EUROOPAN TILINTARKASTUS-TUOMIOISTUIN

Tilintarkastustuomioistuimen päätös 41-2021 EU:n turvallisuusluokiteltujen tietojen suojaamista koskevista säännöistä

EUROOPAN TILINTARKASTUSTUOMIOISTUIN, JOKA

ottaa huomioon Euroopan unionista tehdyn sopimuksen 13 artiklan,

ottaa huomioon Euroopan unionin toiminnasta tehdyn sopimuksen 287 artiklan,

ottaa huomioon unionin yleiseen talousarvioon sovellettavista varainhoitosäännöistä 18 päivänä heinäkuuta 2018 annetun Euroopan parlamentin ja neuvoston asetuksen (EU, Euratom) 2018/1046 257 artiklan,

ottaa huomioon tilintarkastustuomioistuimen työjärjestyksen soveltamissääntöjen (tilintarkastustuomioistuimen päätös 21/2021) 1 artiklan 6 kohdan,

ottaa huomioon muiden EU:n toimielinten, virastojen ja elinten turvallisuusluokiteltujen tietojen suojaamista koskevat säännöt,

ottaa huomioon tilintarkastustuomioistuimen tietoturvallisuutta koskevat toimintaperiaatteet (DEC 127/15 FINAL) ja tietojen luokitusta koskevat toimintaperiaatteet (henkilöstötiedote 123/2020),

katsoo että SEUT-sopimuksen 287 artiklan 3 kohdan nojalla tilintarkastustuomioistuimella on oikeus saada kaikki asiaankuuluvat asiakirjat ja tiedot, joiden se katsoo olevan tarpeen toimeksiantonsa täyttämiseksi, mukaan lukien EU:n turvallisuusluokitellut tiedot, ja niiden käyttöön saamisen on tapahduttava täysin toimielinten vilpittömän yhteistyön periaatteen ja annetun toimivallan periaatteen mukaisesti; että EU:n turvallisuusluokiteltujen tietojen luovuttaja ei voi kyseenalaistaa SEUT-sopimuksessa vahvistettua oikeutta saada EU:n turvallisuusluokiteltuja tietoja, ja katsoo, että tilintarkastustuomioistuinta voidaan pyytää ottamaan käyttöön ja noudattamaan tiettyjä turvatoimia jäljempänä esitetyn mukaisesti;

katsoo että tilintarkastustuomioistuimen jäseniä, sen virkamiehiä ja muuta henkilöstöä sitoo palvelussuhteen päättymisen jälkeenkin SEUT-sopimuksen 339 artiklassa, henkilöstösääntöjen 17 artiklassa ja niiden mukaisesti annetuissa säädöksissä tarkoitettu salassapitovelvollisuus;

katsoo että EU:n turvallisuusluokiteltujen tietojen arkaluonteisuuden vuoksi niiden käsittely edellyttää, että salassapitovelvollisuuden noudattaminen varmistetaan asianmukaisilla turvatoimilla, joilla voidaan taata kyseisille tiedoille korkeatasoinen suoja ja jotka vastaavat muiden EU:n toimielinten, virastojen ja elinten EU:n turvallisuusluokiteltujen tietojen suojaamisesta antamissa säännöissä vahvistettuja toimenpiteitä, siten, että jos tilintarkastustuomioistuin katsoo, että jokin tällainen turvatoimi ei ole

perusteltu EU:n turvallisuusluokiteltujen tietojen luonteen ja tyypin vuoksi, tilintarkastustuomioistuin varaa oikeuden esittää aiheellisiksi katsomiaan huomautuksia EU:n turvallisuusluokiteltujen tietojen turvallisuusluokkaa noudattaen;

katsoo että tilintarkastustuomioistuimelle ilmoitettujen tietojen luottamuksellisuutta, eheyttä ja saatavuutta suojaavien turvatoimien on oltava tarkoituksenmukaisia kyseessä olevien tietojen luonteen ja tyypin kannalta;

katsoo että tilintarkastustuomioistuimelle on myönnettävä pääsy turvallisuusluokiteltuihin tietoihin tiedonsaantitarpeen mukaan perussopimuksissa ja perussopimusten nojalla annetuissa säädöksissä asetettujen tehtävien suorittamiseksi;

katsoo että tiettyjen tietojen luonteen ja arkaluonteisen sisällön vuoksi on tarkoituksenmukaista ottaa käyttöön erityismenettely EU:n turvallisuusluokiteltuja tietoja sisältävien asiakirjojen käsittelemiseksi tilintarkastustuomioistuimessa;

katsoo että toimielimen on varmistettava, että tämä päätös pannaan täytäntöön kaikkien sovellettavien sääntöjen mukaisesti, erityisesti henkilötietojen suojaa, henkilöiden, rakennusten ja tietotekniikan fyysistä turvallisuutta sekä asiakirjojen julkisuutta koskevien säännösten mukaisesti;

ON HYVÄKSYNYT TÄMÄN PÄÄTÖKSEN:

<u>1 artikla.</u> Kohde ja soveltamisala

1) Tällä päätöksellä vahvistetaan turvallisuusluokiteltujen tietojen suojaamista koskevat perusperiaatteet ja vähimmäisvaatimukset, joita sovelletaan, kun tilintarkastustuomioistuin käsittelee tietoja toimeksiantonsa nojalla.

2) Tässä päätöksessä ’turvallisuusluokitelluilla tiedoilla’ tarkoitetaan jotakin seuraavista tietotyypeistä tai kaikkia niitä:

   a) ’EU:n turvallisuusluokitellut tiedot’, jotka määritellään muiden EU:n toimielinten, virastojen, elinten tai laitosten turvallisuussäännöissä ja joissa on jokin seuraavista turvallisuusluokitusmerkinnöistä:

      - TRÈS SECRET UE/EU TOP SECRET: tiedot ja materiaalit, joiden luvaton ilmitulo saattaisi vahingoittaa poikkeuksellisen vakavasti Euroopan unionin taikka yhden tai useamman jäsenvaltion olennaisia etuja;
      - SECRET UE/EU SECRET: tiedot ja materiaalit, joiden luvaton ilmitulo saattaisi vahingoittaa vakavasti Euroopan unionin tai yhden tai useamman jäsenvaltion olennaisia etuja;
      - CONFIDENTIEL UE/EU CONFIDENTIAL: tiedot ja materiaalit, joiden luvaton ilmitulo saattaisi vahingoittaa Euroopan unionin tai yhden tai useamman jäsenvaltion olennaisia etuja;
      - RESTREINT UE/EU RESTRICTED: tiedot ja materiaalit, joiden luvattomasta ilmitulosta saattaisi olla haittaa Euroopan unionin tai yhden tai useamman jäsenvaltion eduille.

b) jäsenvaltioiden toimittamat turvallisuusluokitellut tiedot, joilla on jotakin a alakohdassa lueteltua EU:n turvallisuusluokiteltujen tietojen turvallisuusluokitusmerkintää[1] vastaava kansallinen turvallisuusluokitusmerkintä;

c) kolmansien valtioiden tai kansainvälisten järjestöjen tilintarkastustuomioistuimelle toimittamat turvallisuusluokitellut tiedot, joilla on jotakin a alakohdassa lueteltua EU:n turvallisuusluokiteltujen tietojen turvallisuusluokitusmerkintää vastaava turvallisuusluokitusmerkintä asiaankuuluvien tietoturvasopimusten tai hallinnollisten järjestelyjen mukaisesti.

