loodud ja/või ELi struktuuridesse sisestatud;

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

o) „juurdepääsutõend“ tähendab pädeva asutuse poolt väljastatud tõendit, mis kinnitab, et isikul on kontrollikoja personali, finantsküsimuste ja üldteenuste direktori antud salastatud teabele juurdepääsu luba, millel on märgitud, millisele ELi salastatud teabe tasemele (CONFIDENTIEL UE / EU CONFIDENTIAL või kõrgem tase) on asjaomasele isikule luba antud, vastava juurdepääsutõendi kehtivusaeg ja tõendi enda kehtivuse lõppemise kuupäev;

p) „füüsilise turvalisuse haldur“ tähendab kontrollikoja turvajuhti, kes vastutab ELi salastatud teabe kaitsmiseks vajalike füüsiliste turvameetmete ja -menetluste rakendamise eest;

q) „registriosakonda“ haldab kontrollikoja sekretariaat, mis asub haldustegevuse aladel ja mille eest vastutab kontrollikoja personali, finantsküsimuste ja üldteenuste direktor. Ta vastutab kontrollikojaga vahetatud RESTREINT UE / EU RESTRICTED või samaväärse taseme teabe sisestamise ja väljastamise eest;

r) „ELi salastatud teabe register“ on ala, mis asub turvaalal. Registrit haldab kontrollikoja julgeolekukontrolli läbinud ja volitatud registrikontrolli ametnik. Ta vastutab kontrollikojaga vahetatud CONFIDENTIEL UE / EU CONFIDENTIAL või kõrgema taseme või samaväärsel tasemel teabe sisestamise ja väljastamise eest;

s) „Turvalisuse akrediteerimise asutus“ tähendab kontrollikoja personali, finantsküsimuste ja üldteenuste direktorit.

Artikkel 3. Meetmed ELi salastatud teabe kaitsmiseks

1) Kontrollikoda tagab kogu talle edastatud salastatud teabe kaitsmise viisil, mis on proportsionaalne koostaja poolt määratud salastatuse tasemega ja kooskõlas käesoleva otsusega.

2) Selleks võtab kontrollikoda ELi salastatud teabe käitlemiseks kasutusele füüsilised ja vajaduse korral personali hõlmavad turvameetmed, sealhulgas tuvastatud isikute juurdepääsuload ning side- ja infosüsteemide kaitsemeetmed. Neid meetmeid on kirjeldatud artiklites 4 kuni 6 ja neid kohaldatakse kogu ELi salastatud teabe olelusringi vältel. Need peavad olema vastavuses ELi salastatud teabe salastatuse taseme, teabe või materjali vormi ja hulgaga, ELi salastatud teavet sisaldavate rajatiste asukoha ja ülesehitusega ning kohapeal antud hinnanguga kuritahtliku ja/või kriminaalse tegevuse ohu kohta (sealhulgas spionaažist, sabotaažist ja terrorismist tulenev oht).

3) ELi salastatud teavet kaitstakse füüsiliste turvameetmetega ning teavet, mis on klassifitseeritud tasemele CONFIDENTIEL UE / EU CONFIDENTIAL või kõrgemale, kaitstakse lisaks juurdepääsumeetmetega.

4) ELi salastatud teavet võib anda ainult institutsioonis kindlaks tehtud teadmisvajadusega isikutele. ELi salastatud teabe mis tahes eseme valdaja peab seda kaitsma nii, nagu on käesolevas otsuses nõutud.

5) ELi salastatud teavet ei tohi avalikustada suuliselt ega kirjalikult. Kontrollikoja esialgsed tähelepanekud, aruanded, arvamused, pressiteated ja muud tooted, selle veebisait ja sisevõrk, suulised seisukohavõtud, vastused dokumentidele juurdepääsu taotlustele[3] ning hääle- või videosalvestised ei tohi sisaldada ELi salastatud teavet ja nende väljavõtteid ega viidata neile. Kui koostaja on avaldanud dokumente või teavet, mis sisaldavad viidet ELi salastatud teabele, võib seda viidet mainida.

6) Olenemata lõikest 5 võivad kontrollikoda ja koostaja kokku leppida, et konkreetse auditi korral võib kontrollikoda oma dokumentides ELi salastatud teabe elemente korrata või kasutada. Sellisel juhul adresseeritakse kontrollikoja dokument enne ärakuulamismenetlust või selle ajal kõigepealt ELi salastatud teabe koostajale. Sellises olukorras lepivad kontrollikoda ja koostaja kokku, kas kontrollikoja vastu võetud dokument tuleb salastada. Kui kontrollikoja aruandev liige peab vajalikuks edastada Euroopa Parlamendis või nõukogus teatavatele adressaatidele täielikult või osaliselt salastatud auditiaruanne, võttes arvesse kõiki käesoleva otsusega seotud turvameetmeid, on selleks vaja salastatud teabe koostaja nõusolekut. Selliste dokumentide vahetamise õiguslik raamistik ja kord on sätestatud artiklis 7.

