EUROOPAN UNIONIN
NEUVOSTO

Bryssel, 1. heinäkuuta 2009 (26.08)
(OR. en)

11501/09
ADD 1

LIMITE

CSC 22

ILMOITUS

Lähettäjä:	Turvallisuuskomitea
Vastaanottaja:	Pysyvien edustajien komitea (Coreper II)
Asia:	Ehdotus neuvoston päätökseksi turvallisuussäännöistä EU:n turvaluokiteltujen tietojen suojaamiseksi

1. Turvallisuuskomiteassa on päästy laajaan yhteisymmärrykseen suuntaa-antavista keskusteluista, jotka koskevat oheista ehdotusta neuvoston päätökseksi turvallisuussäännöistä EU:n turvaluokiteltujen tietojen suojaamiseksi.

2. Jäljellä on vielä joitakin varaumia:

   – Viestintä- ja tietojärjestelmien hyväksyminen
     - liitteessä IV oleva 7 kohta; 46 kohta
     - liitteessä V oleva 36 kohta
     - Lisäys A: "hyväksymisen" määritelmä

   – Yhteisöturvallisuus
     - liitteessä V olevat 9 kohdan b kohta ja 16 kohta

   – Määritelmät
     - lisäys A: "riski", "turvallisuusriskien hallintaprosessi"

3. Turvallisuuskomitea tarkastelee näitä kysymyksiä ja tekee tekstiin lopullisen tarkistuksen seuraavassa kokouksessaan syyskuussa.

Ehdotus:

NEUVOSTON PÄÄTÖS,

tehty xx päivänä xx kuuta 2009,

turvallisuussäännöistä EU:n turvaluokiteltujen tietojen suojaamiseksi

(2009/xxx/EY)

EUROOPAN UNIONIN NEUVOSTO, joka

ottaa huomioon Euroopan yhteisön perustamissopimuksen ja erityisesti sen 207 artiklan 3 kohdan,

ottaa huomioon neuvoston työjärjestyksen vahvistamisesta 15 päivänä syyskuuta 2006 tehdyn neuvoston päätöksen 2006/683/EY, Euratom[1] ja erityisesti sen 24 artiklan,

sekä katsoo seuraavaa:

(1) Neuvoston toimintojen kehittämiseksi kaikilla turvaluokiteltujen tietojen käsittelyä edellyttävillä aloilla on asianmukaista perustaa turvaluokiteltujen tietojen suojaamiseksi kattava turvallisuusjärjestelmä, joka koskee neuvostoa, sen pääsihteeristöä ja jäsenvaltioita.

(2) Tämän päätöksen säännöksiä olisi sovellettava, kun neuvosto, sen valmistelevat elimet ja neuvoston pääsihteeristö käsittelevät EU:n turvaluokiteltuja tietoja.

(3) Jäsenvaltioiden olisi kansallisten lakiensa ja asetustensa mukaisesti ja neuvoston toiminnan edellyttämässä määrin noudatettava tämän päätöksen säännöksiä, kun niiden toimivaltaiset viranomaiset, henkilöstö tai hankeosapuolet käsittelevät EU:n turvaluokiteltuja tietoja, jotta kaikki osapuolet voivat olla vakuuttuneita siitä, että EU:n turvaluokiteltujen tietojen suojaamisessa noudatetaan vastaavaa tasoa.

[1] EUVL L 285, 16.10.2006, s. 47. Päätös sellaisena kuin se on viimeksi muutettuna päätöksellä 2008/945/EY (EUVL L 337, 16.12.2008, s. 92).

(4) Neuvosto ja Euroopan komissio ovat sitoutuneet soveltamaan vastaavia turvallisuusvaatimuksia EU:n turvaluokiteltujen tietojen suojaamiseen.

(5) Neuvosto korostaa sitä, että Euroopan parlamentti ja EU:n muut toimielimet, virastot, elimet tai toimistot on tärkeää saada tarvittaessa mukaan noudattamaan turvaluokiteltujen tietojen suojaamista koskevia periaatteita, vaatimuksia ja sääntöjä, jotka ovat välttämättömiä Euroopan unionin ja jäsenvaltioiden etujen suojaamiseksi.

(6) Euroopan unionista tehdyn sopimuksen V tai VI osaston nojalla perustetut EU:n virastot ja elimet soveltavat omassa organisaatiossaan tässä päätöksessä säädettyjä perusperiaatteita ja vähimmäisvaatimuksia EU:n turvaluokiteltujen tietojen suojaamiseksi, siten kuin niiden perustamissäädöksissä säädetään.

(7) Euroopan unionista tehdyn sopimuksen V osaston nojalla perustetut kriisinhallintaoperaatiot ja niiden henkilöstö soveltavat turvallisuussääntöjä, jotka neuvosto on hyväksynyt EU:n turvaluokiteltujen tietojen suojaamiseksi.

(8) EU:n erityisedustajat ja heidän alaisuudessaan työskentelevät henkilöt soveltavat turvallisuussääntöjä, jotka neuvosto on hyväksynyt EU:n turvaluokiteltujen tietojen suojaamiseksi.

(9) Tämän päätöksen tekeminen ei rajoita Euroopan yhteisön perustamissopimuksen 255 ja 286 artiklan eikä niiden täytäntöönpanosäädösten soveltamista.

(10) Tämän päätöksen tekeminen ei rajoita jäsenvaltioiden olemassa olevien käytäntöjen soveltamista niiden ilmoittaessa kansallisille parlamenteilleen EU:n toimista,

ON PÄÄTTÄNYT SEURAAVAA:

1 artikla

Tarkoitus, soveltamisala ja määritelmät

1. Tällä päätöksellä säädetään EU:n turvaluokiteltujen tietojen suojaamista koskevista perusperiaatteista ja vähimmäisvaatimuksista.

2. Näitä perusperiaatteita ja vähimmäisvaatimuksia sovelletaan neuvostoon ja neuvoston pääsihteeristöön, jäljempänä 'pääsihteeristö', ja jäsenvaltioiden on noudatettava niitä kansallisten lakiensa ja asetustensa mukaisesti, jotta kaikki osapuolet voivat olla vakuuttuneita siitä, että EU:n turvaluokiteltujen tietojen suojaamisessa noudatetaan vastaavaa tasoa.

3. Tässä päätöksessä sovelletaan lisäyksessä A vahvistettuja määritelmiä.

2 artikla

EU:n turvaluokiteltujen tietojen määrittely, turvaluokat ja merkinnät

1. "EU:n turvaluokitelluilla tiedoilla" tarkoitetaan mitä tahansa tietoja tai aineistoja, joille on määritelty EU:n turvaluokka ja joiden luvaton ilmitulo saattaisi vaihtelevassa määrin vahingoittaa EU:n tai sen yhden tai useamman jäsenvaltion etuja.

2. EU:n turvaluokitellut tiedot jaetaan seuraaviin turvaluokkiin:

a) TRES SECRET UE/EU TOP SECRET tiedot ja aineistot, joiden luvaton ilmitulo saattaisi vahingoittaa poikkeuksellisen vakavasti Euroopan unionin tai yhden tai useamman jäsenvaltion olennaisia etuja.

b) SECRET UE/EU SECRET: tiedot ja aineistot, joiden luvaton ilmitulo saattaisi vahingoittaa vakavasti Euroopan unionin tai yhden tai useamman jäsenvaltion olennaisia etuja.

c) CONFIDENTIEL UE/EU CONFIDENTIAL: tiedot ja aineistot, joiden luvaton ilmitulo saattaisi vahingoittaa Euroopan unionin tai yhden tai useamman jäsenvaltion olennaisia etuja.

d) RESTREINT UE/EU RESTRICTED: tiedot ja aineistot, joiden luvattomasta ilmitulosta saattaisi olla haittaa Euroopan unionin tai yhden tai useamman jäsenvaltion eduille.

3. EU:n turvaluokiteltuihin tietoihin lisätään turvaluokitusmerkintä 2 kohdan mukaisesti. Niissä voi olla myös muita merkintöjä, jotka liittyvät toimialaan, jota tiedot koskevat, tai joilla ilmoitetaan luovuttaja, rajoitetaan jakelua, rajoitetaan käyttöä tai ilmoitetaan luovutettavuus.

3 artikla

Turvaluokittelun hallinnointi

1. Toimivaltaisten viranomaisten on varmistettava, että EU:n turvaluokitellut tiedot on asianmukaisesti turvaluokiteltu, että ne on selkeästi määritelty turvaluokitelluiksi tiedoiksi ja että niiden turvaluokka säilytetään vain niin kauan kuin se on tarpeen.

2. EU:n turvaluokiteltujen tietojen turvaluokkaa ei saa alentaa eikä poistaa eikä niissä olevia 2 artiklan 3 kohdassa tarkoitettuja merkintöjä saa muuttaa eikä poistaa ilman niiden luovuttajan kirjallista etukäteissuostumusta.

3. Neuvosto hyväksyy EU:n turvaluokiteltujen tietojen tuottamisessa noudatettavat turvallisuusperiaatteet, joihin sisältyy käytännön turvaluokitusopas.

4 artikla

Turvaluokiteltujen tietojen suojaaminen

1. EU:n turvaluokiteltujen tietojen suojaamisessa on noudatettava tämän päätöksen säännöksiä.

2. Minkä tahansa EU:n turvaluokitellun tiedon haltija on vastuussa sen suojaamisesta tämän päätöksen säännösten mukaisesti.

3. Jäsenvaltioiden tuodessa EU:n rakenteisiin tai verkostoihin turvaluokiteltuja tietoja, joissa on kansallinen turvaluokitusmerkintä, neuvosto ja pääsihteeristö noudattavat kyseisten tietojen suojaamisessa vastaavan tason EU:n turvaluokiteltuihin tietoihin sovellettavia vaatimuksia lisäyksessä B olevan turvaluokkien vastaavuustaulukon mukaisesti.

4. Jos EU:n turvaluokiteltuja tietoja on suuria määriä tai jos niitä kootaan, ne voivat edellyttää korkeampaan turvaluokkaan sovellettavaa suojaa.

5 artikla

Turvallisuusriskien hallinta

1. EU:n turvaluokiteltuihin tietoihin kohdistuvia riskejä on hallittava prosessina. Prosessissa on pyrittävä määrittelemään tunnetut turvallisuusriskit ja turvatoimet niiden vähentämiseksi hyväksyttävälle tasolle tässä päätöksessä säädettyjen perusperiaatteiden ja vähimmäisvaatimusten mukaisesti sekä soveltamaan kyseisiä turvatoimia syvyyssuuntaisen turvallisuuden käsitteen pohjalta. Turvatoimien tehokkuutta on arvioitava jatkuvasti.

2. Turvatoimet EU:n turvaluokiteltujen tietojen suojaamiseksi koko niiden elinkaaren ajan on suhteutettava erityisesti tietojen tai aineistojen turvaluokitukseen, muotoon ja määrään, EU:n turvaluokiteltujen tietojen sijoitustilojen sijaintiin ja rakentamiseen sekä paikallisesti arvioituun vihamielisen ja/tai rikollisen toiminnan uhkaan, vakoilu, sabotaasi ja terrorismi mukaan luettuina.

3. Varautumissuunnitelmissa on otettava huomioon tarve suojata EU:n turvaluokitellut tiedot hätätilanteissa, jotta estetään luvaton pääsy tietoihin, tietojen paljastuminen tai niiden eheyden tai käytettävyyden menettäminen.

4. Toiminnan jatkuvuussuunnitelmiin on sisällytettävä ennalta ehkäiseviä ja vaarantumistilanteen korjaamistoimenpiteitä, jotta minimoitaisiin merkittävien toimintahäiriöiden tai poikkeuksellisten tapahtumien vaikutukset EU:n turvaluokiteltujen tietojen käsittelyyn ja säilyttämiseen.

6 artikla

Tämän päätöksen säännösten täytäntöönpano

1. Neuvosto hyväksyy tarvittaessa turvallisuuskomitean suosituksesta turvallisuusperiaatteet, joissa esitetään toimenpiteet tämän päätöksen säännösten panemiseksi täytäntöön.

2. Turvallisuuskomitean tasolla voidaan hyväksyä turvallisuutta koskevia suuntaviivoja, joilla täydennetään tai tuetaan tämän päätöksen säännöksiä ja neuvoston mahdollisesti hyväksymiä turvallisuusperiaatteita.

7 artikla

Henkilöstöturvallisuus

1. Henkilöstöturvallisuudella tarkoitetaan toimenpiteitä sen varmistamiseksi, että pääsy EU:n turvaluokiteltuihin tietoihin myönnetään ainoastaan henkilöille

   – joilla on tiedonsaantitarve (need-to-know);

   – joille on tarvittaessa tehty asianmukaisen tason turvallisuusselvitys; ja

   – joille on tiedotettu heidän vastuustaan.

2. Henkilöturvallisuusselvitystä koskevien menettelyjen tarkoituksena on selvittää, voidaanko henkilölle myöntää pääsy EU:n turvaluokiteltuihin tietoihin, hänen lojaaliutensa, rehellisyytensä ja luotettavuutensa huomioon ottaen.

3. Kaikista pääsihteeristössä työskentelevistä henkilöistä, joilla on tehtäviensä suorittamiseksi oltava pääsy CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeamman tason EU:n turvaluokiteltuihin tietoihin, on tehtävä asianmukaisen tason turvallisuusselvitys ennen kuin heille myönnetään pääsy kyseisiin EU:n turvaluokiteltuihin tietoihin. Pääsihteeristön virkamiehiä ja muuta henkilöstöä koskeva henkilöturvallisuusselvitysmenettely esitetään liitteessä I.

4. Jäljempänä 14 artiklan 3 kohdassa tarkoitetusta jäsenvaltioiden henkilöstöstä, joiden tehtävien suorittaminen voi edellyttää pääsyä CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeamman tason EU:n turvaluokiteltuihin tietoihin, on tehtävä asianmukaisen tason turvallisuusselvitys tai heillä on oltava muu kansallisten lakien ja asetusten mukainen asianmukainen valtuutus tehtäviensä vuoksi ennen kuin heille myönnetään pääsy kyseisiin EU:n turvaluokiteltuihin tietoihin.

5. Kaikille henkilöille on selvitettävä heidän vastuunsa ja heidän on annettava vakuutus vastuustaan suojata EU:n turvaluokitellut tiedot tämän päätöksen mukaisesti ennen kuin heille myönnetään pääsy EU:n turvaluokiteltuihin tietoihin; tämä on uusittava säännöllisin väliajoin.

6. Tämän artiklan täytäntöönpanosäännökset vahvistetaan liitteessä I.

8 artikla

Fyysinen turvallisuus

1. Fyysisellä turvallisuudella tarkoitetaan fyysisten ja teknisten suojatoimenpiteiden toteuttamista niin, että estetään luvaton pääsy EU:n turvaluokiteltuihin tietoihin.

2. Fyysisten turvatoimien tarkoituksena on estää tunkeutuminen salaa tai väkisin, ehkäistä, estää ja havaita luvattomat toimet ja mahdollistaa henkilöstön luokitus ja pääsy EU:n turvaluokiteltuihin tietoihin sen perusteella, mikä heidän tiedonsaantitarpeensa on. Tällaiset toimet on määriteltävä riskinhallintaprosessin perusteella.

3. Fyysiset turvatoimet on toteutettava kaikissa tiloissa, rakennuksissa, toimistoissa, huoneissa ja muissa paikoissa, joissa EU:n turvaluokiteltuja tietoja käsitellään tai säilytetään, 10 artiklassa määritellyt viestintä- ja tietojärjestelmien sijoitusalueet mukaan luettuina.

4. Alueet, joilla säilytetään CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeamman tason EU:n turvaluokiteltuja tietoja, on määriteltävä turva-alueiksi liitteen II mukaisesti, ja toimivaltaisen turvallisuusviranomaisen on hyväksyttävä ne.

5. CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeamman tason EU:n turvaluokiteltujen tietojen suojaamiseen saa käyttää vain hyväksyttyjä välineitä tai laitteita.

6. Tämän artiklan täytäntöönpanosäännökset vahvistetaan liitteessä II.

9 artikla

Turvaluokiteltujen tietojen hallinnointi

1. Turvaluokiteltujen tietojen hallinnoinnilla tarkoitetaan hallinnollisten toimenpiteiden soveltamista EU:n turvaluokiteltujen tietojen valvomiseksi koko niiden elinkaaren ajan niin, että täydennetään 7, 8 ja 10 artiklassa säädettyjä toimenpiteitä ja siten autetaan estämään ja havaitsemaan tällaisten tietojen tahallinen tai tahaton vaarantuminen tai katoaminen sekä korjaamaan vaarantumistilanne. Tällaiset toimenpiteet liittyvät erityisesti EU:n turvaluokiteltujen tietojen tuottamiseen, kirjaamiseen, jäljentämiseen, kääntämiseen, kuljettamiseen ja hävittämiseen.

2. CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeamman turvaluokan tiedot on turvallisuussyistä kirjattava ennen niiden jakelua ja niiden vastaanottamisen yhteydessä. Pääsihteeristön ja jäsenvaltioiden toimivaltaisten viranomaisten on perustettava tätä varten kirjaamisjärjestelmä. TRES SECRET UE/EU TOP SECRET-turvaluokan tiedot on kirjattava niille tarkoitetuissa kirjaamoissa.

3. Toimivaltaisen turvallisuusviranomaisen on tarkastettava säännöllisin väliajoin yksiköt ja tilat, joissa käsitellään tai säilytetään EU:n turvaluokiteltuja tietoja.

4. EU:n turvaluokiteltujen tietojen siirtämisessä yksiköiden ja tilojen välillä fyysisesti suojattujen alueiden ulkopuolella on noudatettava seuraavaa:

   a) Yleisenä sääntönä on, että EU:n turvaluokitellut tiedot on siirrettävä sähköisillä välineillä, jotka on suojattu 10 artiklan 6 kohdan mukaisesti hyväksytyillä salaustuotteilla.

   b) Jos tällaisia välineitä ei käytetä, EU:n turvaluokitellut tiedot on kuljetettava

      i) joko 10 artiklan 6 kohdan mukaisesti hyväksytyillä salaustuotteilla suojatuilla sähköisillä välineillä (kuten USB-muistitikut, CD-levyt, kiintolevyt),

      ii) tai, kaikissa muissa tapauksissa, toimivaltaisen turvallisuusviranomaisen liitteessä III olevien asiaankuuluvien säännösten mukaisesti antamia ohjeita noudattaen.

5. Tämän artiklan täytäntöönpanosäännökset vahvistetaan liitteessä III.

10 artikla
Viestintä- ja tietojärjestelmissä käsiteltävien
EU:n turvaluokiteltujen tietojen suojaaminen

1. Tietojen turvaamisella tarkoitetaan viestintä- ja tietojärjestelmien alalla varmuutta siitä, että kyseiset järjestelmät suojaavat tiedot, joita niissä käsitellään, ja toimivat tarkoituksenmukaisella tavalla, oikeaan aikaan ja oikeutettujen käyttäjien valvonnassa. Tehokkaalla tietojen turvaamisella varmistetaan asianmukainen luottamuksellisuuden, eheyden, käytettävyyden, kiistämättömyyden ja aitouden taso. Tietojen turvaaminen perustuu riskinhallintaprosessiin.

2. Viestintä- ja tietojärjestelmällä tarkoitetaan järjestelmää, joka mahdollistaa tietojen käsittelyn sähköisessä muodossa. Viestintä- ja tietojärjestelmä käsittää kaikki toimintansa kannalta tarpeelliset resurssit, myös infrastruktuurin, organisaation, henkilöstön ja tietoresurssit. Tätä päätöstä sovelletaan edellä tarkoitettuihin järjestelmiin, joissa käsitellään EU:n turvaluokiteltuja tietoja.

3. Viestintä- ja tietojärjestelmissä on käsiteltävä EU:n turvaluokiteltuja tietoja tietojen turvaamisen periaatteen mukaisesti.

4. Kaikkien viestintä- ja tietojärjestelmien on läpikäytävä hyväksymisprosessi. Hyväksymisellä pyritään varmistamaan, että kaikki asiaankuuluvat turvatoimet on pantu täytäntöön ja että on saavutettu riittävä EU:n turvaluokiteltujen tietojen ja viestintä- ja tietojärjestelmän suojaustaso tämän päätöksen säännösten mukaisesti. Hyväksymislausunnossa on määriteltävä niiden tietojen korkein sallittu turvaluokka, joita viestintä- ja tietojärjestelmässä voidaan käsitellä, ja sitä koskevat ehdot ja edellytykset.

5. Viestintä- ja tietojärjestelmät, joissa käsitellään CONFIDENTIEL UE/EU CONFIDENTIAL- ja sitä korkeamman turvaluokan tietoja, on suojattava niin, etteivät tahattomat sähkömagneettiset vuodot vaaranna tietoja (TEMPEST-turvatoimet).

6. Jos EU:n turvaluokiteltujen tietojen suojaamiseen käytetään salaustuotteita, tällaiset tuotteet on hyväksyttävä seuraavasti:

   a) SECRET UE/EU SECRET- tai sitä korkeamman turvaluokan tietojen luottamuksellisuus on suojattava salaustuotteilla, jotka salauslaitteiden hyväksyntäviranomaisena toimiva neuvosto on hyväksynyt turvallisuuskomitean suosituksesta.

   b) CONFIDENTIEL UE/EU CONFIDENTIAL- tai RESTREINT UE/EU RESTRICTED -turvaluokan tietojen luottamuksellisuus on suojattava salaustuotteilla, jotka salauslaitteiden hyväksyntäviranomainen, YUTP:n korkeana edustajana toimiva neuvoston pääsihteeri, jäljempänä 'pääsihteeri', on hyväksynyt turvallisuuskomitean suosituksesta.

   Sen estämättä, mitä b alakohdassa säädetään, EU:n CONFIDENTIEL UE/EU CONFIDENTIAL- tai RESTREINT UE/EU RESTRICTED -turvaluokiteltujen tietojen luottamuksellisuus voidaan suojata jäsenvaltioiden kansallisissa järjestelmissä salaustuotteilla, jotka on hyväksynyt jäsenvaltion salauslaitteiden hyväksyntäviranomainen.

7. Lähetettäessä EU:n turvaluokiteltuja tietoja sähköisesti on käytettävä hyväksyttyjä salaustuotteita. Tästä vaatimuksesta poiketen poikkeuksellisissa olosuhteissa tai tiettyjen liitteessä IV säädettyjen teknisten määritysten osalta voidaan soveltaa erityisiä menettelyjä.

8. Pääsihteeristön ja jäsenvaltioiden toimivaltaisten viranomaisten on molempien perustettava seuraavat tiedonturvaamistehtävät:

   a) tiedonturvaamisviranomainen;

   b) TEMPEST-viranomainen;

   c) salauslaitteiden hyväksyntäviranomainen;

   d) salatun aineiston jakelusta vastaava viranomainen.

9. Pääsihteeristön ja jäsenvaltioiden toimivaltaisten viranomaisten on molempien perustettava kutakin järjestelmää varten

   a) turvallisuusjärjestelyt hyväksyvä viranomainen;

   b) operatiivinen tiedonturvaamisviranomainen.

10. Tämän artiklan täytäntöönpanosäännökset vahvistetaan liitteessä IV.

11 artikla

Yhteisöturvallisuus

1. Yhteisöturvallisuudella tarkoitetaan toimenpiteiden toteuttamista sen varmistamiseksi, että hankeosapuolet tai alihankkijat varmistavat EU:n turvaluokiteltujen tietojen suojaamisen sopimusta edeltävissä neuvotteluissa ja turvaluokiteltujen sopimusten koko elinkaaren ajan. Kyseisiin sopimuksiin ei saa kuulua pääsyä TRES SECRET UE/EU TOP SECRET -turvaluokan tietoihin.

2. Neuvoston pääsihteeristö voi antaa jäsenvaltioon tai sellaiseen kolmanteen valtioon, jonka kanssa EU on tehnyt tietoturvallisuussopimuksen, rekisteröidyille yrityksille tai muille yhteisöille sopimuksella toimeksiantoja, joihin sisältyy tai liittyy pääsy EU:n turvaluokiteltuihin tietoihin tai niiden käsittely tai säilyttäminen.

3. Pääsihteeristön on hankeviranomaisena varmistettava, että tässä päätöksessä säädettyjä ja sopimuksessa tarkoitettuja yhteisöturvallisuutta koskevia vähimmäisvaatimuksia noudatetaan tehtäessä turvaluokiteltuja sopimuksia yritysten tai muiden yhteisöjen kanssa.

4. Kunkin jäsenvaltion kansallisen turvallisuusviranomaisen, nimetyn turvallisuusviranomaisen tai muun toimivaltaisen viranomaisen on mahdollisuuksien mukaan kansallisten lakien ja asetusten mukaisesti varmistettava, että sen alueelle rekisteröidyt hankeosapuolet ja alihankkijat toteuttavat kaikki asianmukaiset toimenpiteet EU:n turvaluokiteltujen tietojen suojaamiseksi sopimusta edeltävien neuvottelujen aikana tai turvaluokitellun sopimuksen toimeenpanovaiheessa.

5. Kunkin jäsenvaltion kansallisen turvallisuusviranomaisen, nimetyn turvallisuusviranomaisen tai muun toimivaltaisen viranomaisen on kansallisten lakien ja asetusten mukaisesti varmistettava, että kyseiseen jäsenvaltioon rekisteröidyillä hankeosapuolilla tai alihankkijoilla, jotka ovat osapuolina turvaluokitelluissa sopimuksissa tai alihankintasopimuksissa, jotka edellyttävät CONFIDENTIEL UE/EU CONFIDENTIAL- tai SECRET UE/EU SECRET- turvaluokan tietojen saamista niiden toimitiloissa joko sopimusten toimeenpanovaiheessa tai sopimuksia edeltävien neuvottelujen aikana, on asiaankuuluvan turvaluokitustason yhteisöturvallisuusselvitys.

6. Asianomaisen kansallisen tai nimetyn turvallisuusviranomaisen tai muun toimivaltaisen turvallisuusviranomaisen on myönnettävä henkilöturvallisuusselvitys hankeosapuolen tai alihankkijan henkilöstölle, jolla on oltava pääsy CONFIDENTIEL UE/EU CONFIDENTIAL- tai SECRET UE/EU SECRET -turvaluokan tietoihin turvaluokitellun sopimuksen toimeenpanemiseksi, kansallisten lakien ja asetusten sekä tämän päätöksen liitteessä I säädettyjen vähimmäisvaatimusten mukaisesti.