3) Tilintarkastustuomioistuin käsittelee RESTREINT UE/EU RESTRICTED -tason tietoja tiloissaan ja toteuttaa sitä varten kaikki tarvittavat suojatoimet. Niiden tilintarkastustuomioistuimen henkilöstön jäsenten osalta, joiden on saatava korkeamman tason EU:n turvallisuusluokiteltuja tietoja, sovitaan järjestelyistä, joiden perusteella he voivat käyttää tietoja tähän soveltuvissa muiden EU:n toimielinten, elinten tai virastojen tiloissa.

4) Tämä päätös koskee kaikki tilintarkastustuomioistuimen osastoja ja tiloja.

5) Tätä päätöstä sovelletaan tilintarkastustuomioistuimen jäseniin, Euroopan unionin virkamiehiin sovellettavien henkilöstösääntöjen ja unionin muuhun henkilöstöön sovellettavien palvelussuhteen ehtojen[2] alaiseen tilintarkastustuomioistuimen henkilöstöön, tilintarkastustuomioistuimeen lähetettyihin kansallisiin asiantuntijoihin, palveluntarjoajiin ja niiden henkilöstöön, harjoittelijoihin sekä kaikkiin henkilöihin, joilla on pääsy tilintarkastustuomioistuimen rakennuksiin tai muuhun omaisuuteen taikka tilintarkastustuomioistuimen käsittelemiin tietoihin, paitsi jos säännös koskee tiettyjä henkilöstöryhmiä.

6) Ellei toisin todeta, EU:n turvallisuusluokiteltuja tietoja koskevat säännöt koskevat samalla tavalla tämän artiklan 2 kohdan b ja c alakohdassa tarkoitettuja turvallisuusluokiteltuja tietoja.

2 artikla. **Määritelmät**

Tässä päätöksessä

a) ’valtuutuksella EU:n turvallisuusluokiteltuihin tietoihin pääsyä varten’ tarkoitetaan päätöstä, jonka tilintarkastustuomioistuimen henkilöstöhallinnon, taloushallinnon ja yleispalvelujen osaston johtaja tekee jäsenvaltion toimivaltaisen viranomaisen antaman lausunnon perusteella ja jonka mukaan tilintarkastustuomioistuimen virkamiehelle, toimihenkilölle tai kansalliselle asiantuntijalle voidaan myöntää pääsy EU:n turvallisuusluokiteltuihin tietoihin tiettyyn turvallisuusluokkaan (CONFIDENTIEL UE/EU CONFIDENTIAL tai sitä korkeampi) ja tiettyyn päivämäärään asti edellyttäen, että henkilön tiedonsaantitarve on todennettu ja että hänelle on tiedotettu asianmukaisesti hänelle kuuluvasta vastuusta. Henkilön katsotaan tämän jälkeen olevan ’turvallisuusvaltuutettu’;

b) ’luokituksella’ tarkoitetaan turvallisuusluokan osoittamista tiedoille sen haitan tason perusteella, jonka tietojen luvaton ilmitulo voisi aiheuttaa;

---

[1] Ks. neuvostossa kokoontuneiden Euroopan unionin jäsenvaltioiden välinen 4. toukokuuta 2011 tehty sopimus Euroopan unionin edun vuoksi vaihdettujen turvallisuusluokiteltujen tietojen suojaamisesta ja sen liite (EUVL 2011/C 202/13).

[2] Asetus N:o 31/ETY virkamiehiin sovellettavien henkilöstösääntöjen ja näiden yhteisöjen muuta henkilöstöä koskevien palvelussuhteen ehtojen vahvistamisesta, sellaisena kuin se on muutettuna, EUVL 01 962R0031 – 1.1.2020 – 019.003–1 (https://eur-lex.europa.eu/eli/reg/1962/31 (1)/2020-01–01).

c) ’salausaineistolla’ tarkoitetaan salausalgoritmeja, salauslaitteistoja ja -ohjelmistomoduuleja sekä tuotteita, joihin sisältyy täytäntöönpanoa koskevia yksityiskohtia sekä niihin liittyviä asiakirjoja ja avainnusaineistoa;

d) ’turvallisuusluokan poistamisella’ tarkoitetaan minkä tahansa turvallisuusluokan poistamista;

e) ’asiakirjalla’ tarkoitetaan mitä tahansa tallennettua tietoa sen fyysisestä muodosta tai ominaisuuksista riippumatta;

f) ’turvallisuusluokan alentamisella’ tarkoitetaan salassapitotason alentamisesta johtuvaa turvallisuusluokan muuttamista;

g) ’yhteisöturvallisuusselvityksellä’ tarkoitetaan toimivaltaisen tietoturvaviranomaisen hallinnollista päätöstä, jonka mukaan toimitila tarjoaa turvallisuusnäkökulmasta riittävän suojan tiettyyn turvallisuusluokkaan kuuluville EU:n turvallisuusluokitelluille tiedoille;

h) EU:n turvallisuusluokiteltujen tietojen ’käsittelyllä’ tarkoitetaan kaikkia mahdollisia toimia, joita EU:n turvallisuusluokiteltuihin tietoihin voidaan kohdistaa niiden elinkaaren aikana. Tällaisia toimia ovat tietojen tuottaminen, rekisteröinti, muokkaaminen, kuljetus, hävittäminen sekä turvallisuusluokan alentaminen ja poistaminen. Viestintä- ja tietojärjestelmien tapauksessa niihin kuuluvat myös tietojen kerääminen, näyttäminen, siirtäminen ja säilyttäminen;

i) ’haltijalla’ tarkoitetaan asianmukaisesti valtuutettua henkilöä, jonka tiedonsaantitarve on todennettu ja jonka hallussa on EU:n turvallisuusluokiteltu tieto, jonka suojaamisesta hän on näin ollen vastuussa;

j) ’tietoturvaviranomaisella’ tarkoitetaan tilintarkastustuomioistuimen tietoturvavastaavaa, joka voi siirtää tässä päätöksessä tarkoitettuja tehtäviä kokonaan tai osittain;

k) ’tiedolla’ tarkoitetaan kirjallista tai suullista tietoa sen tallennevälineestä tai laatijasta riippumatta;

l) ’materiaalilla’ tarkoitetaan mitä tahansa viestintä, tiedonsiirtovälinettä, konetta tai laitetta;

m) ’luovuttajalla’ tarkoitetaan EU:n toimielintä, elintä tai virastoa, jäsenvaltiota, kolmatta valtiota tai kansainvälistä järjestöä, jonka alaisuudessa turvallisuusluokiteltuja tietoja on tuotettu ja/tai tuotu EU:n rakenteisiin;

n) ’henkilöturvallisuusselvityksellä’ tarkoitetaan jäsenvaltion toimivaltaisen viranomaisen lausuntoa, joka annetaan jäsenvaltion toimivaltaisten viranomaisten tekemän turvallisuustutkinnan päätteeksi ja jonka mukaan henkilölle voidaan myöntää pääsy EU:n turvallisuusluokiteltuihin tietoihin tiettyyn turvallisuusluokkaan (CONFIDENTIEL UE/EU CONFIDENTIAL tai sitä korkeampi) ja tiettyyn päivämäärään saakka edellyttäen, että hänen tiedonsaantitarpeensa on todennettu ja että hänelle on tiedotettu asianmukaisesti hänelle kuuluvasta vastuusta;