7) Kui tema volituste täitmiseks on vaja salastatud dokumendi või teabe teatud elementide laiemat jagamist (kui on olemas ülekaalukas avalik huvi), konsulteerib kontrollikoda enne nende elementide või teabe kasutamise otsustamist koostajaga, võttes nõuetekohaselt arvesse salastatuse taset. Teavet kasutatakse aruandes ainult nii, et see ei kahjustaks dokumendi koostaja huve. Selleks palutakse dokumendi koostajal esitada oma kommentaarid, et jõuda kokkuleppele teabe anonüümseks muutmise, tihendamise, üldistamise jms osas, austades samal ajal nende huve, keda avaldatud teave peamiselt puudutab.

8) Kontrollikoda ei esita ELi salastatud teavet ühelegi teisele ELi institutsioonile, organile, asutusele, liikmesriigile, kolmandale riigile ega rahvusvahelisele organisatsioonile ilma dokumendi koostajaga eelnevalt konsulteerimata ja tema kirjaliku nõusolekuta.

9) Kui SECRET UE / EU SECRET või madalama taseme dokumendi koostaja ei ole selle paljundamisele või tõlkimisele piiranguid seadnud, võib selliseid dokumente teabe valdaja taotlusel paljundada või tõlkida vastavalt kontrollikoja infoturbeametniku praktilistele tööjuhistele. Originaaldokumendi suhtes kohaldatavaid turvameetmeid rakendatakse ka selle dokumendi koopiate ja tõlgete suhtes.

10) Kui kontrollikoda vajab salastatud dokumendi, millele ta on saanud juurdepääsu või millel on luba juurdepääsuks, salastatuse taseme vähendamist või salastatuse kustutamist, konsulteerib kontrollikoda dokumendi koostajaga, et küsida, kas koostaja saab esitada dokumendi madalamal salastatuse tasemel või salastamata versiooni.

Artikkel 4. Töötajatega seotud turvalisus

1) Oma ülesannete täitmise tõttu on kontrollikoja liikmetele antud juurdepääs kogu ELi salastatud teabele ja neil on lubatud osaleda koosolekutel, kus ELi salastatud teavet käideldakse. Liikmeid teavitatakse ELi salastatud teabe kaitsega seotud turvakohustustest ja nad kinnitavad kirjalikult oma vastutust sellise teabe kaitsmise eest.

[3] Vastavalt kontrollikoja otsusele nr 12–2005 kontrollikoja dokumentidele avaliku juurdepääsu kohta, mida on muudetud otsusega nr 14–2009 (ELT 2009/C 67/1).

2) Kontrollikoja töötajale, olenemata sellest, kas tegemist on ametniku või töötajaga, kelle suhtes kehtivad muude teenistujate teenistustingimused, või lähetatud riikliku eksperdiga, antakse juurdepääs ELi salastatud teabele alles pärast järgmist:

   i. nende teadmisvajadus on kindlaks tehtud;

   ii. neid on teavitatud ELi salastatud teabe kaitseks vajalikest turvanormidest ja vastavatest turvastandarditest ja -suunistest ning nad on kirjalikult kinnitanud oma vastutust seoses kõnealuse teabe kaitsmisega; ja

   iii. teabe puhul, mis on klassifitseeritud CONFIDENTIEL UE / EU CONFIDENTIAL või kõrgemale tasemele, on nad läbinud julgeolekukontroll ja neile on antud juurdepääsuluba.

3) Menetlus selle kindlaksmääramiseks, kas kontrollikoja ametnikul või muul töötajal võib olla juurdepääs CONFIDENTIEL UE / EU CONFIDENTIAL või kõrgemale tasemele liigitatud teabele, võttes arvesse isiku lojaalsust, ausust ja usaldusväärsust ning pärast artikli 2 punktis n osutatud liikmesriigi pädevatelt asutustelt kinnituse saamist sätestatakse see artikli 10 lõike 10 kohaselt vastuvõetud delegeeritud otsuses. Juurdepääsuloa andmise otsused teeb kontrollikoja personali, finantsküsimuste ja üldteenuste direktor.