7. Tämän artiklan täytäntöönpanosäännökset vahvistetaan liitteessä V.

12 artikla

Turvaluokiteltujen tietojen vaihto

kolmansien valtioiden ja kansainvälisten järjestöjen kanssa

1. Jos neuvosto toteaa, että jonkin kolmannen valtion tai kansainvälisen järjestön kanssa on tarpeen vaihtaa EU:n turvaluokiteltuja tietoja, tätä varten on perustettava asianmukaiset puitteet.

2. Tällaisten puitteiden perustamiseksi ja vaihdettavien turvaluokiteltujen tietojen suojaamista koskevien vastavuoroisten sääntöjen määrittelemiseksi

   a) neuvosto tekee sopimuksia turvaluokiteltujen tietojen vaihtoa ja suojaamista koskevista turvallisuusmenettelyistä, jäljempänä 'tietoturvallisuussopimukset'; tai

   b) pääsihteeri voi liitteessä VI olevan 17 kohdan mukaisesti sopia hallinnollisista järjestelyistä, jos luovutettavien EU:n turvaluokiteltujen tietojen turvaluokka on yleensä korkeintaan RESTREINT UE/EU RESTRICTED.

3. Edellä 2 kohdassa tarkoitettuihin tietoturvallisuussopimuksiin tai hallinnollisiin järjestelyihin on sisällytettävä määräyksiä, joilla varmistetaan, että kolmansien valtioiden tai kansainvälisten järjestöjen vastaanottaessa EU:n turvaluokiteltuja tietoja kyseiset tiedot suojataan niiden turvaluokan edellyttämällä tavalla ja vähintään yhtä tiukkojen vaatimusten mukaisesti kuin tässä päätöksessä vahvistetut vähimmäisvaatimukset.

4. Neuvosto tekee päätöksen neuvostosta peräisin olevien EU:n turvaluokiteltujen tietojen luovuttamisesta kolmannelle valtiolle tai kansainväliselle järjestölle tapauskohtaisesti kyseisten tietojen luonteen ja sisällön, vastaanottajan tiedonsaantitarpeen ja EU:lle koituvan edun arvioinnin perusteella. Jos luovutuspyynnön kohteena olevien turvaluokiteltujen tietojen luovuttaja ei ole neuvosto, pääsihteeristön on ensin saatava tietojen alkuperäisen luovuttajan kirjallinen suostumus luovutukselle. Jos luovuttajaa ei tiedetä, neuvosto ottaa luovuttajan vastuun itselleen.

5. Luovutettujen tai vaihdettujen EU:n turvaluokiteltujen tietojen suojaamiseksi kolmannessa valtiossa tai kansainvälisessä järjestössä toteutettujen turvatoimien tehokkuus on varmistettava järjestämällä arviointikäyntejä.

6. Tämän artiklan täytäntöönpanosäännökset vahvistetaan liitteessä VI.

13 artikla

Tietoturvaloukkaukset ja EU:n turvaluokiteltujen tietojen vaarantuminen

1. Tietoturvaloukkaus tapahtuu, kun henkilö ei noudata tässä päätöksessä säädettyjä turvallisuussääntöjä tai laiminlyö niitä.

2. EU:n turvaluokitellut tiedot vaarantuvat, kun ne ovat tietoturvaloukkauksen seurauksena paljastuneet kokonaisuudessaan tai osittain sivullisille henkilöille.

3. Tapahtuneesta tai epäillystä tietoturvaloukkauksesta on ilmoitettava välittömästi toimivaltaiselle turvallisuusviranomaiselle.

4. Jos EU:n turvaluokiteltujen tietojen tiedetään tai voidaan perustellusti olettaa vaarantuneen tai kadonneen, toimivaltaisen turvallisuusviranomaisen on toteutettava kaikki asiaankuuluvien lakien ja asetusten mukaiset tarpeelliset toimenpiteet

   – ilmoittaakseen tietojen luovuttajalle;

   – varmistaakseen, että henkilöstö, joka ei ole välittömästi tekemisissä tietoturvaloukkauksen kanssa, tutkii tapauksen tosiasioiden selvittämiseksi;

   – arvioidakseen EU:n tai jäsenvaltioiden eduille aiheutuneen mahdollisen vahingon;

   – toteuttaakseen tarvittavat toimenpiteet tapahtuneen toistumisen estämiseksi; ja

   – ilmoittaakseen asianmukaisille viranomaisille toteutetuista toimista.

5. Henkilölle, joka on vastuussa tässä päätöksessä säädettyjen turvallisuussääntöjen loukkauksesta, voidaan määrätä kurinpitoseuraamus asiaankuuluvien sääntöjen ja määräysten mukaisesti. Henkilöön, joka on aiheuttanut EU:n turvaluokiteltujen tietojen vaarantumisen, voidaan kohdistaa kurinpidollisia ja/tai oikeudellisia toimenpiteitä sovellettavien lakien, sääntöjen ja määräysten mukaisesti.

14 artikla

Täytäntöönpanovastuu

1. Neuvosto toteuttaa kaikki tarpeelliset toimenpiteet varmistaakseen tämän päätöksen johdonmukaisen soveltamisen.

2. Pääsihteeri toteuttaa kaikki tarpeelliset toimenpiteet sen varmistamiseksi, että käsiteltäessä tai säilytettäessä EU:n tai muita turvaluokiteltuja tietoja neuvoston käyttämissä tiloissa ja pääsihteeristössä, myös sen kolmansissa valtioissa sijaitsevissa yhteystoimistoissa, pääsihteeristön virkamiehet ja muu henkilöstö, pääsihteeristöön lähetetty henkilöstö ja pääsihteeristön hankeosapuolet soveltavat tämän päätöksen säännöksiä.

3. Jäsenvaltioiden on toteutettava kaikki asianmukaiset toimenpiteet kansallisten lakiensa ja asetustensa mukaisesti sen varmistamiseksi, että seuraavat henkilöt noudattavat tämän päätöksen säännöksiä käsitellessään tai säilyttäessään EU:n turvaluokiteltuja tietoja:

   a) jäsenvaltioiden Euroopan unionissa olevien pysyvien edustustojen henkilöstö sekä neuvoston tai sen valmistelevien elinten kokouksiin tai neuvoston muuhun toimintaan osallistuvat kansallisten valtuuskuntien jäsenet;

   b) muu jäsenvaltioiden kansallisen hallinnon henkilöstö, myös kyseisiin hallintoihin lähetetty henkilöstö, riippumatta siitä, ovatko henkilöt palveluksessa jäsenvaltioiden alueella vai ulkomailla;

   c) muut jäsenvaltioissa olevat henkilöt, joilla on tehtäviensä vuoksi asianmukainen valtuutus päästä EU:n turvaluokiteltuihin tietoihin; ja

   d) jäsenvaltioiden hankeosapuolet riippumatta siitä, ovatko ne jäsenvaltioiden alueella vai kolmansissa valtioissa.

15 artikla

Turvallisuusjärjestelyt neuvostossa

1. Osana tehtäväänsä varmistaa tämän päätöksen soveltamisen yleinen johdonmukaisuus neuvosto hyväksyy

   a) 12 artiklan 2 kohdan a alakohdassa tarkoitetut sopimukset;

   b) päätökset, joilla sallitaan EU:n turvaluokiteltujen tietojen luovuttaminen kolmansille valtioille ja kansainvälisille järjestöille;

   c) pääsihteerin ehdottaman ja turvallisuuskomitean suositteleman vuosittaisen tarkastusohjelman, jonka mukaan tarkastetaan jäsenvaltioiden ja EU:n virastojen ja elinten yksiköt ja tilat ja tehdään arviointikäyntejä kolmansiin valtioihin ja kansainvälisiin järjestöihin EU:n turvaluokiteltujen tietojen suojaamiseksi toteutettujen toimenpiteiden tehokkuuden varmistamiseksi; ja

   d) edellä 6 artiklan 1 kohdassa tarkoitetut turvallisuusperiaatteet.

2. Pääsihteeri toimii pääsihteeristön turvallisuusviranomaisena. Siinä ominaisuudessa hän

   a) panee täytäntöön neuvoston turvallisuusperiaatteet ja seuraa niiden toteutumista;

   b) koordinoi jäsenvaltioiden kansallisten turvallisuusviranomaisten kanssa kaikki turvallisuusasiat, jotka liittyvät neuvoston toiminnan kannalta merkityksellisten turvaluokiteltujen tietojen suojaamiseen;

   c) myöntää pääsihteeristön virkamiehille ja muulle henkilöstölle EU-turvallisuusselvitykset 7 artiklan 3 kohdan mukaisesti ennen kuin heille voidaan myöntää pääsy CONDIFENTIEL UE/EU CONFIDENTIAL- tai sitä korkeamman turvaluokan tietoihin;

d) määrää tarvittaessa tutkinnasta, joka koskee neuvoston hallussa olevien tai neuvostosta peräisin olevien EU:n turvaluokiteltujen tietojen todettua tai epäiltyä vaarantumista tai katoamista, ja pyytää asiaankuuluvia turvallisuusviranomaisia auttamaan tällaisessa tutkinnassa;

e) huolehtii turvaluokiteltujen tietojen suojaamiseksi toteutettujen turvallisuusjärjestelyjen määräaikaistarkastuksista pääsihteeristön tiloissa;

f) huolehtii EU:n turvaluokiteltujen tietojen suojaamiseksi toteutettujen turvallisuusjärjestelyjen määräaikaistarkastuksista EU:n virastoissa ja elimissä, Euroopan unionista tehdyn sopimuksen V osaston nojalla perustetuissa kriisinhallintaoperaatioissa sekä EU:n erityisedustajien ja heidän alaisuudessaan työskentelevien henkilöiden osalta;

g) huolehtii yhdessä ja keskinäisestä sopimuksesta asianomaisten kansallisten turvallisuusviranomaisten kanssa EU:n turvaluokiteltujen tietojen suojaamiseksi toteutettujen turvallisuusjärjestelyjen määräaikaistarkastuksista jäsenvaltioiden yksiköissä ja tiloissa;

h) koordinoi turvatoimet jäsenvaltioiden ja tarvittaessa kolmansien valtioiden tai kansainvälisten järjestöjen turvaluokiteltujen tietojen suojaamisen osalta toimivaltaisten viranomaisten kanssa, mukaan lukien EU:n turvaluokiteltuihin tietoihin kohdistuvien turvallisuusuhkien luonne ja keinot suojautua niitä vastaan;

i) sopii 12 artiklan 2 kohdan b alakohdassa tarkoitetuista hallinnollisista järjestelyistä; ja

j) järjestää alustavat ja määräaikaiset arviointikäynnit kolmansiin valtioihin tai kansainvälisiin järjestöihin sen varmistamiseksi, että niille luovutettujen tai niiden kanssa vaihdettujen EU:n turvaluokiteltujen tietojen suojaamiseksi on toteutettu tehokkaat toimenpiteet.

Pääsihteeristön turvallisuusyksikkö on pääsihteerin käytettävissä näihin tehtäviin.

3. Jäsenvaltioiden on 14 artiklan 3 kohdan täytäntöönpanemiseksi

a) nimettävä kansallinen turvallisuusviranomainen, joka vastaa turvallisuusjärjestelyistä EU:n turvaluokiteltujen tietojen suojaamiseksi. Kansalliset turvallisuusviranomaiset luetellaan lisäyksessä C. Kussakin jäsenvaltiossa kansallisen turvallisuusviranomaisen on toteutettava tarvittavat toimenpiteet varmistaakseen, että

i) julkisten tai yksityisten kotimaassa tai ulkomailla toimivien kansallisten yksiköiden, elinten tai virastojen hallussa olevat EU:n turvaluokitellut tiedot on suojattu tämän päätöksen säännösten mukaisesti;

ii) EU:n turvaluokiteltujen tietojen suojaamiseksi toteutetut turvallisuusjärjestelyt tarkastetaan määräajoin;

iii) kaikista kansallisessa hallinnossa tai hankeosapuolen palveluksessa työskentelevistä henkilöistä, joille voidaan myöntää pääsy EU:n CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeamman tason turvaluokiteltuihin tietoihin, on tehty asianmukainen turvallisuusselvitys tai että heillä on tehtäviensä vuoksi muu kansallisten lakien ja asetusten mukainen asianmukainen valtuutus;

iv) tarpeellisiksi katsotut turvallisuusohjelmat on laadittu sen estämiseksi, etteivät EU:n turvaluokitellut tiedot vaarannu eivätkä katoa; ja

v) EU:n turvaluokiteltujen tietojen suojaamiseen liittyvät turvallisuusasiat koordinoidaan muiden toimivaltaisten kansallisten viranomaisten kanssa, tässä päätöksessä tarkoitetut viranomaiset mukaan luettuina;

b) varmistettava, että niiden toimivaltaiset viranomaiset antavat hallituksilleen ja sitä kautta neuvostolle tietoja ja neuvoja EU:n turvaluokiteltuihin tietoihin kohdistuvien turvallisuusuhkien luonteesta ja keinoista suojautua niitä vastaan; ja

c) vastattava EU:n virastojen ja elinten, Euroopan unionista tehdyn sopimuksen V osaston nojalla perustettujen kriisinhallintaoperaatioiden ja EU:n erityisedustajien ja heidän alaisuudessaan työskentelevien henkilöiden esittämiin turvallisuusselvityspyyntöihin.

16 artikla

Turvallisuuskomitea

1. Perustetaan turvallisuuskomitea. Turvallisuuskomitea tutkii ja arvioi tämän päätöksen soveltamisalaan kuuluvat turvallisuusasiat ja antaa tarvittaessa neuvostolle suosituksia.

2. Turvallisuuskomitea muodostuu jäsenvaltioiden kansallisten turvallisuusviranomaisten edustajista, ja Euroopan komission edustaja osallistuu sen kokouksiin. Komitean puheenjohtajana toimii pääsihteeri tai pääsihteerin nimeämä henkilö. Se kokoontuu neuvoston toimeksiannosta tai pääsihteerin taikka kansallisen turvallisuusviranomaisen pyynnöstä.

   EU:n virastojen ja elinten edustajia voidaan kutsua komitean kokouksiin, jos niissä käsitellään niitä koskevia kysymyksiä.

3. Turvallisuuskomitea järjestää toimintansa niin, että se voi antaa suosituksia erityisillä turvallisuuden aloilla. Se muodostaa tiedonturvaamisasioita käsittelevän asiantuntijakokoonpanon ja muita asiantuntijakokoonpanoja tarpeen mukaan. Se laatii kyseisten asiantuntijakokoonpanojen toimeksiannot ja sille toimitetaan niiden toimintakertomukset sekä niiden neuvostolle osoittamat mahdolliset suositukset.

17 artikla

Aiempien päätösten korvaaminen

1. Tällä päätöksellä kumotaan ja korvataan neuvoston turvallisuussääntöjen vahvistamisesta tehty neuvoston päätös 2001/264/EY[1] ja kaikki siihen myöhemmin tehdyt muutokset.

2. Kaikki neuvoston päätöksen 2001/264/EY mukaisesti luokitellut EU:n turvaluokitellut tiedot suojataan edelleen tämän päätöksen asiaankuuluvien säännösten mukaisesti.

[1] EYVL L 101, 11.4.2001, s. 1.

18 artikla

Voimaantulo

Tätä päätöstä sovelletaan päivästä, jona se julkaistaan.

Tehty Brysselissä …

Neuvoston puolesta

Puheenjohtaja

_____

LIITTEET

LIITE I

Henkilöstöturvallisuus

LIITE II

Fyysinen turvallisuus

LIITE III

Turvaluokiteltujen tietojen hallinnointi

LIITE IV

Viestintä- ja tietojärjestelmissä käsiteltävien EU:n turvaluokiteltujen tietojen suojaaminen

LIITE V

Yhteisöturvallisuus

LIITE VI

Turvaluokiteltujen tietojen vaihto kolmansien valtioiden ja kansainvälisten järjestöjen kanssa

HENKILÖSTÖTURVALLISUUS

I JOHDANTO

1. Tässä liitteessä vahvistetaan 7 artiklan täytäntöönpanosäännökset. Siinä säädetään erityisesti perusteista sen päättämiseksi, voidaanko henkilölle hänen lojaaliutensa, rehellisyytensä ja luotettavuutensa huomioon ottaen myöntää pääsy EU:n turvaluokiteltuihin tietoihin, sekä asiassa noudatettavista tutkinta- ja hallinnollisista menettelyistä.

2. Koko tässä liitteessä "henkilöturvallisuusselvityksellä" tarkoitetaan lisäyksessä A määriteltyä kansallista henkilöturvallisuusselvitystä ("kansallinen turvallisuusselvitys") ja/tai EU:n henkilöturvallisuusselvitystä ("EU-turvallisuusselvitys") lukuun ottamatta kohtia, joissa nämä on erotettava toisistaan.

II PÄÄSYN MYÖNTÄMINEN EU:N TURVALUOKITELTUIHIN TIETOIHIN

3. Henkilölle voidaan myöntää pääsy CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeamman turvaluokan tietoihin vasta sen jälkeen, kun

   a) hänen tiedonsaantitarpeensa (need-to-know) on selvitetty; ja

   b) hänelle on myönnetty asianmukaisen tason henkilöturvallisuusselvitys tai hänet on muulla tavoin tehtäviensä vuoksi asianmukaisesti valtuutettu kansallisten lakien ja asetusten mukaisesti; ja

   c) hänelle on selvitetty EU:n turvaluokiteltujen tietojen suojaamista koskevat turvallisuussäännöt ja -menettelyt ja hän on tunnustanut tällaisten tietojen suojaamista koskevan vastuunsa.

4. Kunkin jäsenvaltion ja pääsihteeristön on määritettävä omissa hallintorakenteissaan ne tehtävät, jotka edellyttävät pääsyä CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeamman turvaluokan tietoihin ja siksi asiaankuuluvan tason turvallisuusselvitystä.

III HENKILÖTURVALLISUUSSELVITYSTÄ KOSKEVAT VAATIMUKSET

5. Vastaanotettuaan asianmukaisesti valtuutetun pyynnön kansalliset turvallisuusviranomaiset tai muut toimivaltaiset kansalliset viranomaiset vastaavat siitä, että niiden kansalaisista, joilla on oltava pääsy CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeamman turvaluokan tietoihin, tehdään turvallisuustutkinta. Tutkintaa koskevien vaatimusten on oltava kansallisten lakien ja asetusten mukaisia.

6. Jos asianomainen henkilö asuu toisen jäsenvaltion tai kolmannen valtion alueella, toimivaltaisten kansallisten viranomaisten on pyydettävä apua asuinvaltion toimivaltaisilta viranomaisilta kansallisten lakien ja asetusten mukaisesti. Jäsenvaltioiden on autettava toisiaan turvallisuustutkinnan tekemisessä kansallisten lakien ja asetusten mukaisesti.

7. Kansallisten lakien ja asetusten salliessa kansalliset turvallisuusviranomaiset tai muut toimivaltaiset kansalliset viranomaiset voivat tehdä tutkinnan muista kuin omista kansalaisistaan, joilla on oltava pääsy CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeamman turvaluokan tietoihin. Tutkintaa koskevien vaatimusten on oltava kansallisten lakien ja asetusten mukaisia.

Turvallisuustutkinnan perusteet

8. Henkilön lojaalius, rehellisyys ja luotettavuus on määritettävä tekemällä turvallisuustutkinta, jonka perusteella hänelle voidaan myöntää pääsy CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeamman turvaluokan tietoihin. Toimivaltaisen kansallisen viranomaisen on tehtävä kokonaisarvio turvallisuustutkinnasta saatujen tietojen perusteella. Mikään yksittäinen kielteinen tieto ei välttämättä johda turvallisuusselvityksen epäämiseen. Turvallisuustutkinnan pääasiallisiin perusteisiin olisi kansallisten lakien ja asetusten mukaisesti kuuluttava mahdollisimman laaja tutkinta sen selvittämiseksi,

a) onko henkilö tehnyt tai yrittänyt tehdä vakoiluun, terrorismiin, sabotaasiin, maanpetokseen tai kapinan lietsomiseen liittyvän rikoksen, sopinut toisen kanssa sellaisen tekemisestä tai auttanut toista sellaisen tekemisessä;

b) onko henkilö yhteydessä tai onko hän aikaisemmin ollut yhteydessä vakoojiin, terroristeihin, sabotoijiin tai henkilöihin, joita voidaan kohtuudella epäillä tällaisiksi, tai sellaisten järjestöjen tai vieraiden valtioiden, myös vieraiden valtioiden tiedustelupalvelujen, edustajiin, jotka voivat uhata EU:n ja/tai sen jäsenvaltioiden turvallisuutta, paitsi jos näihin yhteyksiin oli lupa virantoimituksen perusteella;

c) onko henkilö tai onko hän ollut jonkin sellaisen järjestön jäsen, joka väkivaltaisin, kumouksellisin tai muin laittomin keinoin pyrkii muun muassa jonkin jäsenvaltion hallituksen kaatamiseen, perustuslaillisen järjestyksen muuttamiseen tai hallituksen kokoonpanon tai politiikkojen muuttamiseen;

d) onko henkilö tai onko hän ollut jonkin c alakohdassa kuvatun järjestön kannattaja tai onko hän tai onko hän ollut tiiviisti yhteydessä tällaisen järjestön jäseniin;

e) onko henkilö tahallaan salannut tai vääristellyt tai väärentänyt tärkeitä, erityisesti luottamuksellisia tietoja, tai onko hän tahallaan valehdellut henkilöstöturvallisuutta koskevaa kyselylomaketta täyttäessään tai turvallisuutta koskevan haastattelun aikana;

f) onko henkilö tuomittu rikoksesta tai rikoksista;

g) tiedetäänkö henkilön olleen riippuvainen alkoholista, käyttäneen laittomia huumausaineita ja/tai väärinkäyttäneen laillisia lääkeaineita;

h) onko henkilö tai onko hän ollut osallisena sellaisessa toiminnassa, josta voi aiheutua joutuminen alttiiksi kiristykselle tai painostukselle;

i) onko henkilö osoittanut toimillaan tai puheillaan epärehellisyyttä, epälojaaliutta, petollisuutta tai epäluotettavuutta;

j) onko henkilö vakavasti tai toistuvasti rikkonut turvallisuussääntöjä; tai onko hän yrittänyt harjoittaa tai onnistunut harjoittamaan viestintä- ja tietojärjestelmiin kohdistuvaa luvatonta toimintaa;

k) voiko henkilö joutua sellaisten sukulaisten tai läheisten painostamaksi, jotka saattavat olla suojattomia ulkomaiden tiedustelupalveluja, terroristiryhmiä tai muita kumouksellisia järjestöjä tai yksilöitä vastaan, joiden tarkoitusperät voivat uhata EU:n ja/tai jäsenvaltioiden turvallisuusetuja.

9. Tarvittaessa ja kansallisten lakien ja asetusten mukaisesti myös henkilön taloudellista ja lääketieteellistä taustaa voidaan pitää merkityksellisenä turvallisuustutkintaa tehtäessä.

10. Kaksoiskansalaisuus, joista toinen on muun kuin EU:n jäsenvaltion kansalaisuus, ei sinänsä ole syy evätä turvallisuusselvitystä.

11. Tarvittaessa ja kansallisten lakien ja asetusten mukaisesti puolison, avopuolison tai läheisen perheenjäsenen luonne, käytös ja olosuhteet voidaan myös katsoa merkityksellisiksi turvallisuustutkintaa tehtäessä.

Tutkintavaatimukset pääsyn myöntämiseksi EU:n turvaluokiteltuihin tietoihin

Ensimmäisen turvallisuusselvityksen myöntäminen

12. Ensimmäisen turvallisuusselvityksen CONFIDENTIEL UE/EU CONFIDENTIAL- ja SECRET UE/EU SECRET -turvaluokan tietoihin pääsyä varten on perustuttava turvallisuustutkintaan, joka kattaa vähintään viimeiset viisi vuotta tai ajanjakson 18 vuoden iästä nykyhetkeen riippuen siitä, kumpi ajanjakso on lyhyempi, ja johon sisältyy seuraavaa:

    a) henkilöstöturvallisuutta koskevan kansallisen kyselylomakkeen täyttäminen EU:n turvaluokiteltujen tietojen sen turvaluokan osalta, johon henkilön voi olla tarpeen päästä; täytetty kyselylomake on toimitettava toimivaltaiselle turvallisuusviranomaiselle;

    b) henkilöllisyyden tarkistaminen / kansalaisuus / kansalaisuusasema – tarkistetaan henkilön syntymäaika ja -paikka sekä henkilöllisyys. Määritetään henkilön kansalaisuusasema ja/tai kansalaisuus (sekä nykyinen että entiset kansalaisuudet); samalla arvioidaan mahdollinen alttius ulkomaisista lähteistä tulevalle painostukselle, joka liittyy esimerkiksi aiempaan asuinpaikkaan tai aiempiin yhteyksiin; ja

    c) kansallisten ja paikallisten rekisteritietojen tarkistaminen – tarkistetaan kansallisen turvallisuustietorekisterin tiedot ja mahdolliset keskusrikosrekisteritiedot ja/tai muut vastaavat valtion ja poliisin rekisteritiedot. Tarkistetaan sellaisten lainvalvontaviranomaisten merkinnät, jotka ovat oikeudellisesti toimivaltaisia paikkakunnilla, joilla henkilö on asunut tai työskennellyt.