o) ’henkilöturvallisuusselvitykseen perustuvalla todistuksella’ tarkoitetaan tilintarkastustuomioistuimen henkilöstöhallinnon, taloushallinnon ja yleispalvelujen osaston johtajan antamaa todistusta, jonka mukaan henkilöllä on voimassa oleva turvallisuusselvitys tai turvallisuusvaltuutus ja josta käy ilmi turvallisuusluokka, johon kuuluviin EU:n turvallisuusluokiteltuihin tietoihin henkilölle voidaan myöntää pääsy (CONFIDENTIEL UE/EU CONFIDENTIAL tai sitä korkeampi), asianomaisen turvallisuusselvityksen tai -valtuutuksen voimassaoloaika ja todistuksen voimassaolon päättymispäivä;

p) ’fyysisestä turvallisuudesta vastaavalla viranomaisella’ tarkoitetaan tilintarkastustuomioistuimen turvallisuuspäällikköä, joka vastaa tarvittavien fyysisten

turvatoimien ja -menettelyjen toteuttamisesta EU:n turvallisuusluokiteltujen tietojen suojaamiseksi;

q) tilintarkastustuomioistuimen sihteeristö hallinnoi ’rekisteritoimistoa’, joka sijaitsee tilintarkastustuomioistuimen henkilöstöhallinnon, taloushallinnon ja yleispalvelujen osaston johtajan vastuulla olevalla hallinnollisella alueella. Se vastaa tilintarkastustuomioistuimen kanssa vaihdettujen RESTREINT UE/EU RESTRICTED -tasolle luokiteltujen tietojen tai vastaavien tietojen saapumisesta ja lähtemisestä.

r) ’EU:n turvallisuusluokiteltujen tietojen rekisteri’ on turva-alueella sijaitseva alue. Rekisteriä hallinnoi tilintarkastustuomioistuimen turvallisuusselvitetty ja valtuutettu rekisterin valvontavastaava. Se vastaa tilintarkastustuomioistuimen kanssa vaihdettujen CONFIDENTIEL UE/EU CONFIDENTIAL -tasolle luokiteltujen tietojen tai vastaavien tietojen saapumisesta ja lähtemisestä.

s) ’turvallisuusjärjestelyjen hyväksyntäviranomaisella’ tarkoitetaan tilintarkastustuomioistuimen henkilöstöhallinnon, taloushallinnon ja yleispalvelujen osaston johtajaa.

3 artikla. **EU:n turvallisuusluokiteltujen tietojen suojaamistoimet**

1) Tilintarkastustuomioistuin varmistaa, että kaikki sille toimitetut turvallisuusluokitellut tiedot suojataan tämän päätöksen mukaisesti tavalla, joka on suhteutettu tietojen luovuttajan määrittämään turvallisuusluokkaan.

2) Siksi tilintarkastustuomioistuimen on edellytettävä EU:n turvallisuusluokiteltujen tietojen käsittelyltä fyysisiä ja tarvittaessa henkilöstöä koskevia turvatoimia, muun muassa tietoihin pääsyä koskevia valtuutuksia nimetyille henkilöille sekä toimia viestintä- ja tietojärjestelmien suojaamiseksi. Nämä toimet kuvataan 4–6 artiklassa, ja niitä sovelletaan EU:n turvallisuusluokiteltujen tietojen koko elinkaaren ajan. Ne on suhteutettava EU:n turvallisuusluokiteltujen tietojen turvallisuusluokkaan, tietojen tai materiaalin muotoon ja volyymiin, EU:n turvallisuusluokiteltujen tietojen säilytystilojen sijaintiin ja rakenteeseen sekä paikallisesti arvioituun vihamielisen ja/tai rikollisen toiminnan uhkaan, vakoilu, sabotaasi ja terrorismi mukaan lukien.

3) EU:n turvallisuusluokiteltuja tietoja suojataan fyysisillä turvatoimilla, ja CONFIDENTIEL UE/EU CONFIDENTIAL -tasolle tai sitä korkeammalle tasolle luokiteltuja tietoja suojataan lisäksi henkilöstöä koskevilla turvatoimilla.

4) EU:n turvallisuusluokiteltuja tietoja saa antaa toimielimessä vain henkilöille, joilla on tiedonsaantitarve. Minkä tahansa EU:n turvallisuusluokitellun tiedon haltijan on suojattava sitä tämän päätöksen vaatimusten mukaisesti.

5) EU:n turvallisuusluokiteltuja tietoja ei saa paljastaa suullisesti eikä kirjallisesti. Tilintarkastustuomioistuimen alustavat huomautukset, kertomukset, lausunnot, lehdistötiedotteet ja muut tuotteet, sen verkkosivusto ja intranet, puheenvuorot, vastaukset asiakirjapyyntöihin[3] ja ääni- tai kuvatallenteet eivät saa sisältää EU:n turvallisuusluokiteltuja tietoja eikä niissä saa viitata kyseisiin tietoihin tai niistä poimittuihin otteisiin. Jos luovuttaja kuitenkin on julkaissut asiakirjoja tai tietoja, joissa viitataan EU:n turvallisuusluokiteltuihin tietoihin, kyseinen viittaus voidaan mainita.

[3] Tilintarkastustuomioistuimen asiakirjojen julkisesta saatavuudesta tehdyn tilintarkastustuomioistuimen päätöksen 12-2005, sellaisena kuin se on muutettuna päätöksellä 14-2009 (EUVL C 67, 20.3.2009, s. 1), mukaisesti.

6) Sen estämättä, mitä 5 kohdassa säädetään, tilintarkastustuomioistuin ja luovuttaja voivat sopia, että tilintarkastustuomioistuin voi jonkin yksittäisen tarkastuksen osalta jäljentää tai käyttää EU:n turvallisuusluokiteltuja tietoja asiakirjassa. Tällaisessa tapauksessa asianomainen tilintarkastustuomioistuimen asiakirja on ensin toimitettava kyseessä olevien EU:n turvallisuusluokiteltujen tietojen luovuttajalle ennen kuulemismenettelyä tai sen aikana. Tässä tilanteessa tilintarkastustuomioistuimen ja luovuttajan on sovittava siitä, annetaanko tilintarkastustuomioistuimen laatimalle asiakirjalle turvallisuusluokitus. Jos raportoiva tilintarkastustuomioistuimen jäsen katsoo välttämättömäksi välittää kokonaan tai osittain turvallisuusluokitellun tarkastuskertomuksen tietyille vastaanottajille Euroopan parlamentissa tai neuvostossa – kaikki tähän päätökseen liittyvät turvatoimet huomioon ottaen – siihen on saatava turvallisuusluokiteltujen tietojen luovuttajan suostumus. Tällaisten asiakirjojen vaihtamisen oikeudellisesta kehyksestä ja menettelystä säädetään 7 artiklassa.

7) Jos tilintarkastustuomioistuimen toimeksiannon täyttäminen edellyttää turvallisuusluokitellun asiakirjan tai turvallisuusluokiteltujen tietojen tiettyjen osien jakamista laajemmin ja jos tilintarkastustuomioistuin katsoo, että jakamiseen on yleiseen etuun liittyvä pakottava syy, sen on ennen kyseisten osien tai tietojen käyttöä koskevan päätöksen tekemistä kuultava luovuttajaa ja otettava tässä yhteydessä turvallisuusluokitusmerkintä asianmukaisesti huomioon. Tietoja on käytettävä kertomuksessa niin, että luovuttajan etuja ei voida vahingoittaa. Tästä voidaan huolehtia asianmukaisesti pyytämällä luovuttajaa esittämään huomautuksia, jotta saadaan aikaan yhteisymmärrys siitä, miten tietoja voidaan anonymisoida, tiivistää tai yleistää jne. ja samalla kunnioittaa niiden etuja, joita julkaistut tiedot ensisijaisesti koskevat.