4) Kontrollikoja personali, finantsküsimuste ja üldteenuste direktor võib anda juurdepääsuloa, määrates kindlaks salastatuse taseme, mille puhul üksikisikutele võidakse anda juurdepääs ELi salastatud teabele (CONFIDENTIEL UE / EU CONFIDENTIAL või kõrgem tase), vastava juurdepääsuloa kehtivuse ja juurdepääsuloa aegumiskuupäeva.

5) Koosolekutel, kus käideldakse CONFIDENTIEL UE / EU CONFIDENTIAL või kõrgemal salastatuse tasemel teavet, võivad osaleda ainult isikud, kellel on lõike 2 punkti iii kohane luba ja kontrollikoja liikmed vastavalt käesoleva artikli lõikele 1. Kontrollikoda ja koostaja teostavad selliste koosolekute praktilise korralduse igal üksikjuhul eraldi.

6) Kontrollikoja osakonnad, mis vastutavad selliste koosolekute korraldamise eest, kus tuleb käidelda CONFIDENTIEL UE / EU CONFIDENTIAL või kõrgema taseme teavet, teavitavad infoturbeametnikku aegsasti koosolekute kuupäevadest, kellaaegadest ja kohtadest koos osalejate nimekirjadega.

7) Iga isik, kelle valduses on ELi salastatud teave, ja kellel puudub nõuetekohane juurdepääsuluba ja/või kellel puudub tõendatud teadmisvajadus, peab võimalikult kiiresti olukorrast infoturbeametnikule teatama ja tagama, et ELi salastatud teave oleks kaitstud vastavalt käesolevale otsusele.

Artikkel 5. Salastatud teabe kaitseks kasutatavad füüsilised turvameetmed

1) „Füüsiline turvalisus“ tähendab füüsiliste ja tehniliste kaitsemeetmete rakendamist, et vältida volitamata juurdepääsu ELi salastatud teabele.

2) Füüsiliste turvameetmete eesmärk on välistada salajane või jõuga sissetung, hoida ära, takistada ja avastada lubamatuid toiminguid ning võimaldada töötajate eristamist seoses juurdepääsuga ELi salastatud teabele teadmisvajaduse alusel. Need meetmed määratakse kindlaks vastavalt käesolevale otsusele riskijuhtimismenetluse alusel.

3) Kontrollikoja pädev infoturbeametnik kontrollib regulaarselt alasid, kus toimub ELi salastatud teabe käitlemine või säilitamine.

4) ELi salastatud teabe käitlemiseks ja säilitamiseks kasutatakse ainult vahendeid või seadmeid, mis vastavad ELi salastatud teabe kaitsmiseks ELi institutsioonides, organites ja asutustes kohaldatavatele eeskirjadele.

5) Kontrollikoja töötajad võivad saada juurdepääsu ELi salastatud teabele, mille salastatuse tase on CONFIDENTIEL UE / EU CONFIDENTIAL või kõrgem (või samaväärsele teabele) turvaaladel väljaspool kontrollikoja ruume.

6) Kontrollikoda võib sõlmida teenustaseme kokkuleppe mõne teise ELi institutsiooniga Luksemburgis, et võimaldada selle asutuse turvaalal käidelda ja säilitada salastatuse tasemele CONFIDENTIEL UE / EU CONFIDENTIAL või kõrgemale kuuluvat teavet. Kui dokumentide koostajaga ei ole konkreetselt kokku lepitud, ei käidelda ega säilitata seda ELi salastatud teavet kontrollikoja ruumides ning kontrollikoda ei tohi seda paljundada ega tõlkida.

7) Kontrollikoda registreerib vastu võetud RESTREINT UE / EU RESTRICTED teabe. Konfidentsiaalse teabega, mis kuulub salastatuse tasemele CONFIDENTIEL UE / EU CONFIDENTIAL või kõrgemale või on sellega samaväärne, tutvumine väljaspool kontrollikoja ruume registreeritakse turvaeesmärkidel.

8) RESTREINT UE / EU RESTRICTED tasemele klassifitseeritud ELi salastatud teavet säilitatakse sobivas lukustatud kontorimööblis haldustegevuse või turvaalal. Salastatuse tasemele CONFIDENTIEL UE / EU CONFIDENTIAL või SECRET UE / EU SECRET klassifitseeritud ELi salastatud teavet hoitakse teenustaseme kokkuleppe alusel turvaalal turvakonteineris mõnes teises ELi institutsioonis, mis asub Luksemburgis.