13. Ensimmäisen turvallisuusselvityksen TRES SECRET UE/EU TOP SECRET -turvaluokan tietoihin pääsyä varten on perustuttava turvallisuustutkintaan, joka kattaa vähintään viimeiset 10 vuotta tai ajanjakson 18 vuoden iästä nykyhetkeen riippuen siitä, kumpi ajanjakso on lyhyempi. Jos tehdään haastatteluja tämän kohdan e alakohdan mukaisesti, tutkinnan on katettava vähintään viimeiset seitsemän vuotta tai ajanjakso 18 vuoden iästä nykyhetkeen riippuen siitä, kumpi ajanjakso on lyhyempi. Ennen TRES SECRET UE/EU TOP SECRET -turvallisuusselvityksen myöntämistä on tutkittava edellä 8 kohdassa mainittujen perusteiden lisäksi mahdollisimman laajasti kansallisten lakien ja asetusten mukaisesti seuraavia seikkoja, joita voidaan tutkia myös ennen CONFIDENTIEL UE/EU CONFIDENTIAL- ja SECRET UE/EU SECRET -turvallisuusselvityksen myöntämistä, jos sitä vaaditaan kansallisissa laeissa ja asetuksissa:

a) taloudellinen asema – selvitetään henkilön varallisuustilanne, jotta voidaan arvioida mahdollinen alttius joutua vakavista taloudellisista vaikeuksista johtuvan ulkomailta tai omasta maasta tulevan painostuksen kohteeksi ja havaita mahdollinen selittämätön varallisuus;

b) koulutus – selvitetään henkilön opiskelu kouluissa, yliopistoissa ja muissa oppilaitoksissa sen jälkeen, kun hän on täyttänyt 18 vuotta, tai tutkivien viranomaisten asianmukaiseksi katsomana ajanjaksona;

c) työtausta – selvitetään henkilön nykyinen ja entiset työpaikat käyttäen lähteinä muun muassa työpaikkatietoja ja työsuorituksia tai tehokkuutta koskevia raportteja sekä työnantajia ja esimiehiä;

d) asepalvelus – soveltuvissa tapauksissa on tarkistettava henkilön palvelu asevoimissa ja hänelle asevoimien palveluksesta myönnetyn eron laji; ja

e) haastattelut – haastatellaan asianomaista henkilöä yhden tai useamman kerran, jos haastattelusta säädetään kansallisissa laeissa ja asetuksissa ja jos ne ovat niiden mukaisia. Myös sellaisia muita henkilöitä voidaan haastatella, jotka voivat puolueettomasti arvioida tutkittavan henkilön taustaa, toimia, lojaaliutta, rehellisyyttä ja luotettavuutta. Jos on kansallisen käytännön mukaista pyytää tutkittavaa henkilöä toimittamaan suosituksia, haastatellaan suosituksen antajia, paitsi jos on olemassa hyviä syitä olla haastattelematta heitä.

14. Tarvittaessa ja kansallisten lakien ja asetusten mukaisesti voidaan suorittaa lisätutkimuksia, jotta selvitetään kaikki saatavilla olevat merkitykselliset tiedot asianomaisesta henkilöstä ja voidaan perustella tai osoittaa vääriksi kielteiset tiedot.

Turvallisuusselvityksen uusiminen

15. Sen jälkeen, kun ensimmäinen turvallisuusselvitys on myönnetty ja edellyttäen, että henkilö on ollut yhtäjaksoisesti kansallisen hallinnon tai pääsihteeristön palveluksessa ja että hänen tehtävänsä edellyttävät edelleen pääsyä EU:n turvaluokiteltuihin tietoihin, turvallisuusselvitys on uusittava viimeistään viiden vuoden välein, jos kyse on TRES SECRET UE/EU TOP SECRET -turvallisuusselvityksestä, ja viimeistään kymmenen vuoden välein, jos kyse on SECRET UE/EU SECRET- ja CONFIDENTIEL UE/EU CONFIDENTIAL -turvallisuusselvityksistä, laskettuna selvityksen perustana olleen viimeisen turvallisuustutkinnan tulosten tiedoksiantamisajankohdasta. Kaikki turvallisuusselvityksen uusimista varten tehtävät turvallisuustutkinnat on tehtävä ajalta, joka alkaa siitä, mihin edellinen selvitys päättyi.

16. Turvallisuusselvitysten uusimiseksi on tutkittava 12 ja 13 kohdassa esitetyt seikat.

17. Uusimispyynnöt on esitettävä hyvissä ajoin ottaen huomioon turvallisuusselvitysten tekemisen edellyttämä aika. Jos asiaankuuluva kansallinen turvallisuusviranomainen tai muu toimivaltainen kansallinen viranomainen on vastaanottanut asiaankuuluvan uusimispyynnön ja vastaavan henkilöstöturvallisuutta koskevan kyselylomakkeen ennen turvallisuusselvityksen voimassaolon päättymistä ja jos tarvittava turvallisuustutkinta ei ole vielä valmistunut, toimivaltainen kansallinen viranomainen voi kuitenkin jatkaa voimassa olevan turvallisuusselvityksen voimassaoloa korkeintaan 12 kuukaudella, jos se sallitaan kansallisissa laeissa ja asetuksissa. Jos turvallisuustutkinta ei vielä kyseisen 12 kuukauden ajan päättyessä ole valmistunut, asianomainen henkilö on siirrettävä hoitamaan tehtäviä, joissa ei vaadita turvallisuusselvitystä.

Turvallisuusselvitysmenettelyt pääsihteeristössä

18. Pääsihteeristön virkamiesten ja muun henkilöstön osalta pääsihteeristön turvallisuusviranomainen toimittaa henkilöstöturvallisuutta koskevan kyselylomakkeen täytettynä sen jäsenvaltion kansalliselle turvallisuusviranomaiselle, jonka kansalainen asianomainen henkilö on, ja pyytää turvallisuustutkinnan tekemistä EU:n turvaluokiteltujen tietojen sen luokan osalta, johon henkilön voi olla tarpeen päästä.

19. Jos pääsihteeristön tietoon tulee turvallisuustutkinnan kannalta merkityksellisiä tietoja henkilöstä, joka on hakenut EU-turvallisuusselvitystä, pääsihteeristön on ilmoitettava siitä asianomaiselle kansalliselle turvallisuusviranomaiselle asiaankuuluvien sääntöjen mukaisesti.

20. Turvallisuustutkinnan valmistuttua asiaankuuluvan kansallisen turvallisuusviranomaisen on annettava tutkinnan tulokset pääsihteeristön turvallisuusviranomaiselle tiedoksi turvallisuuskomitean kirjeenvaihtoa varten määräämässä vakiomuodossa.

    a) Jos turvallisuustutkinnalla saadaan varmuus siitä, ettei henkilöstä ole tiedossa mitään sellaista kielteistä seikkaa, jonka perusteella voitaisiin epäillä hänen lojaaliuttaan, rehellisyyttään ja luotettavuuttaan, pääsihteeristön nimittävä viranomainen voi myöntää asianomaiselle henkilölle EU-turvallisuusselvityksen ja antaa hänelle pääsyn EU:n turvaluokiteltuihin tietoihin asiaankuuluvaan turvaluokkaan ja määrättyyn päivään asti.

    b) Jos turvallisuustutkinnalla ei saada tällaista varmuutta, pääsihteeristön nimittävä viranomainen ilmoittaa siitä asianomaiselle henkilölle, joka voi pyytää, että nimittävä viranomainen kuulee häntä. Nimittävä viranomainen voi pyytää mahdollista lisäselvitystä toimivaltaiselta kansalliselta turvallisuusviranomaiselta sen kansallisten lakien ja asetusten mukaisesti. Jos tulos vahvistetaan, EU-turvallisuusselvitystä ei myönnetä.

21. Turvallisuustutkintaan ja sen tuloksiin sovelletaan kyseisessä jäsenvaltiossa voimassa olevia asiaa koskevia lakeja ja asetuksia mahdolliset muutoksenhakukeinot mukaan luettuina. Pääsihteeristön nimittävän viranomaisen päätöksiin voi hakea muutosta Euroopan yhteisöjen virkamiehiin sovellettavien henkilöstösääntöjen ja Euroopan yhteisöjen muuhun henkilöstöön sovellettavien palvelussuhteen ehtojen mukaisesti.

22. EU-turvallisuusselvityksen on katettava kaikki asianomaisen henkilön pääsihteeristössä tai Euroopan komissiossa suorittamat tehtävät edellyttäen, että turvallisuusselvityksen perustana oleva varmuus on edelleen pätevä.

23. Jos henkilön palvelusaika ei ala 12 kuukauden kuluessa siitä, kun turvallisuustutkinnan tulokset on annettu tiedoksi pääsihteeristön nimittävälle viranomaiselle, tai jos henkilön palveluksessaolo keskeytyy 12 kuukaudeksi eikä hän sinä aikana ole pääsihteeristön eikä minkään jäsenvaltion kansallisen hallinnon palveluksessa, tuloksista on otettava yhteyttä asiaankuuluvaan kansalliseen turvallisuusviranomaiseen niiden voimassapysymisen ja asianmukaisuuden vahvistamiseksi.

24. Jos pääsihteeristön tietoon tulee, että voimassa olevan EU-turvallisuusselvityksen haltija saattaa aiheuttaa turvallisuusriskin, pääsihteeristön on ilmoitettava siitä asianomaiselle kansalliselle turvallisuusviranomaiselle asiaankuuluvien sääntöjen mukaisesti. Jos kansallinen turvallisuusviranomainen ilmoittaa pääsihteeristölle voimassa olevan EU-turvallisuusselvityksen haltijalle 20 kohdan a alakohdan mukaisesti annetun varmuuden peruuttamisesta, pääsihteeristön nimittävä viranomainen voi pyytää selvennystä, jonka kansallinen turvallisuusviranomainen voi antaa jäsenvaltionsa lakien ja asetusten mukaisesti. Jos kielteinen seikka vahvistetaan, EU-turvallisuusselvitys on peruutettava, henkilöltä on evättävä pääsy EU:n turvaluokiteltuihin tietoihin ja hänet on siirrettävä pois tehtävistä, joissa niihin pääsy on mahdollista tai joissa turvallisuus voisi hänen vuokseen vaarantua.

25. Kaikki pääsihteeristön virkamiehen tai muun henkilöstön jäsenen EU-turvallisuusselvityksen peruuttamista koskevat päätökset ja tapauksen mukaan niiden perusteet on annettava tiedoksi asianomaiselle henkilölle, joka voi pyytää, että nimittävä viranomainen kuulee häntä. Kansallisen turvallisuusviranomaisen toimittamiin tietoihin sovelletaan kyseisessä jäsenvaltiossa voimassa olevia asiaa koskevia lakeja ja asetuksia mahdolliset muutoksenhakukeinot mukaan luettuina. Pääsihteeristön nimittävän viranomaisen päätöksiin voi hakea muutosta Euroopan yhteisöjen virkamiehiin sovellettavien henkilöstösääntöjen ja Euroopan yhteisöjen muuhun henkilöstöön sovellettavien palvelussuhteen ehtojen mukaisesti.

26. Kansallisten asiantuntijoiden, jotka lähetetään pääsihteeristöön EU-turvallisuusselvitystä edellyttäviin tehtäviin, on esitettävä pääsihteeristön turvallisuusviranomaiselle voimassa oleva kansallinen turvallisuusselvitys EU:n turvaluokiteltuihin tietoihin pääsemistä varten ennen tehtäviensä aloittamista.

Turvallisuusselvityksiä koskeva kirjanpito

27. Kukin jäsenvaltio pitää kirjaa niistä kansallisista turvallisuusselvityksistä ja pääsihteeristö niistä EU-turvallisuusselvityksistä, jotka ne ovat myöntäneet pääsyn antamiseksi EU:n turvaluokiteltuihin tietoihin. Kirjanpitoon on merkittävä vähintään korkein turvaluokka, johon kuuluviin EU:n turvaluokiteltuihin tietoihin henkilölle voidaan myöntää pääsy (CONFIDENTIEL UE/EU CONFIDENTIAL tai korkeampi), turvallisuusselvityksen myöntämispäivä ja sen voimassaoloaika.

28. Toimivaltainen turvallisuusviranomainen voi antaa henkilöstöturvallisuusselvitykseen perustuvan todistuksen, josta käyvät ilmi turvaluokka, johon kuuluviin EU:n turvaluokiteltuihin tietoihin asianomaiselle henkilölle voidaan myöntää pääsy (CONFIDENTIEL UE/EU CONFIDENTIAL tai korkeampi), EU:n turvaluokiteltuihin tietoihin pääsyä varten asiaankuuluvan kansallisen turvallisuusselvityksen tai EU-turvallisuusselvityksen voimassaoloaika ja itse todistuksen voimassaolon päättymispäivä.

Vapautukset turvallisuusselvitysvaatimuksesta

29. Jäsenvaltioissa tehtäviensä vuoksi asianmukaisesti valtuutettujen henkilöiden pääsy EU:n turvaluokiteltuihin tietoihin on määriteltävä kansallisten lakien ja asetusten mukaisesti. Kyseisille henkilöille on selvitettävä heidän turvallisuusvelvoitteensa EU:n turvaluokiteltujen tietojen suojaamisen osalta.

IV TURVALLISUUSKOULUTUS JA -TIETOISUUS

30. Kaikkien henkilöiden, joille on myönnetty turvallisuusselvitys, on kirjallisesti vakuutettava ymmärtävänsä velvollisuutensa suojata EU:n turvaluokitellut tiedot sekä seuraukset, joihin EU:n turvaluokiteltujen tietojen vaarantuminen johtaa. Jäsenvaltiot ja tapauksen mukaan pääsihteeristö pitävät kirjaa tällaisista kirjallisista vakuutuksista.

31. Kaikille henkilöille, joille on myönnetty pääsy EU:n turvaluokiteltuihin tietoihin tai joiden edellytetään käsittelevän niitä, on aluksi selvitettävä turvallisuusuhat ja säännöllisin väliajoin tiedotettava niistä, ja heidän on ilmoitettava välittömästi asianomaisille turvallisuusviranomaisille epäilyttävinä tai epätavanomaisina pitämistään yhteydenotoista tai toimista.

32. Kaikille henkilöille, jotka siirtyvät pois tehtävistä, jotka edellyttävät pääsyä EU:n turvaluokiteltuihin tietoihin, on selvitettävä heidän velvollisuutensa edelleen suojata EU:n turvaluokitellut tiedot, ja heidän on tarvittaessa annettava siitä kirjallinen vakuutus.

V POIKKEUKSELLISET OLOSUHTEET

33. Jäsenvaltion toimivaltaisen kansallisen viranomaisen myöntämässä henkilöturvallisuusselvityksessä kansallisten turvaluokiteltujen tietojen saamiseksi voidaan tilapäisesti siihen asti, kunnes kansallinen turvallisuusselvitys pääsystä EU:n turvaluokiteltuihin tietoihin myönnetään, sallia kansallisten virkamiesten pääsy EU:n turvaluokiteltuihin tietoihin lisäyksessä B olevassa vastaavuustaulukossa määriteltyyn vastaavaan turvaluokkaan saakka, jos se sallitaan kansallisissa laeissa ja asetuksissa ja jos tilapäinen pääsy on EU:n etujen vuoksi tarpeen. Kansallisten turvallisuusviranomaisten on ilmoitettava turvallisuuskomitealle, jos tällaista tilapäistä pääsyä EU:n turvaluokiteltuihin tietoihin ei sallita kansallisissa laeissa ja asetuksissa.

34. Jos se on yksikön etujen vuoksi asianmukaisesti perusteltua ja jos täydellistä turvallisuustutkintaa ei ole vielä saatu päätökseen, pääsihteeristön nimittävä viranomainen voi kiireellisyyssyistä ja kuultuaan sen jäsenvaltion kansallista turvallisuusviranomaista, jonka kansalainen henkilö on, ja riippuen kielteisten seikkojen olemassaoloa koskevien alustavien tarkistusten tuloksista, myöntää pääsihteeristön virkamiehille ja muun henkilöstön jäsenille tilapäisen valtuutuksen ja pääsyn EU:n turvaluokiteltuihin tietoihin tietyn tehtävän suorittamiseksi. Kyseiset tilapäiset valtuutukset ovat voimassa korkeintaan kuusi kuukautta, eivätkä ne oikeuta saamaan TRES SECRET UE/EU TOP SECRET -turvaluokan tietoja. Kaikkien henkilöiden, joille on myönnetty tilapäinen valtuutus, on kirjallisesti vakuutettava ymmärtävänsä velvollisuutensa suojata EU:n turvaluokitellut tiedot sekä seuraukset, jos EU:n turvaluokitellut tiedot vaarantuvat. Pääsihteeristö pitää kirjaa tällaisista kirjallisista vakuutuksista.

35. Jos henkilö on määrä nimittää tehtävään, joka edellyttää yhtä tasoa korkeamman tason turvallisuusselvitystä kuin hänellä tuolloin on, nimitys voidaan tehdä väliaikaisesti edellyttäen, että

a) henkilön esimies perustelee kirjallisesti pakottavan tarpeen päästä korkeamman turvaluokan EU:n turvaluokiteltuihin tietoihin;

b) pääsy rajataan koskemaan tiettyjä erikseen määriteltyjä EU:n turvaluokiteltuja tietoja nimityksen mukaisesti;

c) henkilöllä on voimassa oleva kansallinen turvallisuusselvitys tai EU-turvallisuusselvitys;

d) on ryhdytty toimiin valtuutuksen saamiseksi tehtävän edellyttämää tiedonsaantitasoa varten;

e) toimivaltainen viranomainen on riittävin tarkistuksin varmistanut, että henkilö ei ole vakavasti tai toistuvasti rikkonut turvallisuussääntöjä;

f) toimivaltainen viranomainen hyväksyy henkilön nimityksen; ja

g) asiasta vastaavassa keskuskirjaamossa tai alakirjaamossa säilytetään tieto poikkeuksesta ja kuvaus tiedoista, joihin pääsy sallittiin.

36. Edellä kuvattua menettelyä on käytettävä myönnettäessä henkilölle kertaluonteisesti pääsy EU:n turvaluokiteltuihin tietoihin, jotka on luokiteltu yhtä turvaluokkaa korkeammalle kuin se, jota hänen turvallisuusselvityksensä koskee. Menettelyä ei saa käyttää toistuvasti.

37. Erittäin poikkeuksellisissa olosuhteissa eli toteutettaessa operaatioita vihamielisessä ympäristössä tai kasvavien kansainvälisten jännitteiden aikana jäsenvaltiot ja pääsihteeri tai apulaispääsihteeri voivat kiireellisten toimenpiteiden niin edellyttäessä ja erityisesti ihmishenkien pelastamiseksi myöntää mahdollisuuksien mukaan kirjallisesti pääsyn CONFIDENTIEL UE/EU CONFIDENTIAL- tai SECRET UE/EU SECRET -turvaluokan tietoihin henkilöille, joilla ei ole vaadittua turvallisuusselvitystä edellyttäen, että kyseinen lupa on ehdottoman välttämätön eikä asianomaisen henkilön lojaaliudesta, rehellisyydestä ja luotettavuudesta ole perusteltua epäilystä. Tällaisesta luvasta on säilytettävä kirjanpidossa tieto ja kuvaus tiedoista, joihin pääsy hyväksyttiin.

38. TRES SECRET UE/EU TOP SECRET -turvaluokan tietojen osalta kiireellisyyssyistä myönnetty pääsy on rajattava EU:n kansalaisiin, joille on myönnetty pääsy joko TRES SECRET UE/EU TOP SECRET -turvaluokkaa vastaavan kansallisen turvaluokan tietoihin tai SECRET UE/EU SECRET -turvaluokan tietoihin.

39. Turvallisuuskomitealle on ilmoitettava tapauksista, joissa käytetään 37 ja 38 kohdan mukaista menettelyä.

40. Jos jäsenvaltion laeissa ja asetuksissa säädetään tiukemmista säännöistä tilapäisten valtuutusten osalta, väliaikaisista nimityksistä tai henkilöille myönnettävästä pääsystä turvaluokiteltuihin tietoihin kertaluonteisesti tai kiireellisessä tapauksessa, tässä jaksossa kuvattuja menettelyjä on sovellettava ainoastaan asiaankuuluvissa kansallisissa laeissa ja asetuksissa säädetyissä rajoissa.

41. Turvallisuuskomitealle on toimitettava vuosittain selvitys tässä jaksossa säädettyjen menettelyjen käytöstä.

VI NEUVOSTOSSA PIDETTÄVIIN KOKOUKSIIN OSALLISTUMINEN

42. Jollei 29 kohdasta muuta johdu, henkilöiden, jotka on nimetty osallistumaan neuvoston istuntoihin tai neuvoston valmistelevien elinten kokouksiin, joissa käsitellään CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeamman turvaluokan tietoja, on ensin esitettävä vahvistus turvallisuusselvityksestään. Valtuuskuntien jäsenten osalta asianomaisten viranomaisten on toimitettava henkilöturvallisuusselvitykseen perustuva henkilöturvallisuustodistus tai muu todiste turvallisuusselvityksestä pääsihteeristön turvallisuusyksikölle, tai asianomainen valtuuskunnan jäsen voi poikkeuksellisesti esittää sen henkilökohtaisesti. Tarvittaessa voidaan käyttää nimiluetteloa, joka on asianmukainen näyttö turvallisuusselvityksestä.

43. Jos henkilön, jonka tehtävät edellyttävät osallistumista neuvoston tai neuvoston valmistelevien elinten kokouksiin, kansallinen turvallisuusselvitys perutaan turvallisuussyistä, toimivaltaisen viranomaisen on ilmoitettava asiasta pääsihteeristölle.

VII MAHDOLLINEN PÄÄSY EU:N TURVALUOKITELTUIHIN TIETOIHIN

44. Jos henkilöiden on määrä suorittaa tehtäviä, joissa heillä voi mahdollisesti olla pääsy CONFIDENTIEL UE/EU CONDIDENTIAL- tai sitä korkeamman turvaluokan tietoihin, heillä on oltava asianmukainen turvallisuusselvitys tai heillä on aina oltava saattaja.

45. Kuriireilla, vartijoilla ja saattajilla on oltava asiaankuuluvan tason turvallisuusselvitys tai heidän on oltava muulla tavoin asianmukaisesti tutkittuja kansallisten lakien ja asetusten mukaisesti, ja heille on selvitettävä EU:n turvaluokiteltujen tietojen suojaamista koskevat turvallisuusmenettelyt ja annettava ohjeet heidän mainittujen tietojen suojaamiseen liittyvistä tehtävistään.

_____

FYYSINEN TURVALLISUUS

I JOHDANTO

1. Tässä liitteessä vahvistetaan 8 artiklan täytäntöönpanosäännökset. Siinä vahvistetaan EU:n turvaluokiteltujen tietojen käsittelyyn ja säilyttämiseen käytettyjen tilojen, rakennusten, toimistojen, huoneiden ja muiden alueiden, viestintä- ja tietojärjestelmien sijoitusalueet mukaan luettuina, fyysistä suojaamista koskevat vähimmäisvaatimukset.

2. Fyysisten turvatoimien tarkoituksena on estää luvaton pääsy EU:n turvaluokiteltuihin tietoihin

   a) varmistamalla, että EU:n turvaluokiteltuja tietoja käsitellään ja säilytetään asianmukaisesti;

   b) mahdollistamalla henkilöstön luokitus ja pääsy EU:n turvaluokiteltuihin tietoihin sen perusteella, mikä heidän tiedonsaantitarpeensa on, ja tarvittaessa henkilöiden turvallisuusselvitysten perusteella;

   c) ehkäisemällä, estämällä ja havaitsemalla luvattomat toimet; ja

   d) estämällä tunkeutuminen salaa tai väkisin tai viivyttämällä sitä.

II FYYSISET TURVALLISUUSVAATIMUKSET JA TURVATOIMET

3. Fyysisten turvatoimien valinnan on perustuttava toimivaltaisten viranomaisten tekemään uhka-arvioon. Pääsihteeristön ja jäsenvaltioiden on sovellettava riskinhallintaprosessia EU:n turvaluokiteltujen tietojen suojaamiseksi tiloissaan, jotta varmistettaisiin, että fyysisen suojelun taso vastaa arvioitua riskiä. Riskinhallintaprosessissa on otettava huomioon kaikki asiaankuuluvat tekijät, erityisesti seuraavat:

a) EU:n turvaluokiteltujen tietojen turvaluokka;

b) EU:n turvaluokiteltujen tietojen muoto ja määrä pitäen mielessä, että niiden suuri määrä tai kokoaminen yhteen voi edellyttää tiukempien suojatoimenpiteiden soveltamista;

c) EU:n turvaluokiteltujen tietojen sijoitusrakennusten tai -alueiden ympäristö ja rakenne; ja

d) niiden tiedustelupalvelujen muodostama arvioitu uhka, jotka kohdistavat toimiaan EU:hun tai jäsenvaltioihin, ja sabotaasin, terrorismin ja kumouksellisen tai muun rikollisen toiminnan uhka.

4. Toimivaltaisen turvallisuusviranomaisen on syvyyssuuntaisen turvallisuuden käsitettä soveltaen määriteltävä asianmukainen fyysisten turvatoimien yhdistelmä. Ne voivat käsittää yhden tai useampia seuraavista:

a) turvaeste: fyysinen este, jolla suojattava alue rajataan;

b) murronpaljastusjärjestelmät: turvaesteen tarjoaman turvatason parantamiseksi voidaan käyttää murronpaljastusjärjestelmää. Sellaista voidaan käyttää myös huoneissa ja rakennuksissa turvallisuushenkilöstön sijasta tai sen tueksi;

c) kulunvalvonta: kulunvalvontaa voidaan soveltaa alueeseen, alueen yhteen tai useampaan rakennukseen tai rakennuksen alueisiin tai huoneisiin. Valvonta voidaan toteuttaa sähköisin tai sähkömekaanisin välinein, turvahenkilöstön ja/tai vastaanottovirkailijan toimesta tai muunlaisin fyysisin keinoin;

d) turvahenkilöstö: koulutettua, valvottua ja tarvittaessa asianmukaisesti turvallisuusselvitettyä turvallisuushenkilöstöä voidaan ottaa palvelukseen muun muassa tunkeutumista suunnittelevien henkilöiden aikeiden torjumiseksi;

e) kameravalvonta: turvahenkilöstö voi käyttää kameravalvontaa tilanteiden ja murronpaljastusjärjestelmien hälytysten todentamiseksi laajoilla alueilla tai rajatuilla alueilla;

f) turvavalaistus: mahdollisia tunkeutujia voidaan estää käyttämällä turvavalaistusta, jonka ansiosta turvallisuushenkilöstö voi myös valvoa aluetta tehokkaasti joko suoraan tai kameravalvontajärjestelmän välityksellä; ja

g) muut asianmukaiset fyysiset toimenpiteet, joiden tarkoituksena on luvattoman pääsyn estäminen ja havaitseminen tai EU:n turvaluokiteltujen tietojen katoamisen tai vahingoittumisen ehkäiseminen.

5. Toimivaltainen viranomainen voidaan valtuuttaa tekemään sisään- ja ulostulotarkastuksia, millä estetään aineiston luvaton tuonti tai EU:n turvaluokiteltujen tietojen poisvienti tiloista tai rakennuksista.

6. Jos EU:n turvaluokiteltuihin tietoihin kohdistuu salakatselun riski, vahingossa tapahtuva salakatselu mukaan luettuna, on toteutettava asianmukaiset toimenpiteet riskin torjumiseksi.

7. Uusien toimitilojen osalta fyysisten turvallisuusvaatimusten ja niiden toiminnallisten eritelmien määrittelyn on oltava osa toimitilojen suunnittelua. Jo olemassa olevien toimitilojen osalta fyysiset turvallisuusvaatimukset on pantava täytäntöön mahdollisimman täydellisesti.