8) Tilintarkastustuomioistuin ei saa antaa EU:n turvallisuusluokiteltuja tietoja toiselle EU:n toimielimelle, virastolle, elimelle tai laitokselle, jäsenvaltiolle, kolmannelle valtiolle tai kansainväliselle järjestölle kuulematta luovuttajaa etukäteen ja ilman tämän nimenomaista kirjallista suostumusta.

9) Jos SECRET UE/EU SECRET -luokkaan tai sitä alempaan turvallisuusluokkaan kuuluvan asiakirjan luovuttaja ei ole määrännyt rajoituksia asiakirjan jäljentämiselle tai kääntämiselle, se voidaan haltijan pyynnöstä jäljentää tai kääntää tilintarkastustuomioistuimessa käytännön työtä koskevia tietoturvaviranomaisen ohjeita noudattaen. Myös jäljennöksiin ja käännöksiin on sovellettava alkuperäistä asiakirjaa koskevia turvatoimia.

10) Jos turvallisuusluokiteltujen asiakirjojen, jotka tilintarkastustuomioistuin on ottanut vastaan tai joiden saamiseen sillä on oikeus, turvallisuusluokkaa on alennettava tai se on poistettava, tilintarkastustuomioistuimen on kuultava luovuttajaa ja kysyttävä, voiko luovuttaja toimittaa asiakirjasta version, jonka turvallisuusluokkaa on alennettu tai jonka turvallisuusluokka on poistettu.

4 artikla. Henkilöturvallisuus

1) Tilintarkastustuomioistuimen jäsenillä on tehtäviensä vuoksi valtuutus päästä EU:n turvallisuusluokiteltuihin tietoihin ja osallistua kokouksiin, joissa EU:n turvallisuusluokiteltuja tietoja käsitellään. Jäsenille on ilmoitettava heidän EU:n turvallisuusluokiteltujen tietojen suojaamista koskevista turvallisuuteen liittyvistä velvollisuuksista, ja heidän on vahvistettava kyseisten tietojen suojaamista koskeva vastuunsa kirjallisesti.

2) Riippumatta siitä, onko tilintarkastustuomioistuimen henkilöstön jäsen virkamies, muuhun henkilöstöön sovellettavien palvelussuhteen ehtojen piiriin kuuluva henkilöstön jäsen vai kansallinen asiantuntija, hänelle myönnetään pääsy EU:n turvallisuusluokiteltuihin tietoihin vasta sen jälkeen, kun

i. hänen tiedonsaantitarpeensa on todennettu;

ii. hänelle on selvitetty EU:n turvallisuusluokiteltujen tietojen suojaamista koskevat turvallisuussäännöt sekä asiaankuuluvat turvallisuusvaatimukset ja -ohjeet ja hän on vahvistanut tällaisten tietojen suojaamista koskevan vastuunsa kirjallisesti;

iii. hänelle on tehty turvallisuusselvitys ja hänellä on valtuutus CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeamman tason tietoihin pääsyä varten.

3) Menettelystä, jossa määritetään, voidaanko virkamies tai muu tilintarkastustuomioistuimen henkilöstön jäsen valtuuttaa pääsemään CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeamman tason tietoihin, säädetään 10 artiklan 10 kohdan mukaisesti tehtävässä delegoidussa päätöksessä. Menettely edellyttää 2 artiklan n alakohdassa tarkoitetuilta jäsenvaltion toimivaltaisilta viranomaisilta saatua lausuntoa, ja siinä otetaan huomion henkilön lojaalius, rehellisyys ja luotettavuus. Päätökset pääsyn myöntämisestä tekee tilintarkastustuomioistuimen henkilöstöhallinnon, taloushallinnon ja yleispalvelujen osaston johtaja.

4) Tilintarkastustuomioistuimen henkilöstöhallinnon, taloushallinnon ja yleispalvelujen osaston johtaja voi antaa henkilöturvallisuusselvitykseen perustuvia todistuksia, joissa eritellään turvallisuusluokat, joihin kuuluviin EU:n turvallisuusluokiteltuihin tietoihin (CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeampi taso) henkilöille voidaan myöntää pääsy, vastaavan pääsyä koskevan valtuutuksen voimassaoloaika ja henkilöturvallisuusselvitykseen perustuvan todistuksen päättymispäivä.

5) Kokouksiin, joissa käsitellään CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeammalle tasolle luokiteltuja tietoja, voivat osallistua vain henkilöt, joilla on edellä 2 kohdan iii alakohdassa tarkoitettu valtuutus, ja tilintarkastustuomioistuimen jäsenet edellä 1 kohdassa säädetyn mukaisesti. Tilintarkastustuomioistuin ja luovuttaja sopivat tapauskohtaisesti kyseisten kokousten käytännön järjestelyistä.

6) Kokousten, joissa on määrä käsitellä CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeamman tason tietoja, järjestämisestä vastaavien tilintarkastustuomioistuimen osastojen on ilmoitettava tietoturvaviranomaiselle hyvissä ajoin kokouspäivät, -ajat ja -paikat sekä osallistujaluettelo.

7) Kaikkien henkilöiden, joilla on hallussaan EU:n turvallisuusluokiteltuja tietoja ilman asianmukaista valtuutusta ja/tai joilla ei ole todistettua tiedonsaantitarvetta, on ilmoitettava tilanteesta tietoturvaviranomaiselle mahdollisimman pian ja varmistettava, että EU:n turvallisuusluokitellut tiedot on suojattu tämän päätöksen vaatimusten mukaisesti.

5 artikla. Turvallisuusluokiteltujen tietojen suojaamiseen tarkoitetut fyysiset turvatoimet

1) ’Fyysisellä turvallisuudella’ tarkoitetaan fyysisten ja teknisten suojatoimien toteuttamista niin, että estetään luvaton pääsy EU:n turvallisuusluokiteltuihin tietoihin.

2) Fyysisten turvatoimien tarkoituksena on estää tunkeutuminen salaa tai väkisin, ehkäistä, estää ja havaita luvattomat toimet ja mahdollistaa henkilöstön jaottelu EU:n turvallisuusluokiteltuihin tietoihin pääsyä varten heidän tiedonsaantitarpeensa perusteella. Tällaisista toimista päätetään riskinhallintamenettelyn perusteella tämän päätöksen mukaisesti.

3) Tilintarkastustuomioistuimen tietoturvaviranomaisen on tarkastettava säännöllisin väliajoin alueet, joissa käsitellään tai säilytetään EU:n turvallisuusluokiteltuja tietoja.

4) EU:n turvallisuusluokiteltujen tietojen käsittelemiseen ja säilyttämiseen saa käyttää vain EU:n toimielimissä, virastoissa tai elimissä sovellettavien sääntöjen mukaisia välineitä ja laitteita.

5) Tilintarkastustuomioistuimen henkilöstö voi päästä CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeamman tason EU:n turvallisuusluokiteltuihin tietoihin tai vastaaviin tietoihin tilintarkastustuomioistuimen tilojen ulkopuolisilla turva-alueilla.