9) Registriväliselt edastatakse ELi salastatud teavet osakondade ja ruumide vahel järgmiselt:

   a) üldjuhul edastatakse ELi salastatud teave elektrooniliselt, kaitstuna artikli 6 lõike 8 kohaselt heakskiidetud krüptovahenditega;

   b) kui seda ei edastata punktis a kirjeldatud viisil, edastatakse ELi salastatud teave artikli 6 lõike 8 kohaselt heaks kiidetud krüptotoodetega kaitstud andmekandjal (nt USB-mälupulk, CD, kõvaketas) või paberkoopiana läbipaistmatus suletud ümbrikus.

10) Teabe valdaja võib RESTREINT UE / EU RESTRICED taseme teavet hävitada vastavalt kontrollikojas kehtivatele arhiveerimisreeglitele. Salastatuse tasemele CONFIDENTIEL UE / EU CONFIDENTIAL või kõrgemale klassifitseeritud teavet võib hävitada ainult registri kontrolliametnik, kui teabe valdaja või pädev ametiisik on andnud selleks korralduse kooskõlas kontrollikojas kohaldatud arhiveerimise eeskirjadega. Salastatuse tasemele SECRET UE / EU SECRET klassifitseeritud dokumendid hävitatakse sellise tunnistaja juuresolekul, kelle salastatud teabele juurdepääsu luba vastab vähemalt hävitatava dokumendi salastatuse tasemele. Registri kontrolliametnik ja tunnistaja, kui ta peab olema kohal, kirjutavad alla hävitamise protokollile, mis kantakse registrisse. Registri kontrolliametnik peab CONFIDENTIEL UE / EU CONFIDENTIAL ja SECRET UE / EU SECRET dokumentide hävitamise kohta arvestust vähemalt viis aastat.

11) Füüsilise julgeoleku ametiisik ja infoturbeametnik koostavad kohalikke olusid arvesse võttes ühise kava ELi salastatud teabe kaitsmiseks kriisiolukorras, sealhulgas vajaduse korral selle hävitamise või hädaolukorras evakueerimise plaanid. Nad koostavad juhised, mida nad peavad vajalikuks, et välistada ELi salastatud teabe sattumist volitamata isikute kätte.

12) Kui ELi salastatud teavet tuleb füüsiliselt transportida, järgib kontrollikoda dokumentide koostaja kehtestatud meetmeid, et kaitsta neid loata avalikustamise eest transpordi ajal.

13) Füüsilised turvameetmed, mida rakendatakse haldustegevuse aladel, kus käideldakse ja hoitakse RESTREINT UE/EU RESTRICTED teavet, on sätestatud lisas.

Artikkel 6. **ELi salastatud teabe kaitse side- ja infosüsteemides**

1) Käesolevas artiklis kasutatuna tähendab „side- ja infosüsteem“ mis tahes süsteemi, mis võimaldab ELi salastatud teavet elektrooniliselt käidelda. Side- ja infosüsteem hõlmab kõiki selle toimimiseks vajalikke vahendeid, sealhulgas infrastruktuuri, töökorralduse, töötajate ja teabega seotud ressursse.

2) „Seaduslik kasutaja“ tähendab kontrollikoja liiget, ametnikku, muud töötajat või lähetatud riiklikku eksperti, kellel on kindel ja tunnustatud vajadus pääseda juurde konkreetsele infosüsteemile.

3) Kontrollikoda tagab, et tema süsteemid kaitsevad nende poolt käideldavat teavet vajalikul määral ja toimivad vastavalt vajadusele seaduslike kasutajate kontrolli all. Selleks tagavad nad asjakohase taseme järgnevates küsimustes:

- autentsus: tagatakse, et teave on ehtne ja pärineb heausksest allikast;
- käideldavus: teave on volitatud isiku taotluse korral kättesaadav ja kasutatav;
- konfidentsiaalsus: teavet ei avalikustata volitamata isikutele, üksustele või protsessidele;
- terviklikkus: vara ja teabe täpsuse ja terviklikkuse kaitse;
- salgamise vääramine: võime tõendada tegevuse või sündmuse toimumist selliselt, et kõnealuse tegevuse või sündmuse toimumist ei saa hiljem eitada.

Selle kindluse aluseks on riskijuhtimisprotsess. „Risk“ tähendab võimalust, et antud oht kasutab ära organisatsiooni või selle poolt kasutatava süsteemi sisemisi või väliseid haavatavusi ning kahjustab seeläbi organisatsiooni ja selle materiaalset ja mittemateriaalset vara. Riski mõõdetakse olemasolevate ohtude tõenäosuse ja nende mõju kombinatsioonina; Riskijuhtimisprotsess koosneb järgmistest etappidest: ohtude ja haavatavuse kindlakstegemine, riskihindamine, riskide käsitlemine, riski aktsepteerimine ja riskidest teavitamine.