III EU:N TURVALUOKITELTUJEN TIETOJEN FYYSISEEN SUOJELUUN TARKOITETUT LAITTEET

8. Hankittaessa EU:n turvaluokiteltujen tietojen fyysiseen suojeluun tarkoitettuja laitteita (esimerkiksi turvakaappeja, paperisilppureita, ovilukkoja, elektronisia kulunvalvontajärjestelmiä, murronpaljastusjärjestelmiä ja hälytysjärjestelmiä) toimivaltaisen turvallisuusviranomaisen on varmistettava, että laitteet ovat hyväksyttyjen teknisten standardien ja vähimmäisvaatimusten mukaisia.

9. EU:n turvaluokiteltujen tietojen fyysiseen suojeluun käytettyjen laitteiden tekniset eritelmät on esitettävä turvallisuutta koskevissa suuntaviivoissa, jotka turvallisuuskomitea hyväksyy.

10. Turvallisuusjärjestelmät on tarkastettava määräajoin, ja laitteet on huollettava säännöllisin väliajoin. Huolto on tehtävä suoritettujen tarkastusten tulokset huomioon ottaen, jotta varmistettaisiin laitteiden optimaalinen suoritustaso myös jatkossa.

11. Yksittäisten turvatoimien ja koko turvallisuusjärjestelmän tehokkuus on arvioitava uudelleen kunkin tarkastuksen yhteydessä.

IV FYYSISESTI SUOJATUT ALUEET

12. EU:n turvaluokiteltujen tietojen fyysiseksi suojaamiseksi on perustettava kahdentyyppisiä fyysisesti suojattuja alueita tai vastaavia kansallisia alueita:

– hallinnollisia alueita ja

– turva-alueita (teknisesti suojatut turva-alueet mukaan luettuina).

Kaikkia tässä päätöksessä olevia viittauksia hallinnollisiin alueisiin ja turva-alueisiin, teknisesti suojatut turva-alueet mukaan luettuina, on pidettävä viittauksina myös niitä vastaaviin kansallisiin alueisiin.

13. Toimivaltaisen turvallisuusviranomaisen on todettava, että alue täyttää vaatimukset, jotka koskevat nimeämistä hallinnolliseksi alueeksi, turva-alueeksi tai teknisesti suojatuksi turva-alueeksi.

14. Hallinnollisiin alueisiin sovelletaan seuraavaa:

a) alueella on oltava selkeästi määritellyt näkyvät rajat, joilla henkilöt ja mahdollisuuksien mukaan ajoneuvot voidaan tarkastaa;

b) vain toimivaltaisen viranomaisen asianmukaisesti valtuuttamilla henkilöillä on pääsy alueelle ilman saattajaa; ja

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

15. Turva-alueisiin sovelletaan seuraavaa:

a) alueella on oltava selkeästi määritellyt ja suojatut rajat, joilla valvotaan kulkua sisään ja ulos kulkuluvin tai henkilökohtaisesti tunnistamalla;

b) pääsy alueelle ilman saattajaa on vain henkilöillä, joilla on turvallisuusselvitys ja erityinen lupa tulla alueelle tiedonsaantitarpeensa perusteella;

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

16. Jos turva-alueelle tulo merkitsee käytännössä välitöntä pääsyä sillä oleviin turvaluokiteltuihin tietoihin, sovelletaan lisäksi seuraavia vaatimuksia:

a) alueella tavanomaisesti säilytettyjen tietojen korkein turvaluokka on ilmoitettava selkeästi;

b) kaikilla vierailijoilla on oltava erityinen lupa tulla alueelle, heillä on aina oltava saattaja ja heillä on oltava asianmukainen turvallisuusselvitys, paitsi jos on toteutettu toimia sen varmistamiseksi, ettei EU:n turvaluokiteltuihin tietoihin ole pääsyä.

17. Salakuuntelulta suojatut turva-alueet on nimettävä teknisesti suojatuiksi turva-alueiksi. Kyseisiin alueisiin sovelletaan lisäksi seuraavia vaatimuksia:

a) alueilla on oltava murronpaljastusjärjestelmä, ne on pidettävä lukittuina silloin, kun niitä ei käytetä, ja niitä on vartioitava silloin, kun ne ovat käytössä. Avaimia on valvottava jäljempänä olevan VI jakson mukaisesti;

b) alueille tulevia henkilöitä ja aineistoja on valvottava;

c) alueet on tarkastettava fyysisesti ja/tai teknisesti säännöllisin väliajoin toimivaltaisen turvallisuusviranomaisen vaatimusten mukaisesti. Tällaiset tarkastukset on suoritettava myös mahdollisen luvattoman sisäänpääsyn tai sen epäilyn johdosta; ja

d) alueilla ei saa olla luvattomia tietoliikenneyhteyksiä, luvattomia puhelimia eikä muita luvattomia viestintävälineitä eikä sähkö- tai elektronisia laitteita.

18. Sen estämättä, mitä 17 kohdan d alakohdassa säädetään, toimivaltaisen viranomaisen on tarkastettava kaikki viestintä-, sähkö- tai elektroniset laitteet ennen kuin niitä käytetään alueilla, joilla pidetään SECRET UE/EU SECRET- tai sitä korkeamman turvaluokan tietoihin liittyviä kokouksia tai tehdään tällaisiin tietoihin liittyvää työtä, silloin kun EU:n turvaluokiteltuihin tietoihin kohdistuva uhka arvioidaan korkeaksi, ja näin varmistettava, ettei niillä voi tahattomasti eikä tahallisesti välittää ymmärrettävässä muodossa olevia tietoja turva-alueen rajojen ulkopuolelle.

19. Turva-alueet, joilla ei ole henkilöstöä palveluksessa vuorokauden ympäri, on tarvittaessa tarkastettava normaalin työajan päätteeksi ja satunnaisiin aikoihin sen ulkopuolella paitsi, jos alueelle on asennettu murronpaljastusjärjestelmä.

20. Turva-alueita ja teknisesti suojattuja turva-alueita voidaan tilapäisesti perustaa hallinnolliselle alueelle turvaluokiteltua kokousta tai muuta vastaavaa tarkoitusta varten.

21. Kullekin turva-alueelle on laadittava turvallisuusmenettelyt, joissa on määräykset seuraavista:

a) EU:n turvaluokiteltujen tietojen, joita alueella voidaan käsitellä ja säilyttää, turvaluokka;

b) sovellettavat valvonta- ja suojatoimenpiteet;

c) henkilöt, joilla on pääsy alueelle ilman saattajaa tiedonsaantitarpeensa ja turvallisuusselvityksensä perusteella;

d) tarvittaessa menettelyt saattajien käyttämiseksi tai EU:n turvaluokiteltujen tietojen suojaamiseksi silloin, kun muille henkilöille myönnetään pääsy alueelle;

e) muut asiaankuuluvat toimenpiteet ja menettelyt.

22. Turva-alueille on rakennettava kassaholveja. Toimivaltaisen turvallisuusviranomaisen on hyväksyttävä seinät, lattiat, katot, ikkunat ja lukittavat ovet ja määrättävä niiden suojaamisesta samalla tasolla kuin saman turvaluokan EU:n turvaluokiteltujen tietojen säilyttämiseen hyväksytyt turvakaapit.

V EU:N TURVALUOKITELTUJEN TIETOJEN KÄSITTELYSSÄ JA SÄILYTTÄMISESSÄ NOUDATETTAVAT FYYSISET SUOJATOIMENPITEET

23. RESTREINT UE/EU RESTRICTED -turvaluokan EU:n turvaluokiteltuja tietoja voidaan käsitellä

a) turva-alueella,

b) hallinnollisella alueella, jos pääsy EU:n turvaluokiteltuihin tietoihin on suojattu sivullisilta, tai

c) turva-alueen tai hallinnollisen alueen ulkopuolella, jos tietojen haltija kuljettaa EU:n turvaluokiteltuja tietoja liitteessä III olevan 28–38 kohdan mukaisesti ja hän on sitoutunut noudattamaan toimivaltaisen turvallisuusviranomaisen antamissa turvallisuusohjeissa määrättyjä korvaavia toimenpiteitä sen varmistamiseksi, että pääsy EU:n turvaluokiteltuihin tietoihin on suojattu sivullisilta.

24. RESTREINT UE/EU RESTRICTED -turvaluokan EU:n turvaluokiteltuja tietoja on säilytettävä soveltuvissa lukituissa toimistokalusteissa hallinnollisella alueella tai turva-alueella.

Niitä voidaan tilapäisesti säilyttää turva-alueen tai hallinnollisen alueen ulkopuolella, jos tietojen haltija on sitoutunut noudattamaan toimivaltaisen turvallisuusviranomaisen antamissa turvallisuusohjeissa määrättyjä korvaavia toimenpiteitä.

25. CONFIDENTIEL UE/EU CONFIDENTIAL tai SECRET UE/EU SECRET -turvaluokan EU:n turvaluokiteltuja tietoja voidaan käsitellä

a) turva-alueella,

b) hallinnollisella alueella, jos pääsy EU:n turvaluokiteltuihin tietoihin on suojattu sivullisilta, tai

c) turva-alueen tai hallinnollisen alueen ulkopuolella, jos tietojen haltija

i) kuljettaa EU:n turvaluokiteltuja tietoja liitteessä III olevan 28–38 kohdan mukaisesti,

ii) on sitoutunut noudattamaan toimivaltaisen turvallisuusviranomaisen antamissa turvallisuusohjeissa määrättyjä korvaavia toimenpiteitä sen varmistamiseksi, että pääsy EU:n turvaluokiteltuihin tietoihin on suojattu sivullisilta; ja

iii) pitää EU:n turvaluokitellut tiedot kaikkina aikoina henkilökohtaisessa valvonnassaan; ja

iv) on ilmoittanut asiasta asiaankuuluvalle kirjaamolle, jos kyseessä ovat paperimuodossa olevat asiakirjat.

26. CONFIDENTIEL UE/EU CONFIDENTIAL- ja SECRET UE/EU SECRET -turvaluokan EU:n turvaluokitellut tiedot on säilytettävä turva-alueella turvakaapissa tai kassaholvissa.

27. TRES SECRET UE/EU TOP SECRET -turvaluokan EU:n turvaluokiteltuja tietoja on käsiteltävä turva-alueella.

28. TRES SECRET UE/EU TOP SECRET -turvaluokan EU:n turvaluokiteltuja tietoja on säilytettävä turva-alueella seuraavien ehtojen mukaisesti:

a) turvakaapissa 8 kohdan mukaisesti soveltaen yhtä tai useampaa seuraavaa lisävalvontaa:

i) jatkuva suojaus tai turvallisuusselvitetyn turvallisuushenkilöstön tai pysyvän henkilöstön säännölliset tarkastukset;

ii) hyväksytty murronpaljastusjärjestelmä ja hälytyksiin vastaava turvallisuushenkilöstö; tai

b) murronpaljastusjärjestelmällä varustetussa kassaholvissa, minkä lisäksi turvallisuushenkilöstö vastaa hälytyksiin.

29. Ennen poistumistaan EU:n turvaluokiteltujen tietojen säilytysalueelta tietojen haltijoiden on varmistettava, että tiedot ovat turvassa.

30. Säännöt EU:n turvaluokiteltujen tietojen kuljettamisesta fyysisesti suojattujen alueiden ulkopuolella vahvistetaan liitteessä III.

VI EU:N TURVALUOKITELTUJEN TIETOJEN SUOJAAMISEEN KÄYTETTYJEN AVAINTEN JA NUMEROYHDISTELMIEN VALVONTA

31. Toimivaltaisen turvallisuusviranomaisen on määriteltävä toimistojen, huoneiden, kassaholvien ja turvakaappien avainten ja numeroyhdistelmien hallinnointimenettelyt.

32. Avaimet ja numeroyhdistelmät on suojattava ja niihin on sovellettava vähintään samantasoisia valvontatoimenpiteitä kuin EU:n turvaluokiteltuihin tietoihin, joihin pääsyn ne mahdollistavat.

33. Numeroyhdistelmät on annettava mahdollisimman harvoille henkilöille, joiden on tarpeen tietää ne, ja heidän on osattava ne ulkoa. EU:n turvaluokiteltuja tietoja sisältävien turvakaappien numeroyhdistelmät on vaihdettava

a) aina, kun numeroyhdistelmän tuntevassa henkilöstössä tapahtuu muutos,

b) aina, kun tiedot ovat vaarantuneet tai kun niiden epäillään vaarantuneen ja

c) vähintään 12 kuukauden välein.

TURVALUOKITELTUJEN TIETOJEN HALLINNOINTI

I JOHDANTO

1. Tässä liitteessä vahvistetaan 9 artiklan täytäntöönpanosäännökset. Siinä vahvistetaan hallinnolliset toimenpiteet EU:n turvaluokiteltujen tietojen valvomiseksi koko niiden elinkaaren ajan, jotta autetaan estämään ja havaitsemaan tällaisten tietojen tahallinen tai tahaton vaarantuminen tai katoaminen ja korjaamaan vaarantumistilanne.

II TURVALUOKITTELUN HALLINNOINTI

Turvaluokat ja merkinnät

2. Tiedot turvaluokitellaan, jos niiden luottamuksellisuus on suojattava.

3. EU:n turvaluokiteltujen tietojen alkuperäisen luovuttajan on vastattava tietojen turvaluokan määrittelystä ja niiden alustavasta jakelusta.

4. EU:n turvaluokiteltujen tietojen turvaluokka määritellään tämän päätöksen 2 artiklan 2 kohdan mukaisesti ja soveltaen turvallisuusperiaatteita, jotka hyväksytään 3 artiklan 3 kohdan mukaisesti.

5. Turvaluokka on merkittävä selkeästi ja oikein riippumatta siitä, ovatko EU:n turvaluokitellut tiedot paperi-, suullisessa, sähköisessä vai jossakin muussa muodossa.

6. EU:n turvaluokitelluille tiedoille ei saa määritellä liian korkeaa eikä liian matalaa turvaluokkaa.

7. Tietyn asiakirjan yksittäiset osat (sivut, kohdat, jaksot, liitteet, lisäykset, saatteet ja oheistukset) saattavat edellyttää eri turvaluokkia, ja ne on merkittävä vastaavasti, myös silloin, kun ne tallennetaan sähköisesti.

8. Koko asiakirjan tai tiedoston turvaluokan on oltava vähintään yhtä korkea kuin sen korkeimpaan turvaluokkaan määritellyn osan turvaluokka. Jos eri lähteistä peräisin olevia tietoja yhdistetään, lopputuote on tarkistettava sen kokonaisturvaluokan määrittämiseksi, koska asiakirja voi edellyttää korkeampaa turvaluokkaa kuin sen muodostavat osat.

9. Asiakirjat, jotka sisältävät eri turvaluokkiin kuuluvia osia, on mahdollisuuksien mukaan laadittava niin, että eri turvaluokkiin kuuluvat osat voidaan helposti tunnistaa ja tarvittaessa poistaa.

10. Liitteitä sisältävän kirjeen tai ilmoituksen turvaluokan on oltava yhtä korkea kuin sen liitteiden korkein turvaluokka. Luovuttajan on ilmoitettava selvästi asiakirjan turvaluokka ilman liitteitä asianmukaisella merkinnällä esimerkiksi seuraavasti:

CONFIDENTIEL UE/EU CONFIDENTIAL
Ilman liitteitä RESTREINT UE/EU RESTRICTED.

Merkinnät

11. Tämän päätöksen 2 artiklan 2 kohdassa säädettyjen turvaluokitusmerkintöjen lisäksi EU:n turvaluokitelluissa tiedoissa voi olla muita merkintöjä, esimerkiksi

a) tunniste, joka osoittaa tietojen luovuttajan;

b) varoitusmerkintöjä, koodisanoja tai lyhenteitä, joilla tarkennetaan asiakirjan aihealue, erityisjakelu tiedonsaantitarpeen perusteella tai käytön rajoitukset;

c) luovutettavuutta koskevia merkintöjä;

d) tarvittaessa ajankohta tai tietty tapahtuma, jonka jälkeen tietojen turvaluokka voidaan alentaa tai poistaa.

Turvaluokitusmerkintöjen lyhenteet

12. Tekstiin kuuluvien yksittäisten kappaleiden turvaluokan merkitsemiseen voidaan käyttää vakiomuotoisia turvaluokitusmerkintöjen lyhenteitä. Täydellisiä turvaluokitusmerkintöjä ei saa korvata lyhenteillä.

13. EU:n turvaluokitelluissa asiakirjoissa voidaan käyttää seuraavia vakiomuotoisia lyhenteitä, joilla ilmoitetaan alle yhden sivun mittaisten jaksojen tai tekstin osien turvaluokka:

TRES SECRET UE/EU TOP SECRET	TS-UE/EU-TS
SECRET UE/EU SECRET	S-UE/EU-S
CONFIDENTIEL UE/EU CONFIDENTIAL	C-UE/EU-C
RESTREINT UE/EU RESTRICTED	R-UE/EU-R

EU:n turvaluokiteltujen asiakirjojen tuottaminen

14. Tuotettaessa EU:n turvaluokiteltua asiakirjaa

a) turvaluokka on merkittävä selvästi jokaiselle sivulle;

b) jokainen sivu on numeroitava;

c) asiakirjassa on oltava viitenumero ja asiakohta, joka ei ole turvaluokiteltua tietoa, ellei sitä ole merkitty sellaiseksi;

d) asiakirja on päivättävä;

e) SECRET UE/EU SECRET- ja sitä korkeamman turvaluokan asiakirjojen jokaiselle sivulle on merkittävä jäljennöksen numero, jos ne on tarkoitus jakaa useampana kappaleena.

EU:n turvaluokiteltujen tietojen turvaluokan alentaminen ja poistaminen

15. Tietoja tuottaessaan luovuttajan on mahdollisuuksien mukaan ja erityisesti RESTREINT UE/EU RESTRICTED -turvaluokan tietojen osalta ilmoitettava, voidaanko EU:n turvaluokiteltujen tietojen turvaluokkaa alentaa tai turvaluokitus poistaa tiettynä päivänä tai tietyn tapahtuman jälkeen.

16. Pääsihteeristön on tarkistettava hallussaan olevat EU:n turvaluokitellut tiedot säännöllisin väliajoin sen selvittämiseksi, onko turvaluokka edelleen asianmukainen. Pääsihteeristön on perustettava järjestelmä sen luovuttamien kirjattujen EU:n turvaluokiteltujen tietojen turvaluokan tarkistamiseksi vähintään joka viides vuosi. Tarkistaminen ei ole tarpeen, jos tietojen luovuttaja on alun perin ilmoittanut, että tietojen turvaluokkaa alennetaan tai että se poistetaan automaattisesti, ja jos tiedot on merkitty tämän mukaisesti.

III EU:N TURVALUOKITELTUJEN TIETOJEN KIRJAAMINEN TURVALLISUUSSYISTÄ

17. Kaikille pääsihteeristön ja jäsenvaltioiden kansallisten hallintojen organisaatioyksiköille, joissa EU:n turvaluokiteltuja tietoja käsitellään, on määriteltävä vastaava kirjaamo sen varmistamiseksi, että tietoja käsitellään tämän päätöksen mukaisesti. Kirjaamot on perustettava liitteessä II määritellyn mukaisiksi turva-alueiksi.

18. Tässä päätöksessä kirjaamisella turvallisuussyistä, jäljempänä 'kirjaaminen', tarkoitetaan sellaisten menettelyjen soveltamista, joiden avulla turvaluokiteltujen asiakirjojen haltija voidaan selvittää milloin tahansa ja jotka tallentavat kyseisen asiakirjan elinkaaren, myös sen hävittämisen.

19. Kaikki CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeamman turvaluokan tai sitä vastaavan turvaluokan asiakirjat on kirjattava niille tarkoitetuissa kirjaamoissa, kun ne saapuvat organisaatioyksikköön tai lähtevät siitä.

20. Pääsihteeristön keskuskirjaamo pitää kirjaa kaikista neuvoston ja pääsihteeristön kolmansille valtioille ja kansainvälisille järjestöille luovuttamista turvaluokitelluista tiedoista sekä kaikista kolmansilta valtioilta tai kansainvälisiltä järjestöiltä vastaanotetuista turvaluokitelluista tiedoista.

21. Jos kyseessä on viestintä- ja tietojärjestelmä, kirjaamismenettelyt voidaan suorittaa sen omien prosessien avulla.

22. Neuvosto hyväksyy turvallisuussyistä kirjattavia EU:n turvaluokiteltuja tietoja koskevat turvallisuusperiaatteet.

TRES SECRET UE/EU TOP SECRET- turvaluokan tietojen kirjaamot

23. Jäsenvaltioihin ja pääsihteeristöön on nimettävä kirjaamo, joka toimii TRES SECRET UE/EU TOP SECRET -turvaluokan tietojen keskitettynä vastaanottaja- ja lähettäjäviranomaisena. Tarvittaessa voidaan nimetä alakirjaamoja tällaisten tietojen käsittelemiseksi kirjaamistarkoituksiin.

24. TRES SECRET UE/EU TOP SECRET -asiakirjoja ei saa toimittaa suoraan saman TRES SECRET UE /EU TOP SECRET -keskuskirjaamon alakirjaamosta toiseen tai ulkoisille kirjaamoille ilman keskuskirjaamon nimenomaista kirjallista hyväksyntää.

IV EU:N TURVALUOKITELTUJEN ASIAKIRJOJEN JÄLJENTÄMINEN JA KÄÄNTÄMINEN

25. TRES SECRET UE/EU TOP SECRET -asiakirjoja ei saa jäljentää eikä kääntää ilman niiden luovuttajan kirjallista etukäteissuostumusta.

26. Jos SECRET UE/EU SECRET- ja sitä alemman turvaluokan asiakirjojen luovuttaja ei ole kieltänyt jäljentämästä tai kääntämästä asiakirjoja, ne voidaan jäljentää tai kääntää niiden haltijan pyynnöstä.

27. Jäljennöksiin ja käännöksiin sovelletaan alkuperäistä asiakirjaa koskevia turvatoimia.

V EU:N TURVALUOKITELTUJEN TIETOJEN FYYSINEN KULJETTAMINEN

28. EU:n turvaluokiteltujen tietojen fyysiseen kuljettamiseen sovelletaan jäljempänä 30–38 kohdassa esitettyjä suojatoimenpiteitä. Jos EU:n turvaluokiteltuja tietoja siirretään sähköisillä tallennusvälineillä ja sen estämättä, mitä 9 artiklan 4 kohdassa säädetään, edellä esitettyjä suojatoimenpiteitä voidaan täydentää toimivaltaisen turvallisuusviranomaisen määräämillä asianmukaisilla teknisillä vastatoimenpiteillä, jotta minimoitaisiin katoamisen tai vaarantumisen riski.

29. Pääsihteeristön ja jäsenvaltioiden toimivaltaisten turvallisuusviranomaisten on annettava ohjeet EU:n turvaluokiteltujen tietojen kuljettamisesta tämän päätöksen säännösten mukaisesti.

Rakennuksen tai suljetun rakennusryhmän sisällä

30. Rakennuksen tai suljetun rakennusryhmän sisällä kuljetettavat EU:n turvaluokitellut tiedot on peitettävä niin, ettei niiden sisältö ole näkyvissä.

31. TRES SECRET UE/EU TOP SECRET -turvaluokan tiedot on kuljetettava rakennuksen tai suljetun rakennusryhmän sisällä sinetöidyssä kirjekuoressa, johon on merkitty vain vastaanottajan nimi.

EU:n alueella

32. EU:n alueella rakennusten tai tilojen välillä kuljetettavat EU:n turvaluokitellut tiedot on pakattava niin, että ne on suojattu luvattomalta ilmitulolta.

33. SECRET UE/EU SECRET- tai sitä alemman turvaluokan tiedot on kuljetettava fyysisesti rakennusten tai tilojen välillä EU:n alueella jollakin seuraavista tavoista:

    a) sotilaskuriirilla, valtion kuriirilla tai diplomaattikuriirilla tarvittaessa,

    b) kansallisilla postipalveluilla tai kaupallisilla kuriiripalveluilla, joilla on tarvittaessa oltava yhteisöturvallisuusselvitys kansallisten lakien ja asetusten mukaisesti,

    c) henkilökohtaisesti, jos

        i) kirjatuista EU:n turvaluokitelluista tiedoista säilytetään tieto asianmukaisessa kirjaamossa;

        ii) EU:n turvaluokitellut tiedot ovat koko ajan kuljettajansa hallussa, paitsi jos ne on tallennettu liitteessä II säädettyjen vaatimusten mukaisesti;

        iii) EU:n turvaluokiteltuja tietoja ei avata matkalla eikä lueta julkisilla paikoilla;

        iv) henkilöille selvitetään heidän turvallisuutta koskeva vastuunsa;

        v) henkilöille annetaan tarvittaessa kuriiritodistus.

34. TRES SECRET UE/EU TOP SECRET- tai sitä korkeamman turvaluokan tiedot on kuljetettava fyysisesti rakennusten tai tilojen välillä EU:n alueella tapauksen mukaan sotilaskuriirilla, valtion kuriirilla tai diplomaattikuriirilla.

EU:sta kolmanteen valtioon

35. EU:sta kolmanteen valtioon kuljetettavat EU:n turvaluokitellut tiedot on pakattava niin, että ne on suojattu luvattomalta ilmitulolta.

36. SECRET UE/EU SECRET- tai sitä alemman turvaluokan tiedot on kuljetettava fyysisesti EU:sta kolmanteen valtioon jollakin seuraavista tavoista:

    a) sotilas- tai diplomaattikuriirilla;

    b) henkilökohtaisesti, jos

        i) pakkauksessa on virallinen sinetti tai siitä käy ilmi, että kyseessä on virallinen lähetys, jolle ei tehdä tulli- tai turvallisuustarkastusta;

        ii) henkilöillä on kuriiritodistus, jossa yksilöidään pakkaus ja valtuutetaan henkilöt kuljettamaan sitä.

37. RESTREINT UE/EU RESTRICTED -turvaluokan tietoja voidaan kuljettaa myös kansallisten postipalvelujen tai kaupallisten kuriiripalvelujen välityksellä.

38. TRES SECRET UE/EU TOP SECRET -turvaluokan tiedot on kuljetettava fyysisesti EU:sta kolmanteen valtioon sotilas- tai diplomaattikuriirilla.

VI EU:N TURVALUOKITELTUJEN TIETOJEN HÄVITTÄMINEN

39. EU:n turvaluokitellut tiedot, joita ei enää tarvita, voidaan hävittää, sanotun kuitenkaan rajoittamatta arkistointia koskevia sääntöjä ja määräyksiä.