6) Tilintarkastustuomioistuin voi tehdä palvelutasosopimuksen toisen Luxemburgissa sijaitsevan EU:n toimielimen kanssa voidakseen käsitellä ja säilyttää CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeamman tason tietoja kyseisen toimielimen turva-alueella. Ellei luovuttajan kanssa ole nimenomaisesti sovittu, EU:n turvallisuusluokiteltuja tietoja ei saa käsitellä tai säilyttää tilintarkastustuomioistuimen tiloissa eikä tilintarkastustuomioistuin saa jäljentää tai kääntää niitä.

7) Tilintarkastustuomioistuin rekisteröi saapuneet RESTREINT UE/EU RESTRICTED -tason tiedot. CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeamman tason tietoihin tai vastaaviin tietoihin tutustuminen tilintarkastustuomioistuimen tilojen ulkopuolella rekisteröidään turvallisuussyistä.

8) RESTREINT UE/EU RESTRICTED -tason EU:n turvallisuusluokitellut tiedot voidaan säilyttää soveltuvissa lukituissa toimistokalusteissa hallinnollisella alueella tai turva-alueella. CONFIDENTIEL UE/EU CONFIDENTIAL tai SECRET UE/EU SECRET -tason EU:n turvallisuusluokiteltuja tietoja säilytetään palvelutasosopimuksen mukaisesti toisen Luxemburgissa sijaitsevan EU:n toimielimen turva-alueella turvakaapissa.

9) Rekisterin ulkopuolella EU:n turvallisuusluokiteltuja tietoja siirretään osastojen ja tilojen välillä seuraavasti:

   a) yleisenä sääntönä on, että EU:n turvallisuusluokitellut tiedot on siirrettävä sähköisesti välineillä, jotka on suojattu 6 artiklan 8 kohdan mukaisesti hyväksytyillä salaustuotteilla;

   b) jos EU:n turvallisuusluokiteltuja tietoja ei siirretä a alakohdassa kuvatulla tavalla, ne on siirrettävä tiedonsiirtovälineellä (esim. USB-muistitikulla, CD-levyllä, kovalevyllä), joka on suojattu 6 artiklan 8 kohdan mukaisesti hyväksytyillä salaustuotteilla tai paperilla läpinäkymättömässä sinetöidyssä kirjekuoressa.

10) Haltija voi hävittää RESTREINT UE/EU RESTRICED -tason tiedot, jollei tilintarkastustuomioistuimessa sovellettavista arkistointisäännöistä muuta johdu. CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeammalle tasolle luokitellut tiedot voi hävittää vain rekisterin valvontavastaava, kun haltija tai toimivaltainen viranomainen antaa siihen ohjeet tilintarkastustuomioistuimessa sovellettavien arkistointisääntöjen mukaisesti. SECRET UE/EU SECRET -tasolle luokitellut asiakirjat on hävitettävä sellaisen todistajan läsnä ollessa, jolla on vähintään hävitettävän asiakirjan turvaluokkaa vastaava turvallisuusselvitys. Rekisterin valvontavastaava ja todistaja, kun sellaisen on oltava läsnä, allekirjoittavat hävittämisestä tositteen, joka tallennetaan rekisteriin. Rekisterin valvontavastaava säilyttää CONFIDENTIEL UE/EU CONFIDENTIAL- ja SECRET UE/EU SECRET -tason asiakirjojen hävittämistä koskevaa rekisteriä vähintään viisi vuotta.

11) Fyysisestä turvallisuudesta vastaava viranomainen ja tietoturvaviranomainen laativat yhteisen suunnitelman EU:n turvallisuusluokiteltujen tietojen suojaamisesta kriisiaikoina sekä tarvittaessa suunnitelmat niiden hävittämisestä tai evakuoimisesta hätätapauksessa ja ottavat tässä yhteydessä huomioon paikalliset olosuhteet. Ne antavat ohjeet, joita ne pitävät tarpeellisina EU:n turvallisuusluokiteltujen tietojen sivullisille joutumisen estämiseksi.

12) Jos EU:n turvallisuusluokiteltuja tietoja on kuljetettava fyysisesti, tilintarkastustuomioistuimen on noudatettava luovuttajan määräämiä toimenpiteitä, joilla tietoja voidaan suojella luvattomalta paljastamiselta kuljetuksen aikana.

13) Liitteessä esitetään fyysiset turvatoimet, joita sovelletaan hallinnollisilla alueilla, joilla RESTREINT UE/EU RESTRICTED -tason tietoja käsitellään ja säilytetään.

6 artikla. EU:n turvallisuusluokiteltujen tietojen suojaaminen viestintä- ja tietojärjestelmissä

1) Tässä artiklassa ’viestintä- ja tietojärjestelmällä’ tarkoitetaan kaikkia järjestelmiä, joilla EU:n turvallisuusluokiteltuja tietoja voidaan käsitellä sähköisesti. Viestintä- ja tietojärjestelmä käsittää kaikki sen toiminnan kannalta tarpeelliset resurssit, myös infrastruktuurin, organisaation, henkilöstön ja tietoresurssit.

2) ’Oikeutetulla käyttäjällä’ tarkoitetaan tilintarkastustuomioistuimen jäsentä, virkamiestä, toimihenkilöä tai kansallista asiantuntijaa, jolla on todennettu ja hyväksytty tarve päästä tiettyyn tietojärjestelmään.

3) Tilintarkastustuomioistuin antaa varmuuden siitä, että sen järjestelmät suojaavat niissä käsiteltävät tiedot asianmukaisella tasolla ja toimivat oikeutettujen käyttäjien valvonnassa siten kuin ja silloin kun niiden kuuluu toimia. Tätä varten niissä taataan seuraavien osatekijöiden asianmukainen taso:

- aitous: tae siitä, että tiedot ovat aitoja ja peräisin vilpittömässä mielessä toimivista lähteistä;
- käytettävyys: tiedot ovat valtuutetun yksikön pyynnöstä saatavilla ja käytettävissä;
- luottamuksellisuus: tiedot eivät tule ilmi sivullisille henkilöille, yksiköille eikä prosesseille;
- eheys: omaisuuden ja tietojen oikeellisuus ja täydellisyys turvataan;
- kiistattomuus: tietty toimi tai tapahtuma voidaan todistaa tapahtuneeksi niin, ettei sitä voida myöhemmin kiistää.

Tämän varmuuden on perustuttava riskinhallintaprosessiin. ’Riskillä’ tarkoitetaan mahdollisuutta, että tietty uhka hyötyy organisaation tai minkä tahansa sen käyttämän järjestelmän sisäisestä ja ulkoisesta haavoittuvuudesta ja aiheuttaa siten vahinkoa organisaatiolle ja sen aineelliselle tai aineettomalle omaisuudelle. Riskin mittana on uhkien toteutumisen todennäköisyys yhdistettynä niiden vaikutuksiin. Riskinhallintaprosessi käsittää seuraavat vaiheet: uhkien ja haavoittuvuuksien tunnistaminen, riskinarviointi, riskin käsittely, riskin hyväksyntä ja riskiviestintä.