- „Riskihindamine“ sisaldab ohtude ja haavatavuse kindlakstegemist ning sellega seotud riskianalüüsi, st riski tõenäosuse ja mõju hindamist.
- „Riski käsitlemine“ sisaldab riski leevendamist, kõrvaldamist, vähendamist (tehniliste, füüsiliste, korralduslike või menetluslike meetmete asjakohase kombineerimise abil), riski ülekandmist või seiret.
- „Riski aktsepteerimine“ on otsus leppida jääkriski edasise olemasoluga pärast riski käsitlemist.
- „Jääkrisk“ on risk, mis jääb püsima pärast turvameetmete rakendamist, eeldusel et kõiki ohte ei ole tõrjutud ning kõiki haavatavusi ei saa kõrvaldada;
- „Riskidest teavitamine“ sisaldab side- ja infosüsteemide kasutajaskonna riskiteadlikkuse suurendamist, heakskiitvate asutuste teavitamist sellistest riskidest ja riske käsitlevat aruandlust töötlejatele.

4) Kõik ELi salastatud teabe käitlemiseks kasutatavad elektroonilised seadmed ja vahendid vastavad ELi salastatud teabe kaitsmiseks kohaldatavetele eeskirjadele. Eelistatakse elektroonilisi seadmeid ja vahendeid, mille teineELi institutsioon, organ või asutus on juba akrediteerinud. Seadmete turvalisus tagatakse kogu nende olelusringi vältel.

5) Kontrollikoja ELi salastatud teabe käitlemise side- ja infosüsteemi akrediteerib asjakohane asutus. Seetõttu taotleb kontrollikoda teenustaseme kokkulepet ELi institutsiooni julgeoleku akrediteerimisasutusega, kellel on võimalus akrediteerida ELi salastatud teabe käitlemine side- ja infosüsteemides, eesmärgiga saada RESTREINT UE/EU RESTRICTED akrediteerimisavalduse teave, mida võib käidelda kontrollikoja side- ja infosüsteemis ning vastavad toimimistingimused. Teenustaseme kokkulepe viitab ka akrediteerimisprotsessis kohaldatavatele standarditele ja see sõlmitakse artikli 10 lõikes 3 sätestatud korras.

6) Juhul kui kontrollikoda kehtestab side- ja infosüsteemi jaoks oma akrediteerimisprotsessi, kehtestatakse käesoleva otsuse artikli 10 lõikes 10 osutatud delegeeritud otsusega protsess kooskõlas side- ja infosüsteemi akrediteerimisprotsessi standarditega, mis käsitlevad ELi salastatud teabe käitlemist muudes ELi institutsioonides, organites ja asutustes.

7) Kohaldatavate standardite kohaste akrediteerimisfailide ja dokumentide ettevalmistamise eest vastutab täielikult side- ja infosüsteemi omanik.

8) Kui ELi salastatud teave on krüptovahenditega kaitstud, eelistab kontrollikoda tooteid, mille on krüptovahendite heakskiitmise asutusena heaks kiitnud nõukogu või nõukogu peasekretär, või muul juhul teiste ELi institutsioonide, organite ja asutuste poolt heaks kiidetud tooteid ELi salastatud teabe kaitsmiseks.

9) RESTREINT UE/EU RESTRICTED teavet käideldakse ainult elektroonilistes seadmetes (näiteks tööjaamad, printerid, koopiamasinad), mis asuvad haldustegevuse või turvaalal. Elektroonilised seadmed, milles käideldakse RESTREINT UE/EU RESTRICTED teavet, eraldatakse teistest arvutivõrkudest ja kaitstakse asjakohaste füüsiliste või tehniliste meetmetega.

10) Kõik kontrollikoja töötajad, kes osalevad ELi salastatud teavet käitleva side- ja infosüsteemi loomisel, arendamisel, katsetamisel, rakendamisel, haldamisel või kasutamisel, teavitavad infoturbeametnikku kõigist võimalikest teabe turvalisusega seotud puudujääkidest, intsidentidest, rikkumistest või teabe ohtu sattumisest, mis võivad mõjutada side- ja infosüsteemi ja/või selles sisalduva ELi salastatud teabe kaitset.

Artikkel 7. Salastatud teabe vahetamise ja sellele juurdepääsu võimaldamise kord

1) Kui aluslepingute või aluslepingute alusel vastuvõetud õigusaktide kohaselt on see õigusaktidest tulenevalt kohustuslik, annavad ELi institutsioonid, organid ja asutused ning riigiasutused omal algatusel või kontrollikoja presidendi, aruandva liikme (liikmete) või peasekretäri kirjalikul taotlusel kontrollikojale juurdepääsu ELi salastatud teabele. See toimub järgmiselt.