40. Asiakirjat, jotka on kirjattava 9 artiklan 2 kohdan mukaisesti, on hävitettävä niistä vastaavassa kirjaamossa niiden haltijan tai toimivaltaisen viranomaisen määräyksestä. Päiväkirjat ja muut kirjaustiedot on päivitettävä vastaavasti.

41. SECRET UE/EU SECRET - tai TRES SECRET UE/EU TOP SECRET -turvaluokan asiakirjojen hävittäminen on suoritettava todistajan läsnä ollessa. Todistajalla on oltava vähintään hävitettävän asiakirjan turvaluokkaa vastaava turvallisuusselvitys.

42. Sekä kirjaajan että todistajan, jonka on oltava paikalla, on allekirjoitettava hävittämistodistus, joka tallennetaan kirjaamoon. Kirjaamon on säilytettävä TRES SECRET UE/EU TOP SECRET -asiakirjojen hävittämistodistukset vähintään kymmenen vuoden ajan sekä CONFIDENTIEL UE/EU CONFIDENTIAL ja SECRET UE/EU SECRET -asiakirjojen hävittämistodistukset vähintään viiden vuoden ajan.

43. Turvaluokiteltujen asiakirjojen, myös RESTREINT UE/EU RESTRICTED -turvaluokan asiakirjojen, hävittämisessä on käytettävä menetelmiä, jotka vastaavat asiaankuuluvia EN- tai vastaavia standardeja tai jotka jäsenvaltiot ovat hyväksyneet kansallisten teknisten standardien mukaisesti, jotta estetään tietojen kokoaminen uudelleen kokonaan tai osittain.

44. EU:n turvaluokiteltujen tietojen tallentamiseen käytetyt atk-tallennevälineet hävitetään liitteessä IV olevan 36 kohdan mukaisesti.

VII TARKASTUKSET JA ARVIOINTIKÄYNNIT

45. "Tarkastuksella" tarkoitetaan jäljempänä

– 9 artiklan 3 kohdan ja 15 artiklan 2 kohdan e–g alakohdan mukaista tarkastusta, tai

– 12 artiklan 5 kohdan mukaista arviointikäyntiä,

jossa arvioidaan EU:n turvaluokiteltujen tietojen suojaamiseksi toteutettujen toimenpiteiden tehokkuutta.

46. Tarkastuksia tehdään muun muassa

a) sen varmistamiseksi, että tässä päätöksessä säädettyjä EU:n turvaluokiteltujen tietojen suojaamista koskevia vähimmäisvaatimuksia noudatetaan;

b) turvallisuuden ja tehokkaan riskinhallinnan merkityksen korostamiseksi tarkastetuissa yksiköissä;

c) vastatoimien suosittelemiseksi niiden erityisten vaikutusten lieventämiseksi, joita turvaluokiteltujen tietojen luottamuksellisuuden, eheyden tai käytettävyyden menetyksellä on; ja

d) turvallisuusviranomaisten jatkuvan turvallisuuskoulutuksen ja tiedotusohjelmien tehostamiseksi.

47. Neuvosto hyväksyy ennen kunkin kalenterivuoden loppua 15 artiklan 1 kohdan c alakohdassa tarkoitetun tarkastusohjelman seuraavaksi vuodeksi. Kunkin tarkastuksen ajankohdasta sovitaan kyseisen EU:n viraston tai elimen, jäsenvaltion, kolmannen valtion tai kansainvälisen järjestön kanssa.

Tarkastusten suorittaminen

48. Tarkastuksissa on käytävä läpi tarkastettavan yksikön asiaankuuluvat säännöt, määräykset ja menettelyt sekä tarkistettava, ovatko yksikön toimintatavat tässä päätöksessä ja turvaluokiteltujen tietojen vaihtoa kyseisen yksikön kanssa koskevissa säännöksissä säädettyjen vähimmäisvaatimusten mukaisia.

49. Tarkastukset on suoritettava kahdessa vaiheessa. Ennen varsinaista tarkastusta tarkastettavan yksikön kanssa on tarvittaessa pidettävä valmistelukokous. Valmistelukokouksen jälkeen tarkastusryhmän on laadittava yhteisymmärryksessä kyseisen yksikön kanssa yksityiskohtainen tarkastusohjelma, joka kattaa kaikki turvallisuuden alat. Tarkastusryhmän on päästävä kaikkiin paikkoihin, joissa EU:n turvaluokiteltuja tietoja käsitellään, erityisesti kirjaamoihin ja viestintä- ja tietojärjestelmien sijoituspaikkoihin.

50. Jäsenvaltioiden kansallisissa hallinnoissa tehtävistä tarkastuksista vastaa neuvoston pääsihteeristön ja Euroopan komission yhteinen tarkastusryhmä täydessä yhteistyössä tarkastettavan yksikön virkamiesten kanssa.

51. Kolmansissa valtioissa ja kansainvälisissä järjestöissä tehtävistä tarkastuksista vastaa neuvoston pääsihteeristön ja Euroopan komission yhteinen tarkastusryhmä täydessä yhteistyössä tarkastettavan kolmannen valtion tai kansainvälisen järjestön virkamiesten kanssa.

52. EU:n virastojen ja elinten tarkastukset suorittaa pääsihteeristön turvallisuusyksikkö käyttäen viraston tai elimen sijaintijäsenvaltion kansallisen turvallisuusviranomaisen asiantuntija-apua. Euroopan komission turvallisuusyksikkö voi osallistua toimintaan, jos se vaihtaa säännöllisesti EU:n turvaluokiteltuja tietoja kyseisen viraston tai elimen kanssa.

53. Kun tarkastuksia tehdään EU:n virastoissa ja elimissä sekä kolmansissa valtioissa ja kansainvälisissä järjestöissä, kansallisilta turvallisuusviranomaisilta pyydetään apua turvallisuuskomitean päättämien yksityiskohtaisten järjestelyjen mukaisesti.

Tarkastusraportit

54. Tarkastuksen päätteeksi tarkastetulle yksikölle on esitettävä tärkeimmät päätelmät ja suositukset. Tämän jälkeen tarkastuksesta on laadittava raportti pääsihteeristön turvallisuusviranomaisen (turvallisuusyksikön) vastuulla. Jos on ehdotettu korjaavia toimia tai annettu suosituksia, niistä on annettava raportissa riittävästi yksityiskohtaisia tietoja tehtyjen päätelmien tueksi. Raportti on toimitettava tarkastetun yksikön asianmukaiselle vastuuhenkilölle.

55. Jäsenvaltioiden kansallisissa hallinnoissa suoritettavien tarkastusten osalta

a) tarkastusraporttiluonnos toimitetaan asianomaiselle kansalliselle turvallisuusviranomaiselle, joka tarkistaa, että sen sisältämät tiedot ovat oikeita ja että siinä on korkeintaan RESTREINT UE/EU RESTRICTED -turvaluokkaan kuuluvia tietoja;

b) jos asianomaisen jäsenvaltion kansallinen turvallisuusviranomainen ei ole vaatinut yleisestä jakelusta pidättymistä, tarkastusraportit jaetaan turvallisuuskomitean jäsenille ja Euroopan komission turvallisuusyksikölle; raportin turvaluokan on oltava RESTREINT UE/EU RESTRICTED.

Pääsihteeristön turvallisuusviranomaisen (turvallisuusyksikön) vastuulla laaditaan säännöllisin väliajoin raportti, jossa selostetaan tietyn jakson aikana jäsenvaltioissa suoritetuista tarkastuksista saadut kokemukset.

56. Arviointikäynneistä kolmansiin valtioihin ja kansainvälisiin järjestöihin laadittu raportti jaetaan turvallisuuskomitean jäsenille ja Euroopan komission turvallisuusyksikölle. Raportin turvaluokan on oltava vähintään RESTREINT UE/EU RESTRICTED. Mahdollisten korjaavien toimien toteuttaminen tarkistetaan seurantakäynnillä, ja siitä raportoidaan turvallisuuskomitealle.

57. Raportti EU:n virastoihin ja elimiin tehdyistä tarkastuksista jaetaan turvallisuuskomitean jäsenille ja Euroopan komission turvallisuusyksikölle. Tarkastusraporttiluonnos toimitetaan asianomaiselle virastolle tai elimelle, joka tarkistaa, että sen sisältämät tiedot ovat oikeita ja että siinä on korkeintaan RESTREINT UE/EU RESTRICTED -turvaluokkaan kuuluvia tietoja. Mahdollisten korjaavien toimien toteuttaminen tarkistetaan seurantakäynnillä, ja siitä raportoidaan turvallisuuskomitealle.

58. Pääsihteeristön turvallisuusviranomainen suorittaa säännöllisin väliajoin pääsihteeristön organisaatioyksiköiden tarkastuksia 46 kohdan soveltamiseksi.

Tarkastusluettelo

59. Pääsihteeristön turvallisuusviranomainen (turvallisuusyksikkö) laatii ja pitää ajan tasalla luettelon kohteista, jotka on tarkastettava tarkastuksen yhteydessä. Tarkastusluettelo on toimitettava turvallisuuskomitealle.

60. Tarkastusluettelon täydentämiseen tarvittavat tiedot on varsinkin tarkastuksen aikana hankittava tarkastettavan yksikön turvallisuushallinnolta. Kun tarkastusluetteloon on lisätty yksityiskohtaiset vastaukset, sille on määriteltävä turvaluokka tarkastetun yksikön suostumuksella. Luetteloa ei liitetä osaksi tarkastusraporttia.

VIESTINTÄ- JA TIETOJÄRJESTELMISSÄ KÄSITELTÄVIEN EU:N TURVALUOKITELTUJEN TIETOJEN SUOJAAMINEN

I JOHDANTO

1. Tässä liitteessä vahvistetaan 10 artiklan täytäntöönpanosäännökset.

2. Seuraavat tietojen turvaamisen ominaisuudet ja periaatteet ovat olennaisia operaatioiden turvallisuuden ja toimivuuden kannalta viestintä- ja tietojärjestelmissä:

Aitous:	tae siitä, että tiedot ovat aitoja ja vilpittömistä lähteistä;
Käytettävyys:	ominaisuus, että tiedot ovat pyynnöstä valtuutetun yksikön saatavilla ja käytettävissä;
Luottamuksellisuus:	ominaisuus, että tietoja ei paljasteta sivullisille henkilöille, yksiköille eikä prosesseille;
Eheys:	ominaisuus, että tietojen ja resurssien oikeellisuus ja täydellisyys turvataan;
Kiistämättömyys:	kyky todistaa tietyn toimen tai tapahtuman olemassaolo niin, ettei tapahtumaa tai toimea voida myöhemmin kiistää.

II TIEDONTURVAAMISPERIAATTEET

3. Jäljempänä esitetyt säännökset muodostavat kaikkien EU:n turvaluokiteltuja tietoja käsittelevien viestintä- ja tietojärjestelmien turvallisuuden lähtökohdan. Säännösten täytäntöönpanoa koskevat yksityiskohtaiset vaatimukset määritellään tietojen turvaamista koskevissa turvallisuusperiaatteissa ja turvallisuutta koskevissa suuntaviivoissa.

Turvallisuusriskien hallinta

4. Turvallisuusriskien hallinnan on oltava erottamaton osa viestintä- ja tietojärjestelmän määrittelyä, kehittämistä, käyttöä ja ylläpitoa. Riskinhallinta (arviointi, käsittely, hyväksyminen ja viestintä) on toteutettava iteroivana prosessina, jossa järjestelmän omistajien edustajien, hankkeesta vastaavien viranomaisten, toiminnasta vastaavien viranomaisten ja turvallisuusjärjestelyt hyväksyvien viranomaisten on osallistuttava toteuttamiseen, ja siinä on käytettävä vakiintunutta, avointa ja täysin ymmärrettävää riskinarviointiprosessia. Viestintä- ja tietojärjestelmän laajuus ja resurssit on määriteltävä selkeästi riskinhallintaprosessin aluksi.

5. Toimivaltaisten viranomaisten on tarkasteltava viestintä- ja tietojärjestelmiin mahdollisesti kohdistuvia uhkia ja pidettävä yllä ajantasaisia ja tarkkoja uhka-arvioita, jotka perustuvat ajankohtaiseen toimintaympäristöön. Niiden on jatkuvasti päivitettävä haavoittuvuusasioita koskevia tietojaan ja tarkistettava säännöllisin väliajoin haavoittuvuusarviota mukautuakseen muuttuvaan tietotekniikkaympäristöön.

6. Turvallisuusriskin käsittelyllä on pyrittävä toteuttamaan turvatoimien yhdistelmä, jolla saadaan aikaan tyydyttävä tasapaino käyttäjien vaatimusten, kustannusten ja turvallisuuteen kohdistuvan jäännösriskin välillä.

7. Asiaankuuluvan turvallisuusjärjestelyt hyväksyvän viranomaisen viestintä- ja tietojärjestelmän hyväksymistä varten määrittämät erityiset vaatimukset, laajuus ja yksityiskohtaisuus on suhteutettava arvioituun riskiin ottaen huomioon kaikki asiaankuuluvat tekijät, myös viestintä- ja tietojärjestelmässä käsiteltyjen EU:n turvaluokiteltujen tietojen turvaluokka. Hyväksyntään on liitettävä vastaavan viranomaisen virallinen lausunto jäännösriskistä ja sen hyväksymisestä.

Viestintä- ja tietojärjestelmän turvallisuus koko elinkaaren ajan

8. Turvallisuuden varmistamista on pidettävä vaatimuksena koko viestintä- ja tietojärjestelmän elinkaaren ajan sen alullepanosta käytöstä poistamiseen.

9. Elinkaaren kussakin vaiheessa on määriteltävä kunkin viestintä- ja tietojärjestelmään osallistuvan toimijan tehtävät ja toimijoiden vuorovaikutus järjestelmän turvallisuuden kannalta.

10. Viestintä- ja tietojärjestelmien turvallisuus, myös niiden tekniset ja muut kuin tekniset turvatoimet, on testattava hyväksymisprosessin aikana sen varmistamiseksi, että asianmukainen turvaamistaso saavutetaan, ja sen tarkistamiseksi, että ne on moitteettomasti toteutettu, integroitu ja konfiguroitu.

11. Turvallisuutta koskevat arvioinnit, tarkastukset ja uudelleentarkastelut on suoritettava määräajoin viestintä- ja tietojärjestelmän toiminnan ja huollon aikana sekä poikkeuksellisten tilanteiden ilmetessä.

12. Viestintä- ja tietojärjestelmän turvallisuusasiakirjojen on kehityttävä sen elinkaaren aikana erottamattomana osana muutosten ja asetusten hallintaprosessia.

Parhaat toimintatavat

13. Pääsihteeristön ja jäsenvaltioiden on tehtävä yhteistyötä parhaiden toimintatapojen kehittämiseksi viestintä- ja tietojärjestelmissä käsiteltävien EU:n turvaluokiteltujen tietojen suojaamista varten. Parhaita toimintatapoja koskevissa suuntaviivoissa on vahvistettava viestintä- ja tietojärjestelmiä koskevat tekniset, fyysiset, organisatoriset ja menettelyyn liittyvät turvatoimet, joiden tehokkuus tiettyjen uhkien ja haavoittuvuuden torjumisessa on todistettu.

14. Viestintä- ja tietojärjestelmissä käsiteltävien EU:n turvaluokiteltujen tietojen suojaamisessa on hyödynnettävä tietovarmuuteen EU:ssa ja sen ulkopuolella osallistuvien yksiköiden kokemuksia.

15. Parhaiden toimintatapojen levittämisen ja niiden myöhemmän täytäntöönpanon on edesautettava yhtäläisen turvaamistason aikaansaamista pääsihteeristössä ja jäsenvaltioissa käytettävissä eri viestintä- ja tietojärjestelmissä, joissa käsitellään EU:n turvaluokiteltuja tietoja.

Syvyyssuuntainen turvallisuus

16. Viestintä- ja tietojärjestelmiin kohdistuvan riskin vähentämiseksi on toteutettava joukko teknisiä ja muita kuin teknisiä turvatoimia, joilla järjestetään monitasoinen puolustus. Tasoja ovat

a) *ennaltaehkäisy*: turvatoimet, joilla pyritään saamaan mahdolliset viholliset luopumaan viestintä- ja tietojärjestelmään kohdistuvan hyökkäyksen suunnittelusta;

b) *estäminen*: turvatoimet, joilla pyritään vaikeuttamaan hyökkäystä viestintä- ja tietojärjestelmää vastaan tai estämään se;

c) *havaitseminen*: turvatoimet, joilla pyritään paljastamaan hyökkäys viestintä- ja tietojärjestelmää vastaan;

d) *vastustuskyky*: turvatoimet, joilla pyritään rajoittamaan hyökkäys mahdollisimman pieneen osaan tietoja tai viestintä- ja tietojärjestelmän resursseja ja estämään muut vahingot; ja

e) *vaarantumistilanteen korjaaminen*: turvatoimet, joilla pyritään viestintä- ja tietojärjestelmän suojatun tilanteen palauttamiseen.

Tällaisten turvatoimien pakollisuusaste on määriteltävä riskinarvioinnin perusteella.

17. Toimivaltaisten viranomaisten on varmistettava, että ne voivat käsitellä poikkeuksellisia tapahtumia, jotka saattavat ulottua organisaatioiden ja kansallisten rajojen ulkopuolelle, jotta voidaan koordinoida vastatoimia ja jakaa tapahtumia ja niihin liittyviä riskejä koskevat tiedot kolmansien osapuolten kanssa (tietotekniset hätävalmiudet).

Vähimmäistoimintojen ja pienimmän mahdollisen etuoikeuden periaate

18. Tarpeettoman riskin välttämiseksi on pantava täytäntöön vain käyttövaatimusten kannalta olennaiset toiminnot, laitteet ja palvelut.

19. Viestintä- ja tietojärjestelmän käyttäjille ja automaattisille prosesseille on annettava vain ne tiedot, etuoikeudet tai valtuutukset, jotka ovat niiden tehtävien suorittamiseksi välttämättömiä, jotta rajoitettaisiin onnettomuuksista, virheistä tai järjestelmän resurssien luvattomasta käytöstä mahdollisesti aiheutuvia vahinkoja.

20. Jos viestintä- ja tietojärjestelmässä on tarpeen suorittaa kirjaamismenettelyjä, ne on tarkistettava osana hyväksymisprosessia.

Tietojen turvaamisen merkityksen tiedostaminen

21. Tietoisuus riskeistä ja käytettävissä olevista turvatoimista on viestintä- ja tietojärjestelmien turvallisuuden tärkein puolustamiskeino. Viestintä- ja tietojärjestelmien elinkaareen osallistuvien kaikkien henkilöiden, myös käyttäjien, on erityisesti ymmärrettävä

    a) että turvallisuuden vaarantuminen voi merkittävästi vahingoittaa viestintä- ja tietojärjestelmiä;

    b) että yhteenliitettävyydestä ja keskinäisestä riippuvuudesta saattaa aiheutua vahinkoa muille; ja

    c) henkilökohtainen vastuunsa ja tilivelvollisuutensa viestintä- ja tietojärjestelmien turvallisuudesta sen mukaan, mikä on heidän tehtävänsä järjestelmissä ja prosesseissa.

22. Sen varmistamiseksi, että turvallisuuteen liittyvät tehtävät ymmärretään, koko henkilöstölle, myös johtohenkilöstölle ja viestintä- ja tietojärjestelmien käyttäjille, on annettava pakollinen tiedonturvaamis- ja tietoisuuden lisäämiskoulutus.

Tietoturvallisuustuotteiden arviointi ja hyväksyntä

23. Turvatoimilta vaadittava varmuusaste, joka määritellään turvaamistasona, on vahvistettava riskinhallintaprosessin tulosten perusteella asiaankuuluvien turvallisuusperiaatteiden ja turvallisuutta koskevien suuntaviivojen mukaisesti.

24. Turvaamistaso on tarkistettava käyttämällä kansainvälisesti tunnustettuja tai kansallisesti hyväksyttyjä prosesseja ja menettelytapoja. Näitä ovat pääasiassa arviointi, tarkastukset ja auditointi.

25. Jäsenvaltion salauslaitteiden hyväksyntäviranomaisen on arvioitava ja hyväksyttävä EU:n turvaluokiteltujen tietojen suojaamisessa käytettävät salaustuotteet.

26. Ennen kuin salaustuotteiden hyväksymistä suositellaan neuvostolle tai pääsihteerille 10 artiklan 6 kohdan mukaisesti, niiden on läpäistävä jonkin sellaisen jäsenvaltion asianmukaisesti pätevän viranomaisen (AQUA-viranomaisen) ulkopuolinen arviointi, joka ei osallistu laitteiden suunnitteluun eikä valmistukseen. Ulkopuoliselta arvioinnilta edellytettävä yksityiskohtaisuus riippuu korkeimmasta turvaluokasta, johon kuuluvia EU:n turvaluokiteltuja tietoja kyseisillä tuotteilla on tarkoitus suojata. Neuvosto hyväksyy salaustuotteiden arviointia ja hyväksyntää koskevat turvallisuusperiaatteet.

27. Jos se on perusteltua erityisistä toiminnallisista syistä, neuvosto tai tapauksen mukaan pääsihteeri voi turvallisuuskomitean suosituksesta jättää soveltamatta 25 tai 26 kohdan mukaisia vaatimuksia ja myöntää tilapäisen hyväksynnän erikseen määritellyksi ajaksi 10 artiklan 6 kohdassa säädetyn menettelyn mukaisesti.

28. AQUA-viranomaisen on oltava jäsenvaltion salauslaitteiden hyväksyntäviranomainen, joka on neuvoston vahvistamin perustein hyväksytty suorittamaan EU:n turvaluokiteltujen tietojen suojaamiseen tarkoitettujen salaustuotteiden toinen arviointi.

29. Neuvosto hyväksyy sellaisten tietoturvallisuustuotteiden luokittelua ja hyväksyntää koskevat turvallisuusperiaatteet, jotka eivät ole salaustuotteita.

Tietojen lähettäminen turva-alueilla

30. Sen estämättä, mitä tässä päätöksessä säädetään, jos EU:n turvaluokiteltujen tietojen lähettäminen tapahtuu turva-alueilla, salaamatonta jakelua tai alemman tason salausta voidaan käyttää riskinhallintaprosessin tulosten perusteella ja turvallisuusjärjestelyt hyväksyvän viranomaisen luvalla.

Viestintä- ja tietojärjestelmien suojattu yhteenliittäminen

31. Tässä päätöksessä yhteenliittämisellä tarkoitetaan kahden tai useamman tietotekniikkajärjestelmän välitöntä liittämistä toisiinsa tietojen ja muiden tietoresurssien (esimerkiksi viestinnän) jakamiseksi yksi- tai monisuuntaisesti.

32. Viestintä- ja tietojärjestelmän on käsiteltävä kaikkia siihen liitettyjä tietotekniikkajärjestelmiä epäluotettavina ja toteutettava suojatoimia, joilla valvotaan turvaluokiteltujen tietojen vaihtoa.

33. Liitettäessä viestintä- ja tietojärjestelmä toiseen tietotekniikkajärjestelmään seuraavien perusvaatimusten on täytyttävä:

    a) toimivaltaisten viranomaisten on todettava ja hyväksyttävä yhteenliittämistä koskevat toiminta- tai käyttövaatimukset;

b) yhteenliittämisen on käytävä läpi riskinhallinta- ja hyväksyntäprosessi, ja se on hyväksytettävä toimivaltaisella turvallisuusjärjestelyt hyväksyvällä viranomaisella; ja

c) kaikkien viestintä- ja tietojärjestelmien turva-alueella on toteutettava rajojen suojauspalvelut.

34. Hyväksytyn viestintä- ja tietojärjestelmän ja suojaamattoman tai julkisen verkon välillä ei saa olla yhteenliitäntää, paitsi jos viestintä- ja tietojärjestelmään on asennettu tarkoitusta varten hyväksytyt rajojen suojauspalvelut viestintä- ja tietojärjestelmän ja suojaamattoman tai julkisen verkon välille. Toimivaltaisen tiedonturvaamisviranomaisen on tarkistettava tällaisten yhteenliitäntöjen turvatoimet, ja toimivaltaisen turvallisuusjärjestelyt hyväksyvän viranomaisen on hyväksyttävä ne.

Jos suojaamatonta tai julkista verkkoa käytetään ainoastaan siirtovälineenä ja tiedot on salattu 10 artiklan mukaisesti hyväksytyllä salaustuotteella, tällaista liitäntää ei pidetä yhteenliitäntänä.

35. TRES SECRET UE/EU TOP SECRET -turvaluokiteltujen tietojen käsittelyyn hyväksytyn viestintä- ja tietojärjestelmän välitön tai porrastettu yhteenliitäntä suojaamattoman tai julkisen verkon kanssa on kiellettyä.

Atk-tallennevälineiden hävittäminen

36. TRES SECRET UE/EU TOP SECRET - turvaluokan EU:n turvaluokiteltujen tietojen säilyttämiseen käytettyjen atk-tallennevälineiden turvaluokkaa ei saa poistaa eikä niitä saa käyttää uudelleen. SECRET UE/EU SECRET- tai sitä alemman turvaluokan EU:n turvaluokiteltujen tietojen säilyttämiseen käytettyjä atk-tallennevälineitä voidaan käyttää uudelleen, niiden turvaluokkaa voidaan alentaa tai se voidaan poistaa toimivaltaisen turvallisuusviranomaisen hyväksymien menettelyjen mukaisesti. Jos atk-tallennevälineiden turvaluokkaa ei voida poistaa tai niitä ei voida käyttää uudelleen, ne on hävitettävä toimivaltaisen turvallisuusviranomaisen hyväksymien menettelyjen mukaisesti.

Kiireelliset olosuhteet

37. Sen estämättä, mitä tässä päätöksessä säädetään, jäljempänä kuvattuja erityismenettelyjä voidaan soveltaa hätätapauksessa, esimerkiksi kriisitilanteen uhatessa tai toteutuessa, konfliktissa, sotatilanteissa taikka poikkeuksellisissa toimintaolosuhteissa.

38. EU:n turvaluokiteltujen tietojen lähettämisessä voidaan käyttää alempaa turvaluokkaa varten hyväksyttyjä salaustuotteita tai ne voidaan lähettää ilman salausta toimivaltaisen viranomaisen suostumuksella, jos mahdollinen viivästyminen aiheuttaisi selvästi suuremman vahingon kuin turvaluokitellun aineiston mahdollisen paljastumisen aiheuttama vahinko ja jos

– lähettäjällä ja vastaanottajalla ei ole vaadittua salauslaitetta tai ei mitään salauslaitetta;

JA

– turvaluokiteltua aineistoa ei voida toimittaa perille ajoissa muulla tavoin.