- ’Riskinarvioinnilla’ tarkoitetaan uhkien ja haavoittuvuuksien tunnistamista ja niihin liittyvän riskianalyysin suorittamista eli todennäköisyyden ja vaikutusten arviointia.
- ’Riskin käsittely’ on riskin lieventämistä, poistamista, vähentämistä (teknisiä, fyysisiä, organisatorisia tai menettelyyn liittyviä toimenpiteitä tarkoituksenmukaisesti yhdistämällä), siirtämistä ja seuraamista.
- ’Riskin hyväksyntä’ on päätös hyväksyä jäännösriskin olemassaolo riskin käsittelyn jälkeen.
- ’Jäännösriskillä’ tarkoitetaan riskiä, joka jää jäljelle, kun turvatoimet on toteutettu, ottaen huomioon, että kaikkia uhkia ei voida torjua eikä kaikkia haavoittuvuuksia poistaa.
- ’Riskiviestintä’ on viestintä- ja tietojärjestelmien käyttäjäyhteisöjen riskitietoisuuden lisäämistä sekä riskeistä tiedottamista hyväksyntäviranomaisille ja niistä raportoimista toiminnasta vastaaville viranomaisille.

4) Kaikkien EU:n turvallisuusluokiteltujen tietojen käsittelemiseen käytettävien elektronisten laitteiden ja välineiden on täytettävä EU:n turvallisuusluokiteltujen tietojen suojaamiseen sovellettavat säännöt. Etusija on annettava elektronisille laitteille ja välineille, jotka toinen

EU:n toimielin, virasto tai elin on jo hyväksynyt. Laitteiden koko elinkaaren aikainen turvallisuus on taattava.

5) Asianmukaisen viranomaisen on hyväksyttävä tilintarkastustuomioistuimen viestintä- ja tietojärjestelmä. Tätä varten tilintarkastustuomioistuin pyrkii tekemään palvelutasosopimuksen jonkin sellaisen EU:n toimielimen turvallisuusjärjestelyjen hyväksyntäviranomaisen kanssa, jolla on valmiudet hyväksyä EU:n turvallisuusluokiteltujen tietojen käsittely viestintä- ja tietojärjestelmissä, jotta voidaan saada hyväksymislausunto RESTREINT UE/EU RESTRICTED -tason tiedoille, joita voidaan käsitellä tilintarkastustuomioistuimen viestintä- ja tietojärjestelmässä, ja vastaaville käyttöehdoille. Palvelutasosopimuksessa on myös viitattava hyväksyntämenettelyssä sovellettaviin vaatimuksiin, ja se on tehtävä 10 artiklan 3 kohdassa säädetyn menettelyn mukaisesti.

6) Jos tilintarkastustuomioistuimen on vahvistettava viestintä- ja tietojärjestelmälleen oma hyväksyntämenettelynsä, menettely vahvistetaan tämän päätöksen 10 artiklan 10 kohdassa tarkoitetussa delegoidussa päätöksessä noudattaen vaatimuksia, joita toisissa EU:n toimielimissä, virastoissa ja elimissä sovelletaan viestintä- ja tietojärjestelmissä tapahtuvaa EU:n turvallisuusluokiteltujen tietojen käsittelyä koskevaan hyväksyntämenettelyyn.

7) Vastuu hyväksyntäasiakirjojen laatimisesta sovellettavien vaatimusten mukaisesti on yksin viestintä- ja tietojärjestelmän vastaavalla.

8) Jos EU:n turvallisuusluokitellut tiedot suojataan salaustuotteilla, tilintarkastustuomioistuimen on annettava etusija tuotteille, jotka neuvosto tai sen pääsihteeri on hyväksynyt neuvoston salauslaitteiden hyväksyntäviranomaisena, tai tuotteille, jotka on hyväksytty EU:n turvallisuusluokiteltujen tietojen suojaamiseen muissa EU:n toimielimissä, virastoissa ja elimissä.

9) RESTREINT UE/EU RESTRICTED -tason tietoja saa käsitellä vain hallinnollisella alueella tai turva-alueella sijaitsevilla elektronisilla laitteilla (kuten työasemilla, tulostimilla tai kopiokoneilla). RESTREINT UE/EU RESTRICTED -tason tietoja käsittelevät elektroniset laitteet on erotettava muista tietokoneverkoista ja suojattava asianmukaisilla fyysisillä tai teknisillä toimilla.

10) Kaikkien tilintarkastustuomioistuimen henkilöstöön kuuluvien, jotka osallistuvat EU:n turvallisuusluokiteltuja tietoja käsittelevien viestintä- ja tietojärjestelmien suunnitteluun, kehittämiseen, testaukseen, toimintaan, hallinnointiin tai käyttöön, on ilmoitettava tietoturvavastaavalle kaikista mahdollisista turvallisuuspuutteista, vaaratilanteista, tietoturvaloukkauksista ja tietojen vaarantumisista, jotka voivat vaikuttaa viestintä- ja tietojärjestelmän ja/tai sen sisältämien EU:n turvallisuusluokiteltujen tietojen suojaamiseen.

7 artikla. **Menettely turvallisuusluokiteltujen tietojen vaihtamista ja niihin pääsyä varten**

1) EU:n toimielimet, virastot, elimet ja laitokset ja kansalliset viranomaiset antavat omasta aloitteestaan tai presidentin, raportoivien jäsenten tai pääsihteerin kirjallisesta pyynnöstä tilintarkastustuomioistuimelle pääsyn EU:n turvallisuusluokiteltuihin tietoihin seuraavan menettelyn mukaisesti, kun niillä on siihen lakisääteinen velvoite perussopimusten tai perussopimusten perusteella annettujen säädösten nojalla.

2) Tietoihin pääsyä koskevat pyynnöt on lähetettävä kyseessä oleville toimielimille tilintarkastustuomioistuimen rekisteritoimiston kautta.

3) Tilintarkastustuomioistuimen on tarvittaessa sovittava hallinnollisesta järjestelystä, joka koskee EU:n turvallisuusluokiteltujen tietojen tai vastaavien tietojen vaihtamista koskevia käytännön seikkoja.

4) Tilintarkastustuomioistuin antaa tällaisista hallinnollisista järjestelyistä sopimista varten luovuttajalle tietoturvajärjestelmästään kaikki tarvittavat tiedot. Tarvittaessa voidaan järjestää arviointikäynti.

5) Näistä hallinnollisista järjestelyistä on sovittava täysin Euroopan unionista tehdyn sopimuksen 13 artiklassa säädettyjen annetun toimivallan ja vilpittömän yhteistyön periaatteiden mukaisesti. Niistä sovitaan 10 artiklan 4 kohdassa tarkoitettua menettelyä noudattaen.

6) Jos tietyn EU:n toimielimen, elimen tai viraston taikka kolmannen valtion tai kansainvälisen järjestön kanssa ei ole hallinnollista järjestelyä turvallisuusluokiteltujen tietojen antamisesta tilintarkastustuomioistuimelle, tilintarkastustuomioistuimen on annettava lausunto siitä, että sen saamien turvallisuusluokiteltujen tietojen suojaamisesta huolehditaan.

8 artikla. Turvallisuusluokiteltujen tietojen tietoturvaloukkaukset, häviäminen tai vaarantuminen

1) Tietoturvaloukkaus tapahtuu, kun henkilö rikkoo tai laiminlyö tässä päätöksessä ja sen soveltamissäännöissä vahvistettuja turvallisuussääntöjä.

2) EU:n turvallisuusluokitellut tiedot vaarantuvat, kun ne ovat tietoturvaloukkauksen seurauksena paljastuneet kokonaan tai osittain sivullisille.

3) Tapahtuneesta tai epäillystä tietoturvaloukkauksesta on ilmoitettava välittömästi tilintarkastustuomioistuimen tietoturvaviranomaiselle.