2) Juurdepääsutaotlused saadetakse asjaomastele institutsioonidele kontrollikoja registriosakonna kaudu.

3) Vajaduse korral sõlmib kontrollikoda halduskokkuleppe, mis hõlmab ELi salastatud teabe või samaväärse teabe vahetamise praktikat.

4) Sellise halduskokkuleppe sõlmimiseks esitab kontrollikoda dokumendi koostajale kogu vajaliku teabe oma infoturbesüsteemi kohta. Vajaduse korral saab korraldada kontrollvisiidi.

5) Need halduskokkulepped sõlmitakse täielikult kooskõlas Euroopa Liidu lepingu artiklis 13 sätestatud delegeeritud ja lojaalse koostöö põhimõtetega. Halduskokkulepped sõlmitakse artikli 10 lõikes 4 sätestatud menetluse kohaselt.

6) Kui konkreetse ELi institutsiooni, organi või asutuse, kolmanda riigi või rahvusvahelise organisatsiooniga ei ole kontrollikojale salastatud teabe edastamise lepingut sõlmitud, allkirjastab kontrollikoda vastuvõetud salastatud teabe kaitsmise avalduse.

Artikkel 8. Turvanõuete rikkumine, salastatud teabe kadumine või ohtu sattumine

1) Turvanõuete rikkumine tähendab isiku sellist tegevust või tegevusetust, mis on vastuolus käesolevas otsuses sätestatud turvaeeskirjadega ja otsuse rakenduseeskirjadega.

2) Salajasuse kahjustamine tekib siis, kui turvarikkumise tõttu on ELi salastatud teavet täielikult või osaliselt avaldatud kõrvalistele isikutele.

3) Igast turvarikkumisest või turvarikkumise kahtlusest teatatakse viivitamatult kontrollikoja infoturbeametnikule.

4) Kui on teada või kui on alust arvata, et ELi salastatud teavet on kahjustatud või on see kadunud, teavitab infoturbeametnik sellest personali, finantsküsimuste ja üldteenuste direktorit ning kontrollikoja peasekretäri. Personali, finantsküsimuste ja üldteenuste direktor teavitab viivitamatult koostaja vastavat infoturbeametnikku. Eespool nimetatud kontrollikoja direktor viib läbi uurimise, teavitades kontrollikoja peasekretäri ja koostaja infoturbeametnikku uurimise tulemustest ning olukorra kordumise vältimiseks võetud meetmetest. Kui asi puudutab kontrollikoja liiget, vastutab meetmete võtmise eest kontrollikoja president koos kontrollikoja peasekretäriga.

5) Kontrollikoja ametnikule või teisele töötajale, kes on süüdi käesolevas otsuses ja selle rakenduseeskirjades sätestatud turvaeeskirjade rikkumises, kohaldatakse personalieeskirjades ja muude Euroopa Liidu teenistujate teenistustingimustes sätestatud karistusi.

6) Iga kontrollikoja liige, kes ei järgi käesoleva otsuse tingimusi, vastutab aluslepingu artikli 286 lõikes 6 sätestatud meetmete ja karistuste kohaselt.

7) Iga isiku suhtes, kes on süüdi ELi salastatud teabe kadumises või ohtu sattumises, võidakse kohaldada distsiplinaar- ja/või õiguslikke meetmeid vastavalt kohaldatavatele õigusnormidele.

Artikkel 9. Turvalisus välise töövõtjate kasutamise korral

1) Kontrollikoda võib usaldada nende ülesannete, mis lepingutest tulenevalt hõlmavad või nõuavad juurdepääsu ELi salastatud teabele, täitmise mõnes liikmesriigis registreeritud töövõtjatele. See võib juhtuda eelkõige seoses side- ja infosüsteemide ning arvutivõrgu hooldusega.

2) Väliste töövõtjate kasutamise korral võtab kontrollikoda kõik vajalikud käesoleva artikli lõikes 3 osutatud turvameetmed ja nõuab sealhulgas nende rajatiste turvalisuse kontrollimist, et tagada ELi salastatud teabe kaitsmine kandidaatide ja pakkujate poolt kogu hankemenetluse vältel ning töövõtjate ja alltöövõtjate poolt kogu lepingu kehtivusaja jooksul. Avaliku sektori hankija tagab, et lepingutes on nimetatud käesolevas otsuses sätestatud minimaalsed turvastandardid, et kohustada töövõtjaid neid järgima.