39. Edellä olevassa 38 kohdassa esitetyissä olosuhteissa lähetetyissä turvaluokitelluissa tiedoissa ei saa olla mitään merkintöjä eikä mainintoja, jotka erottavat ne turvaluokittelemattomista tiedoista tai tiedoista, jotka voidaan suojata käytettävissä olevalla salaustuotteella. Tietojen vastaanottajille on ilmoitettava turvaluokasta viipymättä muulla tavoin.

40. Jos 38 kohtaa sovelletaan, toimivaltaiselle viranomaiselle ja turvallisuuskomitealle on annettava asiasta raportti.

III TIEDONTURVAAMISTEHTÄVÄT JA VIRANOMAISET

41. Jäsenvaltioiden ja pääsihteeristön on perustettava alla olevat tiedonturvaamistehtävät. Näiden tehtävien hoitamista varten ei ole tarpeen perustaa erillisiä organisaatioyksiköitä. Niillä on oltava erilliset toimeksiannot, mutta ne voidaan yhdistää samaan organisaatioyksikköön tai hajottaa eri organisaatioyksiköille edellyttäen, että sisäiset eturistiriidat tai tehtävien ristiriitaisuus vältetään.

Tiedonturvaamisviranomainen

42. Tiedonturvaamisviranomainen huolehtii

a) tietojen turvaamista koskevien turvallisuusperiaatteiden ja turvallisuutta koskevien suuntaviivojen laatimisesta sekä niiden toimivuuden ja asianmukaisuuden valvomisesta;

b) salaustuotteisiin liittyvien teknisten tietojen tallessa pitämisestä ja hallinnoinnista;

c) sen varmistamisesta, että EU:n turvaluokiteltujen tietojen suojaamiseksi valitut tiedonturvaamistoimenpiteet ovat niiden kelpoisuutta ja valintaa koskevien asiaankuuluvien periaatteiden mukaisia;

d) sen varmistamisesta, että salaustuotteiden valinnassa noudatetaan niiden kelpoisuutta ja valintaa koskevia periaatteita;

e) tietojen turvaamista koskevan koulutuksen ja valistuksen koordinoinnista;

f) järjestelmän toimittajan, turvallisuusalan toimijoiden ja käyttäjien edustajien kuulemisesta tietojen turvaamista koskevien turvallisuusperiaatteiden ja teknisten suuntaviivojen osalta; ja

g) sen varmistamisesta, että tiedonturvaamisasioita käsittelevän turvallisuuskomitean asiantuntijakokoonpanon käytettävissä on riittävä asiantuntemus.

TEMPEST-viranomainen

43. TEMPEST-viranomainen vastaa siitä, että viestintä- ja tietojärjestelmät ovat TEMPEST-periaatteiden ja -suuntaviivojen mukaisia. Se hyväksyy TEMPEST-vastatoimet laitteistoille ja tuotteille, joilla EU:n turvaluokitellut tiedot suojataan määrättyyn turvaluokkaan asti tuotteen käyttöympäristössä.

Salauslaitteiden hyväksyntäviranomainen

44. Salauslaitteiden hyväksyntäviranomainen vastaa sen varmistamisesta, että jäsenvaltion salaustuotteet ovat kansallisten salausperiaatteiden mukaisia tai että pääsihteeristön salaustuotteet ovat neuvoston salausperiaatteiden mukaisia. Se hyväksyy salaustuotteen, jolla EU:n turvaluokitellut tiedot suojataan määrättyyn turvaluokkaan asti tuotteen käyttöympäristössä. Jäsenvaltioiden osalta salauslaitteiden hyväksyntäviranomainen vastaa lisäksi salaustuotteiden arvioinnista.

Salatun aineiston jakelusta vastaava viranomainen

45. Salaisen aineiston jakelusta vastaava viranomainen huolehtii

a) EU:n salausaineiston hallinnoinnista ja kirjanpidosta;

b) sen varmistamisesta, että EU:n salausaineiston kirjanpidossa, suojatussa käsittelyssä, säilyttämisessä ja jakelussa käytetään asianmukaisia menettelyjä ja että sitä varten on perustettu asianmukaiset kanavat; ja

c) EU:n salausaineiston lähettämisestä sitä käyttäville henkilöille tai yksiköille tai sitä käyttäviltä henkilöiltä tai yksiköiltä.

Turvallisuusjärjestelyt hyväksyvä viranomainen

46. Kunkin järjestelmän turvallisuusjärjestelyt hyväksyvä viranomainen huolehtii

a) sen varmistamisesta, että viestintä- ja tietojärjestelmä on asiaankuuluvien turvallisuusperiaatteiden ja turvallisuutta koskevien suuntaviivojen mukainen, lausunnon antamisesta viestintä- ja tietojärjestelmän hyväksymisestä, minkä nojalla EU:n turvaluokiteltuja tietoja voidaan käsitellä tiettyyn turvaluokkaan asti järjestelmän käyttöympäristössä; lausunnossa on ilmoitettava hyväksynnän ehdot ja edellytykset sekä perusteet, joiden täyttyessä järjestelmä on hyväksyttävä uudelleen;

b) asiaankuuluvien periaatteiden mukaisen turvallisuusjärjestelyjen hyväksymisprosessin perustamisesta sekä alaisuudessaan olevien viestintä- ja tietojärjestelmien hyväksymisedellytysten ilmoittamisesta selkeästi;

c) sellaisen turvallisuushyväksyntästrategian määrittelemisestä, jossa määritetään hyväksymisprosessin yksityiskohtaisuus niin, että se on suhteutettu vaadittuun turvaamistasoon;

d) turvallisuuteen liittyvien asiakirjojen tarkastelusta ja hyväksymisestä, riskinhallintaa ja jäännösriskiä koskevat lausunnot, järjestelmäkohtaiset turvavaatimusilmoitukset (jäljempänä "SSRS"), turvallisuusjärjestelyjen täytäntöönpanon tarkistusasiakirjat ja turvamenettelyt (jäljempänä "SecOPs") mukaan luettuina, ja sen varmistamisesta, että ne ovat neuvoston turvallisuussääntöjen ja -periaatteiden mukaisia;

e) viestintä- ja tietojärjestelmiin liittyvien turvatoimien täytäntöönpanon tarkistamisesta tekemällä tai teettämällä turvallisuutta koskevia arviointeja, tarkastuksia tai uudelleentarkasteluja;

f) viestintä- ja tietojärjestelmään liittyvien arkaluonteisten tehtävien turvallisuusvaatimusten (esimerkiksi henkilöturvallisuusselvitysten tasojen) määrittelemisestä;

g) viestintä- ja tietojärjestelmän turvallisuuden varmistamiseen käytettyjen hyväksyttyjen salaus- ja TEMPEST-tuotteiden valinnan vahvistamisesta;

h) viestintä- ja tietojärjestelmän muihin viestintä- ja tietojärjestelmiin liittämisen hyväksymisestä tai tapauksen mukaan osallistumisesta sen yhteiseen hyväksymiseen; ja

i) järjestelmän toimittajan, turvallisuusalan toimijoiden ja käyttäjien edustajien kuulemisesta turvallisuusriskien hallinnasta, erityisesti jäännösriskistä, ja hyväksymislausunnon ehdoista ja edellytyksistä.

47. Pääsihteeristön turvallisuusjärjestelyt hyväksyvä viranomainen vastaa kaikkien pääsihteeristön toimivallan puitteissa käytettävien viestintä- ja tietojärjestelmien hyväksymisestä.

48. Jäsenvaltion asiaankuuluva turvallisuusjärjestelyt hyväksyvä viranomainen vastaa jäsenvaltion toimivallan puitteissa käytettävien viestintä- ja tietojärjestelmien ja niiden osien hyväksymisestä.

49. Yhteinen turvallisuusjärjestelyjen hyväksymislautakunta vastaa sekä pääsihteeristön että jäsenvaltioiden turvallisuusjärjestelyt hyväksyvien viranomaisten toimivallan puitteissa käytettävien viestintä- ja tietojärjestelmien hyväksymisestä. Lautakunnan kokoonpanossa on turvallisuusjärjestelyt hyväksyvän viranomaisen edustajia kustakin jäsenvaltiosta, ja Euroopan komission turvallisuusjärjestelyt hyväksyvän viranomaisen edustaja osallistuu sen kokouksiin. Muut yhteisöt, joilla on solmuja viestintä- ja tietojärjestelmässä, kutsutaan kokouksiin, kun niissä käsitellään kyseistä järjestelmää.

Lautakunnan puheenjohtajana toimii pääsihteeristön turvallisuusjärjestelyt hyväksyvän viranomaisen edustaja. Lautakunta tekee päätöksensä niiden toimielinten, jäsenvaltioiden ja muiden yksiköiden, joilla on solmuja viestintä- ja tietojärjestelmässä, turvallisuusjärjestelyt hyväksyvien viranomaisten edustajien konsensuksella. Se antaa määräajoin toiminnastaan raportteja turvallisuuskomitealle ja ilmoittaa sille kaikista hyväksymislausunnoista.

Operatiivinen tiedonturvaamisviranomainen

50. Kunkin järjestelmän operatiivinen tiedonturvaamisviranomainen huolehtii

a) turvallisuusasiakirjojen laatimisesta turvallisuusperiaatteiden ja turvallisuutta koskevien suuntaviivojen mukaisesti, erityisesti SSRS:n ja siihen kuuluvan jäännösriskiä koskevan lausunnon, SecOPs-turvamenettelyjen ja viestintä- ja tietojärjestelmän hyväksymisprosessiin kuuluvan salaussuunnitelman laatimisesta;

b) osallistumisesta järjestelmäkohtaisten teknisten turvatoimien, laitteiden ja ohjelmistojen valintaan ja testaamiseen niiden täytäntöönpanon valvomiseksi ja sen varmistamiseksi, että ne on asennettu ja konfiguroitu turvallisesti ja että niitä ylläpidetään asiaankuuluvien turvallisuusasiakirjojen mukaisesti;

c) osallistumisesta TEMPEST-turvatoimien ja -laitteiden valintaan, jos sitä edellytetään SSRS:ssä, ja sen varmistamisesta, että laitteet on asennettu turvallisesti ja että niitä ylläpidetään yhteistyössä TEMPEST-viranomaisen kanssa;

d) SecOps-menettelyjen täytäntöönpanon ja soveltamisen valvomisesta, jolloin operatiivinen turvallisuusvastuu voidaan tarvittaessa siirtää järjestelmän omistajalle;

e) salaustuotteiden hallinnoinnista ja käsittelystä, salausvälineiden ja valvottujen esineiden hallussapidon varmistamisesta ja tarvittaessa salauksessa käytettävien muuttujien generoinnin varmistamisesta;

f) turvallisuusanalyysien tarkistusten ja testien suorittamisesta erityisesti turvallisuusjärjestelyt hyväksyvän viranomaisen vaatimien asiaankuuluvien riskiraporttien laatimiseksi;

g) viestintä- ja tietojärjestelmäkohtaisen tiedonturvaamiskoulutuksen antamisesta;

h) viestintä- ja tietojärjestelmäkohtaisten turvatoimien toteuttamisesta ja käytöstä.

YHTEISÖTURVALLISUUS

I JOHDANTO

1. Tässä liitteessä vahvistetaan 11 artiklan täytäntöönpanosäännökset. Siinä vahvistetaan yleiset turvallisuussäännökset, joita sovelletaan yrityksiin tai muihin yhteisöihin sopimusta edeltävissä neuvotteluissa ja pääsihteeristön tekemien turvaluokiteltujen sopimusten koko elinkaaren ajan.

2. Neuvosto hyväksyy yhteisöturvallisuutta koskevat periaatteet, joissa korostetaan erityisesti yhteisöturvallisuusselvitystä, turvallisuutta koskevia lisälausekkeita, vierailuja sekä EU:n turvaluokiteltujen tietojen lähettämistä ja kuljettamista koskevia yksityiskohtaisia vaatimuksia.

II TURVALUOKITELLUN SOPIMUKSEN TURVALLISUUTTA KOSKEVAT OSAT

Turvaluokitusopas

3. Ennen tarjouskilpailun käynnistämistä tai turvaluokitellun sopimuksen tekemistä hankeviranomaisena toimivan pääsihteeristön on määriteltävä tarjouksen tekijöille ja hankeosapuolille toimitettavien tietojen turvaluokka sekä hankeosapuolen tuottamien tietojen turvaluokka. Pääsihteeristön on sitä varten laadittava turvaluokitusopas, jota noudatetaan sopimuksen toimeenpanossa.

4. Turvaluokitellun sopimuksen eri osien turvaluokan määrittämiseksi sovelletaan seuraavia periaatteita:

a) turvaluokitusopasta laatiessaan pääsihteeristön on otettava huomioon kaikki asiaankuuluvat turvallisuusnäkökohdat, mukaan lukien turvaluokka, jonka tietojen alkuperäinen luovuttaja on antanut niille ja hyväksynyt myös sopimuksen osalta;

b) koko sopimuksen turvaluokka ei voi olla alempi kuin sen minkä tahansa osan korkein turvaluokka; ja

c) pääsihteeristön on tarvittaessa oltava yhteydessä jäsenvaltioiden kansallisiin tai nimettyihin turvallisuusviranomaisiin tai muuhun asianomaiseen toimivaltaiseen turvallisuusviranomaiseen siinä tapauksessa, että sopimusta toimeenpantaessa hankeosapuolten tuottamien tai niille toimitettujen tietojen turvaluokkaa muutetaan ja että turvaluokitusoppaaseen tehdään tämän vuoksi muutoksia.

Turvallisuutta koskeva lisälauseke

5. Sopimuskohtaiset turvallisuusvaatimukset on ilmoitettava turvallisuutta koskevassa lisälausekkeessa. Turvallisuutta koskevan lisälausekkeen on tarvittaessa sisällettävä turvaluokitusopas, ja sen on oltava erottamaton osa turvaluokiteltua sopimusta tai alihankintasopimusta.

6. Turvallisuutta koskevassa lisälausekkeessa on oltava määräykset, joiden mukaan hankeosapuolen ja/tai alihankkijan on noudatettava tässä päätöksessä säädettyjä vähimmäisvaatimuksia. Näiden vähimmäisvaatimusten noudattamatta jättäminen voi olla riittävä peruste sopimuksen irtisanomiselle.

Ohjelman tai hankkeen turvallisuusohjeet

7. EU:n turvaluokiteltuihin tietoihin pääsyä tai tietojen käsittelyä tai säilyttämistä edellyttävien ohjelmien tai hankkeiden soveltamisalasta riippuen niiden hallinnointia varten nimetty hankeviranomainen voi laatia niitä koskevat erityiset turvallisuusohjeet. Ohjelman tai hankkeen turvallisuusohjeille on saatava jäsenvaltioiden kansallisten tai nimettyjen turvallisuusviranomaisten tai muun ohjelmaan tai hankkeeseen osallistuvan toimivaltaisen turvallisuusviranomaisen hyväksyntä, ja niihin voi sisältyä muitakin turvallisuusvaatimuksia.

III YHTEISÖTURVALLISUUSSELVITYS

8. Yhteisöturvallisuusselvityksen myöntää jäsenvaltion kansallinen tai nimetty turvallisuusviranomainen tai muu toimivaltainen turvallisuusviranomainen kansallisten lakien ja asetusten mukaisena osoituksena siitä, että yritys tai muu yhteisö pystyy suojaamaan asianomaiseen turvaluokkaan kuuluvat EU:n turvaluokitellut tiedot toimitiloissaan. Yhteisöturvallisuusselvitys on esitettävä hankeviranomaisena toimivalle pääsihteeristölle ennen kuin hankeosapuolelle tai alihankkijalle taikka mahdolliselle hankeosapuolelle tai alihankkijalle voidaan luovuttaa EU:n turvaluokiteltuja tietoja tai myöntää pääsy niihin.

9. Asiaankuuluvan kansallisen tai nimetyn turvallisuusviranomaisen on yhteisöturvallisuusselvityksen myöntämisen yhteydessä vähintään

   a) arvioitava yrityksen tai muun yhteisön eheys;

   b) arvioitava omistajuutta, valvontaa tai alttiutta epäilyttäville vaikutteille, joita voidaan pitää turvallisuusriskinä;

   c) tarkistettava, että yritys tai muu yhteisö on ottanut toimitilassa käyttöön turvallisuusjärjestelmän, joka kattaa kaikki asianmukaiset CONFIDENTIEL UE/EU CONFIDENTIAL tai SECRET UE/EU SECRET- turvaluokan tietojen tai aineistojen suojaamisen edellyttämät turvatoimet tässä päätöksessä säädettyjen vähimmäisvaatimusten mukaisesti;

   d) tarkistettava, että johtohenkilöstön, omistajien ja työntekijöiden, joiden tehtävät edellyttävät pääsyä CONFIDENTIEL UE/EU CONFIDENTIAL tai SECRET UE/EU SECRET- turvaluokkaan kuuluviin tietoihin, henkilöturvallisuus on selvitetty tämän päätöksen liitteessä I olevien vaatimusten mukaisesti;

   e) tarkistettava, että yritys tai muu yhteisö on nimennyt yhteisöturvallisuuspäällikön, joka on vastuussa yhteisön johdolle turvallisuuteen liittyvien velvoitteiden noudattamisesta yhteisössä.

10. Hankeviranomaisena toimivan pääsihteeristön on tarvittaessa ilmoitettava asianmukaiselle kansalliselle tai nimetylle turvallisuusviranomaiselle tai muulle toimivaltaiselle turvallisuusviranomaiselle, että yhteisöturvallisuusselvitys vaaditaan sopimuksen tekemistä edeltävässä vaiheessa tai sopimuksen toimeenpanoa varten. Yhteisöturvallisuusselvitys tai henkilöturvallisuusselvitys vaaditaan sopimuksen tekemistä edeltävässä vaiheessa, jos tarjousmenettelyn aikana on annettava CONFIDENTIEL UE/EU CONFIDENTIAL- tai SECRET UE/EU SECRET - turvaluokan tietoja.

11. Hankeviranomainen ei saa tehdä turvaluokiteltua sopimusta valitun tarjoajan kanssa ennen kuin se on saanut sen jäsenvaltion kansalliselta tai nimetyltä turvallisuusviranomaiselta tai muulta toimivaltaiselta turvallisuusviranomaiselta, johon asianomainen hankeosapuoli tai alihankkija on rekisteröity, vahvistuksen siitä, että mahdollisesti vaadittava asianmukainen yhteisöturvallisuusselvitys on myönnetty.

12. Kansallisen tai nimetyn turvallisuusviranomaisen tai muun toimivaltaisen turvallisuusviranomaisen, joka on myöntänyt yhteisöturvallisuusselvityksen, on ilmoitettava hankeviranomaisena toimivalle pääsihteeristölle yhteisöturvallisuusselvitykseen vaikuttavista muutoksista. Kun kyseessä on alihankintasopimus, kansalliselle tai nimetylle turvallisuusviranomaiselle tai muulle toimivaltaiselle turvallisuusviranomaiselle on ilmoitettava vastaavasti.

13. Jos asiaankuuluva kansallinen tai nimetty turvallisuusviranomainen tai muu toimivaltainen turvallisuusviranomainen peruuttaa yhteisöturvallisuusselvityksen, se antaa hankeviranomaisena toimivalle pääsihteeristölle riittävän perusteen päättää turvaluokiteltu sopimus tai sulkea tarjoaja kilpailun ulkopuolelle.

IV TURVALUOKITELLUT SOPIMUKSET JA ALIHANKINTASOPIMUKSET

14. Jos EU:n turvaluokiteltuja tietoja luovutetaan tarjoajalle sopimusta edeltävässä vaiheessa, tarjouspyynnössä on oltava määräys, jolla tarjoaja, joka ei esitä tarjousta tai jonka tarjousta ei valita, velvoitetaan palauttamaan kaikki turvaluokitellut asiakirjat tietyn ajan kuluessa.

15. Kun turvaluokiteltu sopimus tai alihankintasopimus on tehty, hankeviranomaisena toimivan pääsihteeristön on annettava hankeosapuolen tai alihankkijan kansalliselle tai nimetylle turvallisuusviranomaiselle tai muulle toimivaltaiselle turvallisuusviranomaiselle tiedoksi turvaluokitellun sopimuksen turvallisuusmääräykset.

16. Kun tällaiset sopimukset päätetään, hankeviranomaisena toimivan pääsihteeristön (ja/tai tapauksen mukaan alihankintasopimuksen ollessa kyseessä kansallisen tai nimetyn turvallisuusviranomaisen tai muun toimivaltaisen turvallisuusviranomaisen) on ilmoitettava asiasta viipymättä hankeosapuolen tai alihankkijan rekisteröintijäsenvaltion kansalliselle tai nimetylle turvallisuusviranomaiselle tai muulle toimivaltaiselle turvallisuusviranomaiselle.

17. Yleensä hankeosapuolen tai alihankkijan edellytetään palauttavan hankeviranomaiselle turvaluokitellun sopimuksen tai alihankintasopimuksen päättyessä kaikki hallussaan olevat EU:n turvaluokitellut tiedot.

18. Turvallisuutta koskevaan lisälausekkeeseen on sisällytettävä erityiset säännökset EU:n turvaluokiteltujen tietojen hallussapidosta sopimuksen täytäntöönpanon aikana tai sopimuksen päättyessä.

19. Jos hankeosapuoli tai alihankkija saa luvan säilyttää EU:n turvaluokiteltuja tietoja sopimuksen päätyttyä, tässä päätöksessä säädettyjä vähimmäisvaatimuksia on yhä noudatettava, ja hankeosapuolen tai alihankkijan on suojattava EU:n turvaluokiteltujen tietojen luottamuksellisuus.

20. Tarjouspyynnössä ja sopimuksessa on määriteltävä, millä edellytyksin hankeosapuoli voi tehdä alihankintasopimuksia.

21. Hankeosapuolen on saatava hankeviranomaisena toimivan pääsihteeristön lupa ennen kuin se antaa turvaluokitellun sopimuksen mitään osia alihankkijoiden toteutettavaksi. Alihankintasopimuksia ei saa tehdä sellaisten yritysten tai muiden yhteisöjen kanssa, jotka on rekisteröity EU:n ulkopuolisessa valtiossa, joka ei ole tehnyt tietoturvallisuussopimusta EU:n kanssa.

22. Hankeosapuolen on vastattava siitä, että kaikki alihankintatoimet suoritetaan tässä päätöksessä säädettyjen vähimmäisvaatimusten mukaisesti, eikä se saa antaa EU:n turvaluokiteltuja tietoja alihankkijalle ilman hankeviranomaisen kirjallista etukäteissuostumusta.

23. Jos hankeosapuoli tai alihankkija tuottaa tai käsittelee EU:n turvaluokiteltuja tietoja, hankeviranomainen käyttää tietojen luovuttajan oikeuksia.

V TURVALUOKITELTUIHIN SOPIMUKSIIN LIITTYVÄT VIERAILUT

24. Jos pääsihteeristön, hankeosapuolien tai alihankkijoiden on saatava CONFIDENTIEL UE/EU CONFIDENTIAL- tai SECRET UE/EU SECRET -turvaluokan tietoja toistensa toimitiloissa turvaluokitellun sopimuksen toimeenpanemiseksi, vierailuista on sovittava asianomaisten kansallisten tai nimettyjen turvallisuusviranomaisten tai muun toimivaltaisen turvallisuusviranomaisen kanssa. Kansalliset tai nimetyt turvallisuusviranomaiset voivat kuitenkin myös sopia menettelystä, jossa vierailut voidaan järjestää suoraan.

25. Kaikilla vierailijoilla on oltava asianmukainen turvallisuusselvitys ja tiedonsaantitarve, jotta heille voidaan myöntää pääsy pääsihteeristön tekemään sopimukseen liittyviin EU:n turvaluokiteltuihin tietoihin.

26. Vierailijoille on annettava pääsy vain käynnin tarkoitukseen liittyviin EU:n turvaluokiteltuihin tietoihin.

VI EU:N TURVALUOKITELTUJEN TIETOJEN LÄHETTÄMINEN JA KULJETTAMINEN

27. EU:n turvaluokiteltujen tietojen lähettämiseen sähköisesti sovelletaan tämän päätöksen 9 artiklassa ja liitteessä III olevia asiaankuuluvia säännöksiä.

28. EU:n turvaluokiteltujen tietojen fyysiseen kuljettamiseen sovelletaan tämän päätöksen liitteessä IV olevia asiaankuuluvia säännöksiä kansallisten lakien ja asetusten mukaisesti.

29. EU:n turvaluokiteltujen tietojen fyysistä kuljettamista koskevia turvallisuusjärjestelyjä määritettäessä on sovellettava seuraavia periaatteita:

    a) turvallisuus on taattava kuljetuksen kaikissa vaiheissa lähtöpisteestä lopulliseen määräpaikkaan saakka;

    b) lähetyksen suojan taso on määriteltävä siinä olevan aineiston korkeimman turvaluokan mukaan;

c) kuljetuksen suorittaville yrityksille on tarvittaessa hankittava yhteisöturvallisuusselvitys. Tällaisissa tapauksissa lähetystä käsittelevällä henkilöstöllä on oltava tämän liitteen mukainen turvallisuusselvitys;

d) lähettäjän on ennen CONFIDENTIEL UE/EU CONFIDENTIAL- tai SECRET UE/EU SECRET -turvaluokitellun aineiston rajatylittäviä siirtoja laadittava kuljetussuunnitelma, joka kansallisen tai nimetyn turvallisuusviranomaisen tai muun asianomaisen toimivaltaisen turvallisuusviranomaisen on hyväksyttävä;

e) kuljetusmatkojen on oltava mahdollisuuksien mukaan yhtäjaksoisia, ja ne on suoritettava niin nopeasti kuin olosuhteet sallivat;

f) reittien olisi mahdollisuuksien mukaan kuljettava ainoastaan jäsenvaltioiden kautta. Muiden kuin jäsenvaltioiden kautta kulkevia reittejä olisi käytettävä ainoastaan, kun niihin on sekä lähettäjävaltion että vastaanottajavaltion kansallisen tai nimetyn turvallisuusviranomaisen tai muun toimivaltaisen turvallisuusviranomaisen lupa.