4) Jos EU:n turvallisuusluokiteltujen tietojen tiedetään tai voidaan perustellusti olettaa vaarantuneen tai hävinneen, tietoturvaviranomaisen on ilmoitettava tilintarkastustuomioistuimen henkilöstöhallinnon, taloushallinnon ja yleispalvelujen osaston johtajalle ja pääsihteerille. Henkilöstöhallinnon, taloushallinnon ja yleispalvelujen osaston johtajan on välittömästi ilmoitettava tästä asiaankuuluvalle luovuttajan tietoturvaviranomaiselle. Edellä mainittu tilintarkastustuomioistuimen johtaja tekee selvityksen ja ilmoittaa tilintarkastustuomioistuimen pääsihteerille ja luovuttajan tietoturvaviranomaiselle tuloksista ja toimista, joita tilanteen toistumisen estämiseksi on toteutettu. Jos kyse on tilintarkastustuomioistuimen jäsenestä, tilintarkastustuomioistuimen presidentti on vastuussa toimien toteuttamisesta yhteistyössä tilintarkastustuomioistuimen pääsihteerin kanssa.

5) Tässä päätöksessä ja sen soveltamissäännöissä säädettyjen turvallisuussääntöjen rikkomisesta vastuussa olevaan tilintarkastustuomioistuimen virkamieheen tai toimihenkilöön sovelletaan henkilöstösäännöissä ja muuhun henkilöstöön sovellettavissa palvelussuhteen ehdoissa esitettyjä seuraamuksia.

6) Kaikkiin tilintarkastustuomioistuimen jäseniin, jotka eivät noudata tämän päätöksen ehtoja, sovelletaan perussopimuksen 286 artiklan 6 kohdassa tarkoitettuja toimenpiteitä ja seuraamuksia.

7) Henkilöön, joka on aiheuttanut EU:n turvallisuusluokiteltujen tietojen häviämisen tai vaarantumisen, voidaan soveltaa kurinpidollisia ja/tai oikeudellisia seuraamuksia asiassa sovellettavien lakien, sääntöjen ja asetusten mukaisesti.

9 artikla. Turvallisuus ulkoisen intervention yhteydessä

1) Tilintarkastustuomioistuin voi antaa sellaisten tehtävien suorittamisen, joihin liittyy pääsy EU:n turvallisuusluokiteltuihin tietoihin tai jotka edellyttävät sitä, jäsenvaltioon

rekisteröityneille toimeksisaajille niiden kanssa tehdyn sopimuksen nojalla. Näin voidaan tehdä erityisesti, kun on kyse viestintä- ja tietojärjestelmien ja tietokoneverkon ylläpidosta.

2) Ulkoisen intervention yhteydessä tilintarkastustuomioistuimen on toteutettava kaikki tämän artiklan 3 kohdassa tarkoitetut tarvittavat turvatoimet. Sen on muun muassa pyydettävä yhteisöturvallisuusselvitystä sen varmistamiseksi, että hakijat ja tarjoajat suojaavat EU:n turvallisuusluokiteltuja tietoja koko tarjouskilpailu- ja hankintamenettelyn ajan ja että toimeksisaajat ja alihankkijat suojaavat tietoja koko sopimuksen elinkaaren ajan. Hankintaviranomaisen on varmistettava, että sopimuksissa mainitaan tässä päätöksessä tarkoitetut turvallisuutta koskevat vähimmäisvaatimukset, jotta toimeksisaajat velvoitetaan noudattamaan niitä.

3) Turvallisuussääntöjen, hankintamenettelyjen ja sellaisia hankinta- ja alihankintasopimuksia koskevien mallien, jotka edellyttävät pääsyä EU:n turvallisuusluokiteltuihin tietoihin, hankintailmoitusten, sellaisia olosuhteita koskevien ohjeiden, joissa edellytetään yhteisö- ja henkilöturvallisuusselvitystä, ohjelman tai hankkeen turvallisuusohjeiden, turvallisuutta koskevien lisälausekkeiden samoin kuin vierailuja sekä EU:n turvallisuusluokiteltujen tietojen siirtoa ja kuljetusta kyseisten turvallisuusluokiteltujen hankinta- ja avustussopimusten nojalla koskevien sääntöjen on noudatettava Euroopan komission EU:n turvallisuusluokiteltujen tietojen suojaamista koskevista säännöistä 13. maaliskuuta 2015 antamassa päätöksessä (EU, Euratom) 2015/444 turvallisuusluokiteltuja sopimuksia varten vahvistamia sääntöjä ja malleja.

<u>10 artikla.</u> Päätöksen ja siihen liittyvien vastuiden täytäntöönpano

1) Tilintarkastustuomioistuimen osastot toteuttavat kaikki niiden vastuulle kuuluvat tarvittavat toimet sen varmistamiseksi, että EU:n tai minkä tahansa muiden turvallisuusluokiteltujen tietojen käsittelyssä tai säilytyksessä sovelletaan tätä päätöstä ja asiaankuuluvia soveltamissääntöjä.

2) Pääsihteeri on nimittävä viranomainen ja viranomainen, jolla on valtuudet tehdä kaikkia virkamiehiä ja toimihenkilöitä koskevia työsopimuksia. Pääsihteeri voi siirtää henkilöstöhallinnon, taloushallinnon ja yleispalvelujen osaston johtajalle vastuun valtuutuksen myöntämisestä virkamiehille ja toimihenkilöille CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeamman tason EU:n turvallisuusluokiteltuihin tietoihin pääsystä, pääsihteerille kuuluvan turvallisuusjärjestelyjen hyväksyntäviranomaisen tehtävän harjoittamisesta ja tilintarkastustuomioistuimen sihteeristön valvonnasta EU:n turvallisuusluokiteltujen tietojen käsittelyn osalta.

3) Pääsihteerillä on toimivalta tehdä palvelutasosopimuksia tilintarkastustuomioistuimen viestintä- ja tietolaitteiden ja -järjestelmien hyväksymisestä, turva-alueen käytöstä toisessa EU:n toimielimessä ja menettelystä, joka koskee pyyntöjä henkilöturvallisuusselvitysten tekemisestä EU:n turvallisuusluokiteltuihin tietoihin pääsemistä varten.

4) Henkilöstöhallinnon, taloushallinnon ja yleispalvelujen osaston johtajalla on toimivalta sopia EU:n toimielinten, virastojen ja muiden elinten kanssa hallinnollisista järjestelyistä niiden EU:n turvallisuusluokiteltujen tietojen vaihtamisesta, joita tilintarkastustuomioistuin tarvitsee toimeksiantonsa täyttämistä varten. Kyseinen johtaja voi myös sopia hallinnollisista järjestelyistä kolmansien valtioiden tai kansainvälisten järjestöjen kanssa minkä tahansa saatujen turvallisuusluokiteltujen tietojen suojaamisen osalta.

5) Henkilöstöhallinnon, taloushallinnon ja yleispalvelujen osaston johtajalla on valtuudet allekirjoittaa mikä tahansa EU:n turvallisuusluokiteltujen tietojen suojaamista koskeva lausunto, joka on annettava poikkeuksellisen tilapäisen luovutuksen yhteydessä.