3) Turvaeeskirjad, hankemenetlused ning selliste lepingute ja allhankelepingute tüüpvormid ja näidised, mis hõlmavad juurdepääsu ELi salastatud teabele, hanketeateid, juhiseid tingimuste kohta, mille korral on vajalik rajatise ja personali jaoks salastatud teabele juurdepääsu luba, programmi või projekti turvajuhised, turvaaspektide kirjad, külastused ja selliste lepingute ja allhankelepingute alusel ELi salastatud teabe edastamine ja transportimine peab vastama eeskirjadele, tüüpvormidele ja näidistele, mille Euroopa Komisjon on salastatud lepingute jaoks kehtestanud komisjoni 13. märtsi 2015. aasta otsuses (EL, Euratom) 2015/444 ELi salastatud teabe kaitsmise turvaeeskirjade kohta.

Artikkel 10. Otsuse rakendamine ja sellega seotud kohustused

1) Kontrollikoja talitused võtavad oma vastutusalas kõik vajalikud meetmed tagamaks, et nad kohaldavad ELi salastatud teabe või mis tahes muu salastatud teabe käitlemisel või säilitamisel käesolevat otsust ja asjakohaseid rakenduseeskirju.

2) Peasekretär on ametisse nimetatav ametiisik ja ametiisik, kellel on õigus sõlmida kõikide ametnike ja teiste töötajate töölepinguid. Peasekretär võib delegeerida personali, finantsküsimuste ja üldteenuste direktorile vastutuse ametnikele ja teistele töötajatele volituste andmise eest juurdepääsuks CONFIDENTIEL UE/EU CONFIDENTIAL või kõrgema salastatuse tasemega teabele, turvalisuse akrediteerimise asutusena oma ülesannete täitmise eest ja kontrollima kontrollikoja sekretariaati ELi salastatud teabe käitlemisel.

3) Peasekretär on pädev sõlmima teenustaseme kokkuleppeid kontrollikoja side- ja infoseadmete ja -süsteemide akrediteerimise ning turvaala kasutamise kohta mõnes teises ELi institutsioonis ja ELi salastatud teabele juurdepääsu lubade taotluste korra kohta.

4) Personali, finantsküsimuste ja üldteenuste direktor on pädev sõlmima ELi institutsioonide, organite ja muude asutustega ELi salastatud teabe vahetamiseks halduskokkuleppeid, mida kontrollikoda vajab oma volituste täitmiseks. Samuti võib direktor sõlmida mis tahes saadud salastatud teabe kaitset käsitlevaid halduskokkuleppeid kolmandate riikide ja rahvusvaheliste organisatsioonidega.

5) Personali, finantsküsimuste ja üldteenuste direktor on pädev allkirjastama erandliku sihipärase ELi salastatud teabe avaldamise korral vajalikud avaldused ELi salastatud teabe kaitsmise kohta.

6) Kontrollikoja infoturbeametnik tegutseb infoturbeametnikuna. Infoturbeametnikud ja isikud, kellele nad delegeerivad kõik oma ülesanded või osa neist, peavad läbima asjakohase julgeolekukontrolli. Infoturbeametnik täidab oma kohustusi tihedas koostöös personali, finantsküsimuste ja üldteenuste direktoraadi, informatsiooni, töökeskkonna ja innovatsiooni direktoraadi ning auditi kvaliteedikontrolli komitee direktoraadiga (vt eelkõige artiklid 4, 6 ja 8). Infoturbeametnik vastutab ka infoturbealaste koolituste ja teadlikkuse tõstmise kohtumiste ning perioodiliste kontrollide eest, et kontrollida käesoleva otsuse täitmist, sealhulgas ka väliste töövõtjate puhul, ja tagada kõigi meetmete järgimine.

7) Turvajuht vastutab füüsiliste turvameetmete eest (eelkõige artikkel 5).

8) Kontrollikoja sekretariaadis asutatud registriosakond on RESTREINT UE/EU RESTRICTED tasemele liigitatud teabe, mida kontrollikoda võib vahetada teiste ELi institutsioonide, organite ja asutuste ning liikmesriikidega, sisend- ja väljundpunkt. See on ka kolmandate riikide ja rahvusvaheliste organisatsioonide samaväärse teabe sisend- ja väljundpunkt. Registriosakond korraldatakse delegeeritud otsuses sätestatud korras. Registriosakonna ametnik võtab endale järgmised põhikohustused:

   a) RESTREINT UE/EU RESTRICTED tasemele liigitatud teabe sisenemise ja väljumise registreerimine;

   b) RESTREINT UE/EU RESTRICTED tasemele liigitatud ELi salastatud teabe käitlemise, säilitamise ja sellega tutvumise jaoks loodud spetsiaalsete haldustegevuse alade haldamine.