VII EU:N TURVALUOKITELTUJEN TIETOJEN LÄHETTÄMINEN KOLMANSISSA VALTIOISSA SIJAITSEVILLE HANKEOSAPUOLILLE

30. EU:n turvaluokiteltuja tietoja lähetetään kolmansissa valtioissa sijaitseville hankeosapuolille ja alihankkijoille hankeviranomaisena toimivan pääsihteeristön ja sen kolmannen valtion, johon hankeosapuoli on rekisteröity, kansallisen tai nimetyn turvallisuusviranomaisen välillä sovittujen turvatoimien mukaisesti.

VIII RESTREINT UE/EU RESTRICTED -TURVALUOKAN TIETOJEN KÄSITTELY JA SÄILYTTÄMINEN

31. Pääsihteeristö voi tarvittaessa hankeviranomaisena yhdessä jäsenvaltion kansallisen tai nimetyn turvallisuusviranomaisen kanssa tehdä vierailuja hankeosapuolten tai alihankkijoiden toimitiloihin sopimusmääräysten pohjalta sen varmistamiseksi, että sopimuksessa edellytetyt tarpeelliset turvatoimet RESTREINT UE/EU RESTRICTED -turvaluokan EU:n turvaluokiteltujen tietojen suojaamiseksi on toteutettu.

32. Hankeviranomaisen on annettava kansallisille tai nimetyille turvallisuusviranomaisille tai muulle toimivaltaiselle turvallisuusviranomaiselle tiedoksi RESTREINT UE/EU RESTRICTED -turvaluokan tietoja sisältävät sopimukset, jos sitä edellytetään kansallisissa laeissa ja asetuksissa.

33. Hankeosapuolilta tai alihankkijoilta ja niiden henkilöstöltä ei vaadita yhteisöturvallisuusselvitystä eikä henkilöturvallisuusselvitystä sellaisia pääsihteeristön tekemiä sopimuksia varten, joissa on RESTREINT UE/EU RESTRICTED -turvaluokan tietoja.

34. Hankeviranomaisena toimivan pääsihteeristön on tutkittava tarjouspyyntöihin saadut vastaukset, jos sopimuksen tekeminen edellyttää RESTREINT UE/EU RESTRICTED -turvaluokan tietojen saamista, tämän rajoittamatta vaatimuksia, joita kansallisissa laeissa ja asetuksissa saattaa olla yhteisöturvallisuusselvityksistä tai henkilöturvallisuusselvityksistä.

35. Edellytysten, joilla hankeosapuoli voi tehdä alihankintasopimuksia, on oltava 21 kohdan mukaisia.

36. Jos sopimukseen kuuluu RESTREINT UE/EU RESTRICTED -turvaluokan EU:n turvaluokiteltujen tietojen käsittelyä hankeosapuolen käyttämässä viestintä- ja tietojärjestelmässä, hankeviranomaisena toimivan pääsihteeristön on varmistettava, että sopimuksessa tai alihankintasopimuksessa määrätään viestintä- ja tietojärjestelmän hyväksymistä koskevista tarvittavista teknisistä ja hallinnollisista vaatimuksista, jotka ovat oikeassa suhteessa arvioituun riskiin ja joissa on otettu huomioon kaikki asiaankuuluvat tekijät. Viestintä- ja tietojärjestelmän hyväksymisen laajuudesta on sovittava hankeviranomaisen ja kansallisen tai nimetyn turvallisuusviranomaisen kesken.

TURVALUOKITELTUJEN TIETOJEN VAIHTO KOLMANSIEN VALTIOIDEN JA KANSAINVÄLISTEN JÄRJESTÖJEN KANSSA

I JOHDANTO

1. Tässä liitteessä vahvistetaan 12 artiklan täytäntöönpanosäännökset.

II TURVALUOKITELTUJEN TIETOJEN VAIHDON PUITTEET

2. Jos neuvosto toteaa, että turvaluokiteltujen tietojen vaihtoon on pitkäaikainen tarve,

   – tehdään tietoturvallisuussopimus, tai

   – sovitaan hallinnollisesta järjestelystä

   12 artiklan 2 kohdan ja jäljempänä olevien III ja IV jakson mukaisesti turvallisuuskomitean suosituksen pohjalta.

3. Jos ETPP-operaatiota varten tuotettuja EU:n turvaluokiteltuja tietoja on tarkoitus luovuttaa operaatioon osallistuville kolmansille valtioille tai kansainvälisille järjestöille ja jos kumpiakaan 2 kohdassa tarkoitetuista puitteista ei ole olemassa, EU:n turvaluokiteltujen tietojen vaihtoon osallistuvan kolmannen valtion tai kansainvälisen järjestön kanssa sovelletaan

   – osallistumista koskevaa puitesopimusta; tai

   – osallistumista koskevaa tilapäistä sopimusta; tai

   – jos kumpaakaan edellä mainituista ei ole tehty, tilapäistä hallinnollista järjestelyä.

4. Jos 2 ja 3 kohdassa tarkoitettuja puitteita ei ole olemassa ja jos EU:n turvaluokiteltuja tietoja päätetään poikkeuksellisesti ja tapauskohtaisesti luovuttaa kolmannelle valtiolle tai kansainväliselle järjestölle jäljempänä olevan VI jakson mukaisesti, asianomaiselta kolmannelta valtiolta tai kansainväliseltä järjestöltä on pyydettävä kirjallinen vakuutus sen varmistamiseksi, että se suojaa sille mahdollisesti luovutetut EU:n turvaluokitellut tiedot tässä päätöksessä säädettyjen perusperiaatteiden ja vähimmäisvaatimusten mukaisesti.

III TIETOTURVALLISUUSSOPIMUKSET

5. Tietoturvallisuussopimuksissa on määrättävä perusperiaatteista ja vähimmäisvaatimuksista, joita sovelletaan turvaluokiteltujen tietojen vaihtoon EU:n ja kolmannen valtion tai kansainvälisen järjestön välillä.

6. Tietoturvallisuussopimuksissa on määrättävä teknisistä täytäntöönpanojärjestelyistä, joista on sovittava pääsihteeristön turvallisuusyksikön, Euroopan komission turvallisuusyksikön ja kyseisen kolmannen valtion tai kansainvälisen järjestön toimivaltaisen turvallisuusviranomaisen kesken. Täytäntöönpanojärjestelyissä on otettava huomioon asianomaisessa kolmannessa valtiossa tai kansainvälisessä järjestössä sovellettavien turvallisuussääntöjen, -rakenteiden ja -menettelyjen tarjoaman suojan taso. Ne on hyväksyttävä turvallisuuskomiteassa.

7. EU:n turvaluokiteltuja tietoja ei saa vaihtaa sähköisesti, ellei siitä nimenomaisesti määrätä tietoturvallisuussopimuksessa tai teknisissä täytäntöönpanojärjestelyissä.

8. Tietoturvallisuussopimuksissa on määrättävä, että ennen sopimuksen mukaista turvaluokiteltujen tietojen vaihtoa pääsihteeristön turvallisuusyksikön ja Euroopan komission turvallisuusyksikön on todettava, että vastaanottava osapuoli kykenee suojaamaan ja pitämään tallessa sille annetut tiedot asianmukaisella tavalla.

9. Kun neuvosto tekee tietoturvallisuussopimuksen, yksi kunkin osapuolen kirjaamo on nimettävä pääasialliseksi saapumis- ja lähtöpaikaksi turvaluokiteltujen tietojen vaihtoa varten.

10. Asianomaisen kolmannen valtion tai kansainvälisen järjestön turvallisuussääntöjen, -rakenteiden ja -menettelyjen toimivuuden arvioimiseksi turvallisuusyksikön on tehtävä arviointikäyntejä yhdessä Euroopan komission turvallisuusyksikön kanssa, mistä on keskinäisesti sovittava asianomaisen kolmannen valtion tai kansainvälisen järjestön kanssa. Arviointikäynnit on tehtävä liitteessä III olevien asiaankuuluvien säännösten mukaisesti, ja niiden perusteella on arvioitava

    a) turvaluokiteltujen tietojen suojaamiseen sovellettavia sääntelypuitteita;

    b) kolmannen valtion tai kansainvälisen järjestön turvallisuusperiaatteiden ja turvallisuutta koskevien järjestelyjen erityispiirteitä, jotka saattavat vaikuttaa mahdollisesti vaihdettavien turvaluokiteltujen tietojen tasoon;

    c) tosiasiallisesti käytössä olevia turvatoimia ja turvallisuusmenettelyjä; ja

    d) luovutettavien EU:n turvaluokiteltujen tietojen turvaluokkaan sovellettavia turvallisuusselvitysmenettelyjä.

11. Arviointikäynnin EU:n puolesta tekevän ryhmän on arvioitava, ovatko kyseisen kolmannen maan tai kansainvälisen järjestön turvallisuussäännöt ja -menettelyt riittävät suojaamaan EU:n turvaluokitellut tiedot määrätyssä turvaluokassa.

12. Arviointikäyntien havainnot on esitettävä raportissa, jonka perusteella turvallisuuskomitea määrittelee korkeimman turvaluokan, johon kuuluvia EU:n turvaluokiteltuja tietoja voidaan vaihtaa asianomaisen kolmannen osapuolen kanssa paperitulosteina ja tarvittaessa sähköisesti, ja vaihtoon kyseisen osapuolen kanssa mahdollisesti sovellettavat erityisedellytykset.

13. Kyseiseen kolmanteen valtioon tai kansainväliseen järjestöön on kaikin tavoin pyrittävä tekemään täysimääräinen turvallisuuden arviointikäynti ennen kuin turvallisuuskomitea hyväksyy täytäntöönpanojärjestelyt, jotta selvitettäisiin käytössä olevan turvallisuusjärjestelmän laatu ja toimivuus. Jos tämä ei kuitenkaan ole mahdollista, pääsihteeristön turvallisuusyksikkö toimittaa turvallisuuskomitealle käytössään olevien tietojen perusteella mahdollisimman täydellisen selvityksen, jossa turvallisuuskomitealle tiedotetaan kolmannen valtion tai kansainvälisen järjestön soveltamista turvallisuussäännöistä ja turvallisuusalan järjestelyistä.

14. Turvallisuuskomitea voi päättää, että mitään EU:n turvaluokiteltuja tietoja ei saa luovuttaa ennen kuin arviointikäynnin tulosten tarkastelu on saatu päätökseen, tai että niitä saa luovuttaa vain tiettyyn turvaluokkaan asti. Se voi myös määrätä muita erityisiä ehtoja EU:n turvaluokiteltujen tietojen luovuttamiselle kyseiselle kolmannelle valtiolle tai kansainväliselle järjestölle. Pääsihteeristön turvallisuusyksikön on ilmoitettava asiasta kyseiselle kolmannelle valtiolle tai kansainväliselle järjestölle.

15. Pääsihteeristön turvallisuusyksikön on keskinäisestä sopimuksesta asianomaisen kolmannen valtion tai kansainvälisen järjestön kanssa tehtävä säännöllisin väliajoin arviointikäyntien seurantakäyntejä sen tarkistamiseksi, että käytössä olevat järjestelyt vastaavat edelleen sovittuja vähimmäisvaatimuksia.

16. Kun tietoturvallisuussopimus on tullut voimaan ja asianomaisen kolmannen valtion tai kansainvälisen järjestön kanssa on alettu vaihtaa turvaluokiteltuja tietoja, turvallisuuskomitea voi päättää muuttaa korkeinta turvaluokkaa, johon kuuluvia EU:n turvaluokiteltuja tietoja voidaan vaihtaa paperitulosteina tai sähköisesti, varsinkin mahdollisten seurantakäyntien perusteella.

IV HALLINNOLLISET JÄRJESTELYT

17. Jos on olemassa pitkäaikainen tarve vaihtaa kolmannen valtion tai kansainvälisen järjestön kanssa tietoja, joiden turvaluokka on yleensä korkeintaan RESTREINT UE/EU RESTRICTED, ja jos turvallisuuskomitea on katsonut, että kyseisen osapuolen turvallisuusjärjestelmä ei ole riittävän kehittynyt tietoturvallisuussopimuksen tekemiseksi, pääsihteeri voi neuvoston hyväksyttyä asian sopia hallinnollisesta järjestelystä kyseisen kolmannen valtion tai kansainvälisen järjestön asiaankuuluvien viranomaisten kanssa.

18. Jos turvaluokiteltujen tietojen vaihtoa varten on kiireellisistä toiminnallisista syistä perustettava puitteet nopeasti, neuvosto voi poikkeuksellisesti päättää, että korkeampaan turvaluokkaan kuuluvien tietojen vaihtoon voidaan tilapäisesti käyttää hallinnollista järjestelyä.

19. Hallinnollisista järjestelyistä sovitaan pääsääntöisesti kirjeenvaihtona.

20. EU:n turvaluokiteltuja tietoja ei saa tosiasiallisesti luovuttaa kyseiselle kolmannelle valtiolle tai kansainväliselle järjestölle ennen kuin on tehty 10 kohdassa tarkoitettu arviointikäynti ja ennen kuin turvallisuuskomitea on hyväksynyt sille toimitetun raportin. EU:n turvaluokiteltuja tietoja saa kuitenkin luovuttaa, jos turvaluokiteltujen tietojen kiireelliseen vaihtoon on poikkeuksellisia syitä, joista neuvostolle on ilmoitettu, edellyttäen, että tällainen arviointikäynti pyritään kaikin tavoin tekemään mahdollisimman pian.

21. EU:n turvaluokiteltuja tietoja ei saa vaihtaa sähköisesti, ellei siitä nimenomaisesti määrätä hallinnollisessa järjestelyssä.

V TURVALUOKITELTUJEN TIETOJEN VAIHTO ETPP-OPERAATIOIDEN YHTEYDESSÄ

22. Kolmansien valtioiden tai kansainvälisten järjestöjen osallistumisesta ETPP-operaatioihin määrätään osallistumista koskevissa puitesopimuksissa. Kyseisiin sopimuksiin on sisällytettävä määräyksiä ETPP-operaatioita varten tuotettujen EU:n turvaluokiteltujen tietojen luovuttamisesta osallistuville kolmansille valtioille tai kansainvälisille järjestöille. Korkein turvaluokka, johon kuuluvia EU:n turvaluokiteltuja tietoja voidaan vaihtaa, on määriteltävä kunkin ETPP-operaation perustamista koskevassa yhteisessä toiminnassa.

23. Tiettyä ETPP-operaatiota varten tehtyihin osallistumista koskeviin tilapäisiin sopimuksiin on sisällytettävä määräyksiä kyseistä operaatiota varten tuotettujen EU:n turvaluokiteltujen tietojen luovuttamisesta osallistuvalle kolmannelle valtiolle tai kansainväliselle järjestölle. Korkein turvaluokka, johon kuuluvia EU:n turvaluokiteltuja tietoja voidaan vaihtaa, on määriteltävä kyseisen ETPP-operaation perustamista koskevassa yhteisessä toiminnassa.

24. Kolmannen valtion tai kansainvälisen järjestön osallistumista määrättyyn ETPP-operaatioon koskevissa tilapäisissä hallinnollisissa järjestelyissä voidaan määrätä muun muassa operaatiota varten tuotettujen EU:n turvaluokiteltujen tietojen luovuttamisesta kyseiselle kolmannelle valtiolle tai kansainväliselle järjestölle. Tällaisista tilapäisistä hallinnollisista järjestelyistä on sovittava edellä IV jaksossa olevassa 17 ja 18 kohdassa säädettyjen menettelyjen mukaisesti. Korkein turvaluokka, johon kuuluvia EU:n turvaluokiteltuja tietoja voidaan vaihtaa, on määriteltävä kyseisen ETPP-operaation perustamista koskevassa yhteisessä toiminnassa.

25. Ennen EU:n turvaluokiteltujen tietojen luovuttamista koskevien säännösten täytäntöönpanoa 22, 23 ja 24 kohdan yhteydessä ei tarvitse toteuttaa täytäntöönpanojärjestelyjä eikä arviointikäyntejä.

26. Jos isäntävaltiolla, jonka alueella ETPP-operaatio toteutetaan, ei ole EU:n kanssa voimassa olevaa tietoturvallisuussopimusta eikä hallinnollista järjestelyä turvaluokiteltujen tietojen vaihtoa varten, voidaan perustaa tilapäinen hallinnollinen järjestely siinä tapauksessa, että siihen on erityinen ja välitön toiminnallinen tarve. Tästä mahdollisuudesta on määrättävä ETPP-operaation perustamista koskevassa yhteisessä toiminnassa. Kyseisissä olosuhteissa luovutettavat EU:n turvaluokitellut tiedot on rajoitettava ETPP-operaatiota varten tuotettuihin tietoihin, jotka kuuluvat korkeintaan RESTREINT UE/EU RESTRICTED -turvaluokkaan. Isäntävaltion on tällaisessa tilapäisessä hallinnollisessa järjestelyssä sitouduttava suojaamaan EU:n turvaluokitellut tiedot sellaisten vähimmäisvaatimusten mukaisesti, jotka ovat vähintään yhtä tiukat kuin tässä päätöksessä säädetyt vaatimukset.

27. Edellä 22–24 kohdassa tarkoitettujen osallistumista koskevien puitesopimusten, osallistumista koskevien tilapäisten sopimusten ja tilapäisten hallinnollisten järjestelyjen turvaluokiteltuja tietoja koskevissa osissa on määrättävä, että kyseisen kolmannen valtion tai kansainvälisen järjestön on varmistettava, että sen mihin tahansa operaatioon lähettämä henkilöstö suojaa EU:n turvaluokitellut tiedot neuvoston turvallisuussääntöjen sekä toimivaltaisten viranomaisten, myös operaation komentoketjun antamien muiden ohjeiden mukaisesti.

28. Jos EU:n ja osallistuvan kolmannen valtion tai kansainvälisen järjestön välillä tehdään myöhemmin tietoturvallisuussopimus, tietoturvallisuussopimus syrjäyttää mahdollisen osallistumista koskevan puitesopimuksen, osallistumista koskevan tilapäisen sopimuksen tai tilapäisen hallinnollisen järjestelyn EU:n turvaluokiteltujen tietojen vaihdon ja käsittelyn osalta.

29. EU:n turvaluokiteltuja tietoja ei saa vaihtaa sähköisesti kolmannen valtion kanssa tehdyn osallistumista koskevan puitesopimuksen, osallistumista koskevan tilapäisen sopimuksen eikä tilapäisen hallinnollisen järjestelyn nojalla, ellei siitä nimenomaisesti määrätä kyseisessä sopimuksessa tai järjestelyssä.

30. ETPP-operaatiota varten tuotettuja EU:n turvaluokiteltuja tietoja voidaan luovuttaa kolmansien valtioiden tai kansainvälisten järjestöjen kyseiseen operaatioon lähettämälle henkilöstölle 22–29 kohdan mukaisesti. Kun tällaiselle henkilöstölle myönnetään pääsy EU:n turvaluokiteltuihin tietoihin ETPP-operaation tiloissa tai viestintä- ja tietojärjestelmässä, on toteutettava toimenpiteitä (mukaan lukien luovutettujen EU:n turvaluokiteltujen tietojen kirjaaminen) tietojen katoamisen tai vaarantumisen riskin vähentämiseksi. Toimenpiteet on määriteltävä suunnittelu- tai operaatioasiakirjoissa.

VI EU:N TURVALUOKITELTUJEN TIETOJEN POIKKEUKSELLINEN LUOVUTTAMINEN TAPAUSKOHTAISESTI

31. Jos III–V jakson mukaisia puitteita ei ole olemassa ja jos neuvosto tai jokin sen valmistelevista elimistä päätyy siihen, että EU:n turvaluokiteltujen tietojen luovuttamiseen kolmannelle valtiolle tai kansainväliselle järjestölle on poikkeuksellinen tarve, pääsihteeristön on

a) mahdollisuuksien mukaan tarkistettava asianomaisen kolmannen valtion tai kansainvälisen järjestön viranomaisilta, että sen turvallisuussäännöillä, -rakenteilla ja -menettelyillä pystytään takaamaan sille luovutettujen EU:n turvaluokiteltujen tietojen suojaaminen vähintään yhtä tiukkojen vaatimusten kuin tässä päätöksessä säädettyjen vaatimusten mukaisesti;

b) pyydettävä turvallisuuskomiteaa antamaan käytettävissä olevien tietojen pohjalta suositus turvallisuussääntöjen, -rakenteiden ja -menettelyjen luotettavuudesta kolmannessa valtiossa tai kansainvälisessä järjestössä, jolle EU:n turvaluokiteltuja tietoja on tarkoitus luovuttaa.

32. Jos turvallisuuskomitea antaa suosituksen EU:n turvaluokiteltujen tietojen luovuttamiseksi, asia siirretään Coreperille, joka päättää tietojen luovuttamisesta.

33. Jos turvallisuuskomitean suosituksessa ei puolleta EU:n turvaluokiteltujen tietojen luovuttamista,

a) YUTP- tai ETPP-asioissa poliittisten ja turvallisuusasioiden komitea keskustelee asiasta ja laatii suosituksen pysyvien edustajien komitean päätökseksi;

b) kaikissa muissa asioissa pysyvien edustajien komitea keskustelee ja päättää asiasta.

34. Pysyvien edustajien komitea voi katsoessaan sen asianmukaiseksi ja saatuaan tietojen luovuttajan kirjallisen ennakkosuostumuksen päättää, että turvaluokitellut tiedot voidaan luovuttaa vain osittain tai vain, jos niiden turvaluokka on sitä ennen alennettu tai poistettu, tai että luovutettavat tiedot on valmisteltava niin, ettei niissä viitata lähteeseen eikä alkuperäiseen EU:n turvaluokkaan.

35. Kun EU:n turvaluokiteltujen tietojen luovuttamisesta on päätetty, pääsihteeristö toimittaa asianomaisen asiakirjan, jonka luovutettavuutta koskevassa merkinnässä mainitaan kolmas valtio tai kansainvälinen järjestö, jolle se on luovutettu. Kyseisen kolmannen osapuolen on ennen tietojen luovuttamista tai luovuttamisen yhteydessä kirjallisesti sitouduttava suojaamaan vastaanottamansa EU:n turvaluokitellut tiedot tässä päätöksessä säädettyjen perusperiaatteiden ja vähimmäisvaatimusten mukaisesti.

VII TOIMIVALTA LUOVUTTAA EU:N TURVALUOKITELTUJA TIETOJA KOLMANSILLE VALTIOILLE TAI KANSAINVÄLISILLE JÄRJESTÖILLE

36. Jos turvaluokiteltujen tietojen vaihtamiseksi kolmannen valtion tai kansainvälisen järjestön kanssa on olemassa 2 kohdan mukaiset puitteet, neuvosto tekee päätöksen pääsihteerin valtuuttamisesta luovuttamaan EU:n turvaluokiteltuja tietoja kyseiselle kolmannelle valtiolle tai kansainväliselle järjestölle noudattaen alkuperäisen luovuttajan suostumuksen periaatetta.

37. Jos turvaluokiteltujen tietojen vaihtamiseksi kolmannen valtion tai kansainvälisen järjestön kanssa on olemassa 3 kohdan mukaiset puitteet, pääsihteeri on toimivaltainen luovuttamaan EU:n turvaluokiteltuja tietoja ETPP-operaation perustamista koskevan yhteisen toiminnan mukaisesti ja noudattaen alkuperäisen luovuttajan suostumuksen periaatetta.

38. Pääsihteeri voi siirtää tällaisen valtuutuksen pääsihteeristön johtavassa asemassa oleville virkamiehille tai muille alaisuudessaan oleville henkilöille.

LISÄYKSET

LISÄYS A

Määritelmät

LISÄYS B

Turvaluokkien vastaavuus

LISÄYS C

Luettelo kansallisista turvallisuusviranomaisista

LISÄYS D

Lyhenneluettelo (List of abbreviations)

MÄÄRITELMÄT

Tässä päätöksessä sovelletaan seuraavia määritelmiä:

"Hyväksynnällä" tarkoitetaan prosessia, jonka päätteeksi turvallisuusjärjestelyt hyväksyvä viranomainen antaa virallisen lausunnon siitä, että järjestelmä on hyväksytty käytettäväksi määritellyssä turvaluokassa, tiettyä turvallisuuden takaavaa toimintatapaa noudattaen käyttöympäristössään ja hyväksyttävällä riskitasolla, sen pohjalta, että hyväksytyt tekniset, fyysiset, organisatoriset ja menettelyyn liittyvät turvatoimet on toteutettu.

"Hallinnollinen alue" – ks. liitteessä II oleva 12 kohta.

"Resurssilla" tarkoitetaan kaikkea, millä on arvoa organisaatiolle, sen liiketoimille ja niiden jatkuvuudelle, organisaation tehtävää tukevat tietoresurssit mukaan luettuina.

"Tietoturvaloukkaus" – ks. 13 artiklan 1 kohta.

"Viestintä- ja tietojärjestelmän elinkaarella" tarkoitetaan viestintä- ja tietojärjestelmän koko olemassaoloaikaa, johon kuuluvat alullepano, luominen, suunnittelu, vaatimusten analysointi, laatiminen, kehittäminen, koekäyttö, täytäntöönpano, käyttö ja ylläpito sekä käytöstä poistaminen.

"Turvaluokitellulla sopimuksella" tarkoitetaan pääsihteeristön jonkin hankeosapuolen kanssa tekemää sopimusta, jolla toimitetaan tavaroita, toteutetaan toimeksiantoja tai tarjotaan palveluja, joiden suoritus edellyttää tai sisältää EU:n turvaluokiteltuihin tietoihin pääsemistä tai niiden tuottamista.

"Turvaluokitellulla alihankintasopimuksella" tarkoitetaan pääsihteeristön jonkin hankeosapuolen toisen hankeosapuolen (eli alihankkijan) kanssa tekemää sopimusta, jolla toimitetaan tavaroita, toteutetaan toimeksiantoja tai tarjotaan palveluja, joiden suoritus edellyttää tai sisältää EU:n turvaluokiteltuihin tietoihin pääsemistä tai niiden tuottamista.

"Viestintä- ja tietojärjestelmä" – ks. 10 artiklan 2 kohta.

"Vaarantuminen" – ks. 13 artiklan 2 kohta.

"Hankeosapuolella" tarkoitetaan henkilöä tai oikeudellista yhteisöä, joka on oikeudellisesti kelpoinen tekemään sopimuksia.

"Salausaineistolla" tarkoitetaan salausalgoritmeja, salauslaitteistoja ja -ohjelmistomoduuleja sekä tuotteita, joihin sisältyy täytäntöönpanoa koskevia yksityiskohtia sekä niihin liittyviä asiakirjoja ja avainnusaineistoa.