6) Tilintarkastustuomioistuimen tietoturvavastaava toimii tietoturvaviranomaisena. Tietoturvavastaavalla ja henkilöillä, joille hän siirtää tehtävänsä kokonaan tai osittain, on oltava asianmukainen turvallisuusselvitys. Tietoturvaviranomainen hoitaa velvollisuutensa tiiviissä yhteistyössä henkilöstöhallinnon, taloushallinnon ja yleispalvelujen osaston, tietotekniikan, työympäristön ja innovoinnin osaston ja tarkastusten laatua valvovan komitean kanssa (ks. erityisesti 4, 6 ja 8 artikla). Tietoturvaviranomainen vastaa myös tietoturvaa koskevista koulutus- ja tiedotustapahtumista sekä määräaikaistarkastuksista, joissa tarkastetaan tämän päätöksen noudattaminen, myös silloin, kun kyse on ulkoisesta interventiosta, ja kaikista vaatimustenmukaisuuden varmistamiseksi toteutettavista toimenpiteistä.

7) Turvallisuuspäällikkö on vastuussa fyysisistä turvatoimista (erityisesti 5 artikla).

8) Tilintarkastustuomioistuimen sihteeristöön perustettava rekisteritoimisto on niiden RESTREINT UE/EU RESTRICTED -tasolle turvallisuusluokiteltujen tietojen saapumis- ja lähtöpaikka, joita tilintarkastustuomioistuin voi vaihtaa muiden EU:n toimielinten, virastojen ja elinten sekä jäsenvaltioiden kanssa. Se on saapumis- ja lähtöpaikka myös kolmansien valtioiden ja kansainvälisten järjestöjen vastaaville tiedoille. Rekisteritoimisto on järjestettävä delegoidun päätöksen mukaisesti. Rekisteritoimistolla on seuraavat päävastuualueet:

   a) RESTREINT UE/EU RESTRICTED -tasolle turvallisuusluokiteltujen tietojen saapumisen ja lähtemisen rekisteröinti;

   b) RESTREINT UE/EU RESTRICTED -tason EU:n turvallisuusluokiteltujen tietojen käsittelyn, säilyttämisen ja konsultoinnin rekisteröintiin tarkoitettujen erityisten hallinnollisten alueiden hallinta.

9) Rekisteri perustetaan toisen EU:n toimielimen turva-alueen käyttöä koskevan palvelutasosopimuksen nojalla. Tämä tilintarkastustuomioistuimen sihteeristön tilintarkastustuomioistuimen henkilöstöhallinnon, taloushallinnon ja yleispalvelujen osaston johtajan vastuulla järjestämä rekisteri on niiden CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeammalle tasolle turvallisuusluokiteltujen tietojen saapumis- ja lähtöpaikka, joita tilintarkastustuomioistuin voi vaihtaa muiden EU:n toimielinten, virastojen ja elinten sekä jäsenvaltioiden kanssa. Rekisteri on saapumis- ja lähtöpaikka myös kolmansien valtioiden ja kansainvälisten järjestöjen vastaaville tiedoille. Se on varustettava asianmukaisilla kassaholveilla ja muilla turvalaitteilla, jotka soveltuvat CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeammalle tasolle turvallisuusluokiteltujen tietojen suojaamiseen. Rekisteri on järjestettävä delegoidun päätöksen mukaisesti. Rekisterin valvontavastaavalla on oltava asianmukainen turvallisuusselvitys, ja sen keskeisiä vastuualueita ovat seuraavat:

   a) EU:n turvallisuusluokiteltujen tietojen rekisteröintiin, konsultointiin, säilyttämiseen, jäljentämiseen, kääntämiseen, siirtämiseen, lähettämiseen ja tarvittaessa hävittämiseen liittyvien toimintojen hallinta;

   b) muut EU:n turvallisuusluokiteltujen tietojen suojaamiseen liittyvät, delegoidussa päätöksessä määritellyt tehtävät.

10) Hallintoasioiden komitea hyväksyy delegoidun päätöksen tämän päätöksen soveltamissäännöistä. Tietoturvavastaava laatii tietoturvaohjeet. Tarkastusten laatua valvova komitea laatii tarkastusohjeet.

<u>11 artikla.</u> **Voimaantulo**

Tämä päätös tulee voimaan seuraavana päivänä sen jälkeen, kun se on julkaistu Euroopan unionin virallisessa lehdessä.

Tehty Luxemburgissa 3. kesäkuuta 2021.

Tilintarkastustuomioistuimen

puolesta

Klaus-Heiner Lehne
presidentti

Liite: EU:N TURVALLISUUSLUOKITELTUJEN TIETOJEN HALLINNOLLISIA ALUEITA KOSKEVAT FYYSISET TURVATOIMET

LIITE

EU:N TURVALLISUUSLUOKITELTUJEN TIETOJEN HALLINNOLLISIA ALUEITA KOSKEVAT FYYSISET TURVATOIMET

1) Tässä liitteessä esitetään päätöksen 5 artiklan soveltamissäännökset. Ne ovat vähimmäissääntöjä RESTREINT UE/EU RESTRICTED -tason tietoja koskevien hallinnollisten alueiden fyysiselle suojaamiselle tilintarkastustuomioistuimessa. Hallinnolliset alueet ovat RESTREINT UE/EU RESTRICTED -tasolle turvallisuusluokiteltujen tietojen tallentamiseen, säilyttämiseen ja konsultointiin tarkoitettuja alueita.

2) Hallinnollisilla alueilla toteutettavien fyysisten turvatoimien tarkoituksena on estää luvaton pääsy näille alueille seuraavasti:

   a) alueella on oltava selvästi määritellyt näkyvät rajat, joilla henkilöt voidaan tarkastaa;

   b) vain tilintarkastustuomioistuimen tietoturvaviranomaisen tai muun toimivaltaisen viranomaisen asianmukaisesti valtuuttamilla henkilöillä on pääsy alueelle ilman saattajaa;

   c) kaikilla muilla henkilöillä on oltava aina saattaja tai heille on tehtävä vastaavat tarkastukset.

3) Tilintarkastustuomioistuimen tietoturvaviranomainen voi poikkeuksellisesti myöntää pääsyn sivullisille, myös työskentelyyn hallinnollisella alueella, mikäli siihen ei kuulu pääsyä EU:n turvallisuusluokiteltuihin tietoihin, jotka on pidettävä lukittuina muualle. Kyseiset henkilöt voivat tulla alueelle vain, jos heitä on jatkuvasti valvomassa tietoturvaviranomainen tai rekisterin valvontavastaava.

4) Tietoturvaviranomaisen on laadittava menettelyt kaikkien hallinnollisten alueiden ja turvallisuuskalusteiden avainten ja/tai numeroyhdistelmien hallinnointia varten. Näiden menettelyjen tarkoituksena on estää luvaton pääsy.

5) Numeroyhdistelmät on opeteltava ulkoa, ja ne annetaan mahdollisimman pienelle joukolle ihmisiä, joiden on tarpeen tietää ne. RESTREINT UE/EU RESTRICTED -tason tietojen säilyttämiseen käytettävien turvallisuuskalusteiden numeroyhdistelmät on vaihdettava

   - uuden turvallisuuskalusteenvastaanoton yhteydessä;
   - aina kun numeroyhdistelmän tuntevassa henkilöstössä tapahtuu muutos;
   - jos yhdistelmä on vaarantunut tai sen epäillään vaarantuneen;
   - jos jokin lukoista on huollettu tai korjattu;
   - vähintään 12 kuukauden välein.

6) Tietoturvaviranomainen ja turvallisuuspäällikkö ovat vastuussa näiden sääntöjen noudattamisesta.