9) Teenustaseme kokkulepete kaudu luuakse register teise ELi institutsiooni turvaalade kasutamise kohta. See register, mille kontrollikoja sekretariaat korraldab kontrollikoja personali, finantsküsimuste ja üldteenuste direktori vastutusel, on CONFIDENTIEL UE/EU CONFIDENTIAL või kõrgemale tasemele liigitatud teabe sisend- ja väljundpunkt, mille kaudu saab kontrollikoda vahetada teavet teiste ELi institutsioonide, organite ja asutuste ning liikmesriikidega. Register on ka kolmandate riikide ja rahvusvaheliste organisatsioonide samaväärse teabe sisend- ja väljundpunkt. See peab olema varustatud asjakohaste seifide ja muude turvaseadmetega, mis sobivad salastatuse taseme CONFIDENTIEL UE/EU CONFIDENTIAL või kõrgema taseme teabe kaitsmiseks. Register korraldatakse delegeeritud

otsuses sätestatud korras. Registri kontrolliametnikul peab olema asjakohane salastatud teabele juurdepääsu luba ning ta täidab järgmisi põhikohustusi:

a) ELi salastatud teabe registreerimise, konsulteerimise, säilitamise, paljundamise, tõlkimise, edastamise, saatmise ja vajaduse korral hävitamisega seotud toimingute haldamine;

b) delegeeritud otsustes määratletud muude ELi salastatud teabe kaitsega seotud ülesannete täitmine.

10) Halduskomitee võtab vastu delegeeritud otsuse, millega kehtestatakse käesoleva otsuse rakenduseeskirjad. Infoturbeametnik kehtestab infoturbe suunised. Auditi kvaliteedikontrolli komitee töötab välja auditijuhised.

Artikkel 11. **Jõustumine**

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

Luxembourg, 3. juuni 2021.

Kontrollikoja nimel

president
Klaus-Heiner Lehne

Lisa: FÜÜSILISED TURVAMEETMED ELi SALASTATUD TEABE KÄITLEMISEKS KASUTATAVATEL HALDUSTEGEVUSE ALADEL

LISA

FÜÜSILISED TURVAMEETMED ELi SALASTATUD TEABE KÄITLEMISEKS KASUTATAVATEL HALDUSTEGEVUSE ALADEL

1) Käesolev lisa sisaldab otsuse artikli 5 rakenduseeskirju. Need on kontrollikoja RESTREINT UE / EU RESTRICTED tasemel salastatud teabe käitlemiseks mõeldud haldustegevuse alade füüsilise turvalisuse miinimumnõuded: alad, mis on määratud RESTREINT UE / EU RESTRICTED tasemele liigitatud teabe salvestamiseks, säilitamiseks ja sellega tutvumiseks.

2) Füüsiliste turvameetmete eesmärk on vältida loata juurdepääsu nendele haldustegevuse aladele järgmiselt:

   a) kehtestatakse visuaalselt määratletud perimeeter, mis võimaldab isikuid kontrollida;

   b) saatjata juurdepääs antakse ainult isikutele, kellel on kontrollikoja infoturbeametniku või mõne muu pädeva asutuse nõuetekohane luba; ja

   c) kõik muud isikud võivad neis ruumides viibida ainult koos saatjaga või peavad läbima samaväärse kontrolli.

3) Kontrollikoja infoturbeametnik võib erandkorras lubada juurdepääsu volitamata isikutele, sealhulgas haldustegevuse alal töötamiseks, tingimusel, et sellega ei kaasne juurdepääsu ELi salastatud teabele, mis peab jääma lukustatuks. Sellised isikud võivad siseneda ainult siis, kui neid saadab ja jälgib pidevalt infoturbeametnik või registriosakonna ametnik.

4) Infoturbeametnik kehtestab kõigi haldustegevuse alade ja turvamööbli võtmete ja/või koodide haldamise korra. Nende menetluste eesmärk on tagada kaitse loata juurdepääsu eest.

5) Koodid tuleb pähe õppida ja koode teadvate isikute arv peab olema võimalikult väike. RESTREINT UE / EU RESTRICTED tasemel salastatud teabe säilitamiseks kasutatava turvamööbli koode muudetakse:

   - uue turvamööbli eseme kasutuselevõtul;
   - koodi teadva personali vahetumisel;
   - kui koodi salajasus on kahjustatud või kui tekib kahjustamise kahtlus;
   - kui lukku on hooldatud või parandatud;
   - vähemalt iga 12 kuu järel.

6) Nende eeskirjade järgimise eest vastutavad infoturbeametnik ja turvajuht.