"Syvyyssuuntaisella turvallisuudella" tarkoitetaan sitä, että toteutetaan joukko turvatoimia, joilla järjestetään monitasoinen puolustus.

"Nimetyllä turvallisuusviranomaisella" tarkoitetaan jäsenvaltion kansalliselle turvallisuusviranomaiselle vastuussa olevaa viranomaista, jonka vastuulla on tiedottaa yrityksille tai muille yhteisöille kansallisista periaatteista kaikissa yhteisöturvallisuutta koskevissa asioissa sekä antaa ohjausta ja apua niiden soveltamisessa. Kansallinen turvallisuusviranomainen tai muu toimivaltainen viranomainen voi toimia nimettynä turvallisuusviranomaisena.

"Asiakirjalla" tarkoitetaan mitä tahansa tallennettua tietoa, riippumatta sen fyysisestä muodosta tai ominaisuuksista.

"Turvaluokan alentamisella" tarkoitetaan salassapitotason alentamisesta johtuvaa turvaluokan muuttamista.

"ETPP-operaatiolla" tarkoitetaan Euroopan unionista tehdyn sopimuksen V osaston nojalla toteutettavaa sotilas- tai siviilikriisinhallintaoperaatiota.

"EU:n turvaluokitellut tiedot" – ks. 2 artiklan 1 kohta.

"Yhteisöturvallisuusselvityksellä" tarkoitetaan kansallisen tai nimetyn turvallisuusviranomaisen hallinnollista päätöstä, jonka mukaan toimitila tarjoaa turvallisuuden kannalta riittävän suojan tiettyyn turvaluokkaan kuuluville EU:n turvaluokitelluille tiedoille ja jonka mukaan kyseisissä tiloissa työskentelevälle henkilöstölle, jonka tehtävät edellyttävät EU:n turvaluokiteltuihin tietoihin pääsemistä, on tehty asianmukainen turvallisuusselvitys ja selvitetty EU:n turvaluokiteltuihin tietoihin pääsemisen ja niiden suojaamisen edellyttämät asiaankuuluvat turvallisuusvaatimukset.

EU:n turvaluokiteltujen tietojen "käsittelyllä" tarkoitetaan kaikkia mahdollisia toimia, joita EU:n turvaluokiteltuihin tietoihin voidaan kohdistaa niiden elinkaaren aikana. Näitä ovat tietojen tuottaminen, käsittely, kuljettaminen, turvaluokan alentaminen, turvaluokan poistaminen ja hävittäminen. Viestintä- ja tietojärjestelmien osalta toimia ovat myös tietojen kerääminen, näyttäminen, lähettäminen ja säilyttäminen.

Tietojen tai asiakirjojen "haltijalla" tarkoitetaan asianmukaisesti valtuutettua henkilöä, jonka tiedonsaantitarve on todettu ja jonka hallussa on EU:n turvaluokiteltu tieto, jonka suojaamisesta hän on tämän mukaisesti vastuussa.

"Yrityksellä tai muulla yhteisöllä" tarkoitetaan tavaroiden toimittamiseen, toimeksiantojen suorittamiseen tai palvelujen tarjoamiseen osallistuvaa yhteisöä. Kyseessä voi olla teollinen, kaupallinen, palvelu-, tieteellinen, tutkimus-, koulutus- tai kehitysyhteisö taikka itsenäinen ammatinharjoittaja.

"Yhteisöturvallisuus" – ks. 11 artiklan 1 kohta.

"Tietojen turvaaminen" – ks. 10 artiklan 1 kohta.

"Yhteenliittäminen" – ks. liitteessä IV oleva 31 kohta.

"Turvaluokiteltujen tietojen hallinnointi" – ks. 9 artiklan 1 kohta.

"Aineistolla" tarkoitetaan mitä tahansa asiakirjaa tai konetta tai laitetta, joka on valmistettu tai jota ollaan valmistamassa.

"Luovuttajalla" tarkoitetaan EU:n toimielintä, virastoa tai elintä, kolmatta valtiota tai kansainvälistä järjestöä, jonka alaisuudessa turvaluokiteltuja tietoja on tuotettu ja/tai tuotu EU:n rakenteisiin.

"Henkilöstöturvallisuus" – ks. 7 artiklan 1 kohta.

"Henkilöturvallisuusselvityksellä" tarkoitetaan jompaakumpaa seuraavista tai molempia:

– "EU:n henkilöturvallisuusselvityksellä" ("EU-turvallisuusselvitys") EU:n turvaluokiteltujen tietojen saamista varten tarkoitetaan pääsihteeristön nimitysvallan käyttäjän hallinnollista päätöstä, joka tehdään tämän päätöksen mukaisesti jäsenvaltion toimivaltaisten viranomaisten tekemän turvallisuustutkinnan jälkeen ja jonka nojalla henkilölle voidaan myöntää oikeus saada EU:n turvaluokiteltuja tietoja määrättyyn turvaluokkaan (CONFIDENTIEL UE/EU CONFIDENTIAL tai korkeampi) ja tiettyyn päivämäärään saakka edellyttäen, että hänen tiedonsaantitarpeensa on todettu. Henkilön katsotaan tämän jälkeen olevan "turvallisuusselvitetty".

– "Kansallisella henkilöturvallisuusselvityksellä" ("kansallinen turvallisuusselvitys") EU:n turvaluokiteltujen tietojen saamista varten tarkoitetaan jäsenvaltion toimivaltaisen viranomaisen hallinnollista päätöstä, joka tehdään jäsenvaltion toimivaltaisten viranomaisten tekemän turvallisuustutkinnan jälkeen ja jonka nojalla henkilölle voidaan myöntää oikeus saada EU:n turvaluokiteltuja tietoja määrättyyn turvaluokkaan (CONFIDENTIEL UE/EU CONFIDENTIAL tai korkeampi) ja tiettyyn päivämäärään saakka edellyttäen, että hänen tiedonsaantitarpeensa on todettu. Henkilön katsotaan tämän jälkeen olevan "turvallisuusselvitetty".

"Henkilöturvallisuusselvitykseen perustuvalla henkilöturvallisuustodistuksella" tarkoitetaan toimivaltaisen viranomaisen antamaa todistusta, jossa todetaan henkilön olevan turvallisuusselvitetty ja että tällä on voimassa oleva kansallinen tai EU-turvallisuusselvitys, ja josta käy ilmi turvaluokka, johon kuuluvien EU:n turvaluokiteltujen tietojen saamiseen asianomaiselle henkilölle voidaan myöntää oikeus (CONFIDENTIEL UE/EU CONFIDENTIAL tai korkeampi), asiaankuuluvan turvallisuusselvityksen voimassaoloaika ja itse todistuksen voimassaolon päättymispäivä.

"Fyysinen turvallisuus" – ks. 8 artiklan 1 kohta.

"Ohjelman tai hankkeen turvallisuusohjeilla" tarkoitetaan luetteloa turvallisuusmenettelyistä, joita sovelletaan tiettyyn ohjelmaan tai hankkeeseen turvallisuusmenettelyjen yhdenmukaistamiseksi. Turvallisuusohjeita voidaan tarkistaa koko ohjelman tai hankkeen ajan.

"Kirjaaminen" – ks. liitteessä III oleva 18 kohta.

"Jäännösriskillä" tarkoitetaan riskiä, joka jää jäljelle, kun turvatoimet on toteutettu viestintä- ja tietojärjestelmässä, ottaen huomioon, että kaikkia uhkia ei torjuta ja että kaikkea haavoittuvuutta ei voida poistaa.

"Riskillä" tarkoitetaan mahdollisuutta, että tietty uhka hyötyy organisaation tai minkä tahansa sen käyttämän järjestelmän sisäisestä ja ulkoisesta haavoittuvuudesta ja aiheuttaa tällä tavoin vahinkoa organisaatiolle ja sen aineellisille tai aineettomille resursseille. Sen mittana on uhkien toteutumisen todennäköisyys yhdistettynä niiden vaikutuksiin.

– "Riskin hyväksyminen" on päätös hyväksyä jäännösriskin olemassaolo riskin käsittelyn jälkeen.

– "Riskinarviointi" koostuu uhkien ja haavoittuvuuden määrittelystä ja niihin liittyvän riskianalyysin eli todennäköisyyden ja vaikutusten analyysin tekemisestä.

– "Riskiviestintää" ovat viestintä- ja tietojärjestelmien käyttäjien riskitietoisuuden lisääminen, riskeistä tiedottaminen hyväksyville viranomaisille ja niistä raportoiminen toiminnasta vastaaville viranomaisille.

– "Riskin käsittely" muodostuu riskin lieventämisestä, poistamisesta, vähentämisestä (asianmukaisin teknisin, fyysisin, organisatorisin tai menettelyyn liittyvin toimenpitein), siirtämisestä ja seurannasta.

"Turva-alue" – ks. liitteessä II oleva 12 kohta.

"Turvallisuutta koskevalla lisälausekkeella" tarkoitetaan hankeviranomaisen määräämää erityissopimusehtojen kokonaisuutta, joka on erottamaton osa pääsyä EU:n turvaluokiteltuihin tietoihin tai niiden tuottamista edellyttävää turvaluokiteltua sopimusta ja jossa yksilöidään turvallisuusvaatimukset tai ne sopimuksen osat, joiden turvallisuus on suojattava.

"Turvaluokitusoppaalla" tarkoitetaan asiakirjaa, jossa kuvataan turvaluokitellun ohjelman tai sopimuksen osat ja eritellään sovellettavat turvaluokat. Turvaluokitusopasta voidaan laajentaa ohjelman tai sopimuksen koko keston ajan, ja sen sisältämien tietojen turvaluokat voidaan määritellä uudelleen tai niitä voidaan alentaa. Jos turvaluokitusopas on olemassa, sen on oltava osa turvallisuutta koskevaa lisälauseketta.

"Turvallisuustutkinnalla" tarkoitetaan tutkintamenettelyjä, jotka jäsenvaltion toimivaltainen kansallinen viranomainen suorittaa kansallisten lakien ja asetusten mukaisesti sen varmistamiseksi, että henkilöstä ei ole tiedossa mitään sellaista kielteistä seikkaa, joka estäisi kansallisen tai EU-turvallisuusselvityksen myöntämisen hänelle EU:n turvaluokiteltujen tietojen saamista varten tiettyyn turvaluokkaan saakka (CONFIDENTIEL UE/EU CONFIDENTIAL tai korkeampi).

"Turvallisuuden takaavalla toimintatavalla" tarkoitetaan viestintä- ja tietojärjestelmän toimintaedellytysten määrittelyä, joka perustuu käsiteltyjen tietojen turvaluokkiin ja turvallisuusselvitystasoihin, järjestelmään pääsyn virallisiin hyväksymisiin ja sen käyttäjien tiedonsaantitarpeeseen. Turvaluokiteltujen tietojen käsittelyssä tai lähettämisessä voidaan käyttää neljää eri toimintatapaa: yleisvaltuutusta, korkean turvallisuustason toimintatapaa, osastokohtaista toimintatapaa ja monitasoista toimintatapaa.

– "Yleisvaltuutuksella" tarkoitetaan toimintatapaa, jossa KAIKILLE viestintä- ja tietojärjestelmään pääseville henkilöille tehdään turvallisuusselvitys järjestelmässä käsiteltävien tietojen korkeimman turvaluokan mukaan ja henkilöillä on yhteinen tarve saada KAIKKI järjestelmässä käsiteltävät tiedot.

– "Korkean turvallisuustason toimintatavalla" tarkoitetaan toimintatapaa, jossa KAIKILLE viestintä- ja tietojärjestelmään pääseville henkilöille tehdään turvallisuusselvitys järjestelmässä käsiteltävien tietojen korkeimman turvaluokan mukaan, mutta KAIKILLA järjestelmään pääsevillä henkilöillä EI OLE yhteistä tarvetta saada järjestelmässä käsiteltäviä tietoja. Tällaiset henkilöt voivat myöntää pääsyn tietoihin.

– "Osastokohtaisella toimintatavalla" tarkoitetaan toimintatapaa, jossa KAIKILLE viestintä- ja tietojärjestelmään pääseville henkilöille tehdään turvallisuusselvitys järjestelmässä käsiteltävien tietojen korkeimman turvaluokan mukaan, mutta KAIKILLA järjestelmään pääsevillä henkilöillä EI OLE virallista valtuutusta saada KAIKKIA järjestelmässä käsiteltäviä tietoja. Virallinen valtuutus merkitsee sitä, että tietoihin pääsyn valvontaa hallinnoidaan virallisesti keskitetysti erona menettelyyn, jossa henkilö voi myöntää pääsyn tietoihin harkintansa mukaan.

– "Monitasoisella toimintatavalla" tarkoitetaan toimintatapaa, jossa KAIKILLE viestintä- ja tietojärjestelmään pääseville henkilöille EI TEHDÄ turvallisuusselvitystä järjestelmässä käsiteltävien tietojen korkeimman turvaluokan mukaan, ja KAIKILLA järjestelmään pääsevillä henkilöillä EI OLE yhteistä tarvetta saada järjestelmässä käsiteltäviä tietoja.

"Turvallisuusriskien hallintaprosessilla" tarkoitetaan prosessia, jossa yksilöidään, hallitaan ja minimoidaan epävarmoja tapahtumia, jotka saattavat vaikuttaa organisaation tai joidenkin sen käyttämien järjestelmien turvallisuuteen. Se kattaa kaikki riskeihin liittyvät toiminnot, myös arvioinnin, käsittelyn, hyväksymisen ja viestinnän.

"TEMPESTillä" tarkoitetaan haitallisen elektromagneettisen säteilyn tutkimista ja valvontaa sekä toimenpiteitä sen poistamiseksi.

"Uhalla" tarkoitetaan mahdollista syytä ei-toivottuun tapahtumaan, joka voi johtaa organisaation tai jonkin sen käyttämän järjestelmän vahingoittumiseen. Uhat voivat olla tahattomia tai tahallisia (vihamielisiä), ja niille ovat ominaisia uhkaavat seikat sekä mahdolliset kohteet ja hyökkäysmenetelmät.

"Haavoittuvuudella" tarkoitetaan minkä tahansa laatuista heikkoutta, josta yksi tai useampi uhka voi hyötyä. Haavoittuvuus voi johtua laiminlyönnistä tai liittyä heikkouksiin valvonnan tehokkuudessa, täydellisyydessä tai johdonmukaisuudessa, ja se voi olla luonteeltaan teknistä, menettelyyn liittyvää, fyysistä, organisatorista tai toiminnallista.

LISÄYS B

TURVALUOKKIEN VASTAAVUUS

EU	TRES SECRET UE/ EU TOP SECRET	SECRET UE/ EU SECRET	CONFIDENTIEL UE/ EU CONFIDENTIAL	RESTREINT UE/ EU RESTRICTED
Belgia	Très Secret (Loi 11.12.1998) Zeer Geheim (Wet 11.12.1998)	Secret (Loi 11.12.1998) Geheim (Wet 11.12.1998)	Confidentiel (Loi 11.12.1998) Vertrouwelijk (Wet 11.12.1998)	*ks. huomautus[1] jäljempänä*
Bulgaria	Строго секретно	Секретно	Поверително	За служебно ползване
Tšekin tasavalta	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Tanska	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Saksa	Streng geheim	Geheim	VS[2]— Vertraulich	VS — Nur für den Dienstgebrauch
Viro	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Kreikka	Άκρως Απόρρητο Lyh.: ΑΑΠ	Απόρρητο Lyh.: (ΑΠ)	Εμπιστευτικό Lyh.: (ΕΜ)	Περιορισμένης Χρήσης Lyh.: (ΠΧ)
Espanja	Secreto	Reservado	Confidencial	Difusión Limitada
Ranska	Très Secret Défense	Secret Défense	Confidentiel Défense	*ks. huomautus[3] jäljempänä*
Irlanti	Top Secret	Secret	Salassa pidettävä tieto.	Rajoitettu
Italia	Segretissimo	Segreto	Riservatissimo	Riservato
Kypros	Άκρως Απόρρητο Lyh.: (ΑΑΠ)	Απόρρητο Lyh.: (ΑΠ)	Εμπιστευτικό Lyh.: (ΕΜ)	Περιορισμένης Χρήσης Lyh.: (ΠΧ)
Latvia	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Liettua	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Luxemburg	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Unkari	Szigorúan titkos!	Titkos!	Bizalmas!	Korlátozott terjesztésű!
Malta	L-Ogħla Segretezza	Sigriet	Kunfidenzjali	Ristrett
Alankomaat	Stg ZEER GEHEIM	Stg GEHEIM	Stg CONFIDENTIEEL	Dep VERTROUWELIJK
Itävalta	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Puola	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugali	Muito Secreto	Secreto	Confidencial	Reservado
Romania p.m.	Strict secret de importanţă deosebită	Strict secret	Secret	Secret de serviciu
Slovenia.	Strogo tajno	Tajno	Zaupno	Interno
Slovakia	Prísne tajné	Tajné	Dôverné	Vyhradené
Suomi	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Ruotsi[4]	Hemlig/Top secret Hemlig av synnerlig betydelse för rikets säkerhet	Hemlig/Secret Hemlig	Hemlig/Confidential Hemlig	Hemlig/Restricted Hemlig
Yhdistynyt kuningaskunta	Top Secret	Secret	Salassa pidettävä tieto	Rajoitettu

1 Diffusion Restreinte / Beperkte Verspreiding ei ole Belgiassa turvaluokka. Belgia käsittelee ja suojaa RESTREINT UE/EU RESTRICTED -tiedot vähintään yhtä tiukasti kuin Euroopan unionin neuvoston turvallisuussäännöissä kuvatut vaatimukset ja menettelyt edellyttävät.

2 Saksa: VS = Verschlusssache.

3 Ranska ei käytä turvaluokkaa RESTREINT kansallisessa järjestelmässään. Ranska käsittelee ja suojaa RESTREINT UE/EU RESTRICTED -tiedot vähintään yhtä tiukasti kuin Euroopan unionin neuvoston turvallisuussäännöissä kuvatut vaatimukset ja menettelyt edellyttävät.

4 Ruotsi: ylemmällä rivillä olevia turvaluokitusmerkintöjä käytetään puolustusvoimissa, ja alemmalla rivillä olevia merkintöjä käyttävät muut viranomaiset.

LUETTELO KANSALLISISTA TURVALLISUUSVIRANOMAISISTA

BELGIA
Autorité nationale de Sécurité
SPF Affaires étrangères, Commerce extérieur et Coopération au Développement
15, rue des Petits Carmes
B-1000 Bruxelles
Puhelin (sihteeristö): + 32/2/501 45 42
Fax: + 32/2/501 45 96

BULGARIA
State Commission on Information Security
1A Angel Kanchev Str.
BG-1000 Sofia
Puhelin: + 359/2/921 5911
Fax: + 359/2/987 3750
Sähköposti: dksi@government.bg
Verkkosivut: www.dksi.bg

TŠEKIN TASAVALTA,
Národní bezpečnostní úřad
(National Security Authority)
Na Popelce 2/16
CZ-150 06 Praha 56
Puhelin: + 420/257 28 33 35
Fax: + 420/257 28 31 10
Sähköposti: czech.nsa@nbu.cz
Verkkosivut: www.nbu.cz

TANSKA
Politiets Efterretningstjeneste
(Danish Security Intelligence Service)
Klausdalsbrovej 1
DK-2860 Søborg
Puhelin: + 45/33/14 88 88
Fax: + 45/33/43 01 90

Forsvarets Efterretningstjeneste
(Danish Defence Intelligence Service)
Kastellet 30
DK-2100 Copenhagen Ø
Telephone: + 45/33/32 55 66
Fax: + 45/33/93 13 20

SAKSA
Bundesministerium des Innern
Referat ÖS III 3
Alt-Moabit 101 D
D-11014 Berlin
Puhelin: + 49/30/18 681 1522
Faksi: + 49/30/18 681 1441

VIRO
National Security Authority Department
Estonian Ministry of Defence
Sakala 1
15094 Tallinn, Estonia
Puhelin: +372/7170 113, +372/7170 117
Faksi: +372/7170 213
Sähköposti: nsa@kmin.ee

KREIKKA
Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Διακλαδική Διεύθυνση Στρατιωτικών Πληροφοριών (ΔΔΣΠ)
Διεύθυνση Ασφαλείας και Αντιπληροφοριών
ΣΤΓ 1020 -Χολαργός (Αθήνα)
Ελλάδα
Τηλέφωνα: + 30/210/657 20 45 (ώρες γραφείου)
+ 30/210/657 20 09 (ώρες γραφείου)
Φαξ: + 30/210/653 62 79
+ 30/210/657 76 12

Hellenic National Defence General Staff
(HNDGS)
Military Intelligence Sectoral Directorate
Security Counterintelligence Directorate
GR-STG 1020 Holargos – Athens
Puhelin: + 30/210/657 20 45
+ 30/210/657 20 09
Faksi: + 30/210/653 62 79
+ 30/210/657 76 12

ESPANJA
Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
E-28023 Madrid
Puhelin: + 34/91/372 50 00
Fax: + 34/91/372 58 08
E-mail: nsa-sp@areatec.com

RANSKA
Secrétariat général de la Défense Nationale
Service de Sécurité de Défense (SGDN/SSD)
51 Boulevard de la Tour-Maubourg
F-75700 Paris 07 SP
Puhelin: + 33/1/71 75 81 77
Fax: + 33/1/71 75 82 00

IRLANTI
Kansallinen turvallisuusviranomainen
Department of Foreign Affairs
76 - 78 Harcourt Street
Dublin 2
Irlanti
Puhelin: + 353/1/ 478 08 22
Faksi: + 353/1/ 408 29 59

ITALIA
Presidenza del Consiglio dei Ministri
Autorità Nazionale per la Sicurezza
D.I.S. - U.C.Se.
Via di Santa Susanna, 15
I-00187 Roma
Puhelin: + 39/06/611 742 66
Fax: + 39/06/488 52 73

KYPROS
ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ
ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Υπουργείο Άμυνας
Λεωφόρος Εμμανουήλ Ροΐδη 4
1432 Λευκωσία, Κύπρος
Τηλέφωνα: + 357/22/80 75 69, + 357/22/80 76 43, + 357/22/80 77 64
Τηλεομοιότυπο: + 357/22/30 23 51
Ministry of Defence
Minister's Military Staff
National Security Authority (NSA)
4 Emanuel Roidi street
CY-1432 Nicosia
Puhelin: + 357/22/80 75 69, + 357/22/80 76 43, +357 /22/80 77 64, + 357/99 35 80 00
Fax: + 357/22/30 23 51

LATVIA
Kansallinen turvallisuusviranomainen
Constitution Protection Bureau of the Republic of Latvia
P.O.Box 286
LV 1001, Riga
Puhelin: +371/6702 54 18
Faksi: +371/6702 54 54
Sähköposti: ndi@sab.gov.lv

LIETTUA
National Security Authority of the Republic of Lithuania
Gedimino 40/1
LT-2600 Vilnius
Puhelin: + 370/5/266 32 05
Fax: + 370/5/266 32 00

LUXEMBURG
Autorité nationale de Sécurité
Boîte postale 2379
L-1023 Luxembourg
Puhelin: + 352/2478 22 10 central
+ 352/2478 22 53 direct
Fax: + 352/2478 22 43

UNKARI
Nemzeti Biztonsági Felügyelet
P.O. Box 2
HU-1357 Budapest
Puhelin: + 361/346 96 52
Fax: + 361/346 96 58
Verkkosivut: www.nbf.hu

MALTA
Ministry of Justice and Home Affairs
P.O. Box 146
MT-Valletta
Puhelin: + 356/21 24 98 44
Fax: + 356/25 69 53 21

ALANKOMAAT
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20010
NL-2500 EA Den Haag
Puhelin: + 31/70/320 44 00
Fax: + 31/70/320 07 33

Ministerie van Defensie
Beveiligingsautoriteit
Postbus 20701
NL-2500 ES Den Haag
Puhelin: + 31/70/318 70 60
Fax: + 31/70/318 75 22

ITÄVALTA
Informationssicherheitskommission
Bundeskanzleramt
Ballhausplatz 2
A-1014 Wien
Puhelin: + 43/1/531 15 25 94
Fax: + 43/1/531 15 26 15

PUOLA
kansallinen turvallisuusyksikkö
(Agencja Bezpieczeństwa Wewnętrznego – ABW)
2A Rakowiecka St.
PL-00-993 Warszawa
Puhelin: + 48/22/585 73 60
Faksi: + 48/22/585 85 09
Sähköposti: nsa@abw.gov.pl
Verkkosivut: www.abw.gov.pl

Military Counter-Intelligence Service
(Służba Kontrwywiadu Wojskowego)
Classified Information Protection Bureau
Oczki 1
PL-02-007 Warszawa
Puhelin: + 48/22/684 12 47
Faksi: + 48/22/684 10 76
Sähköposti: skw@skw.gov.pl

PORTUGALI
Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Rua da Junqueira, 69
1300-342 Lisboa
Puhelin: +351/ 213 031 710
Faksi: +351/ 213 031 711

ROMANIA
Romanian NSA - ORNISS
National Registry Office for Classified Information
Oficiul Registrului Național al Informațiilor Secrete de Stat
4 Mures Street
RO-012275 Bucharest
Puhelin: 00 4 021 224 58 30
Fax: 00 4 021 224 07 14
Sähköposti: nsa.romania@nsa.ro
Verkkosivut: www.orniss.ro

SLOVENIA
Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
SVN-1000 Ljubljana
Puhelin: + 386/1/478 13 90
Fax: + 386/1/478 13 99

SLOVAKIA
Národný bezpečnostný úrad
(National Security Authority)
Budatínska 30
P.O. Box 16
SVK-850 07 Bratislava
Puhelin: + 421/2/68 69 23 14
Fax: + 421/2/63 82 40 05
Verkkosivut: www.nbusr.sk

SUOMI
National Security Authority
Ministry for Foreign Affairs
P.O. Box 453
FI-00023 Government
Telephone: + 358/9/160 56487
Fax: + 358/9/160 56494
Sähköposti: NSA@formin.fi

RUOTSI
Utrikesdepartementet
SSSB
S-103 39 Stockholm
Puhelin: + 46/8/405 54 44
Fax: + 46/8/723 11 76

YHDISTYNYT KUNINGASKUNTA
UK National Security Authority
PO Box 60628
London SW1P 9HA
Puhelin: + 44/(0)20 7233 8181
Fax: + 44/(0)20 7233 818

LIST OF ABBREVIATIONS

Acronym	Meaning
AQUA	Appropriately Qualified Authority
BPS	Boundary Protection Services
CAA	Crypto Approval Authority
CCTV	Closed Circuit Television
CDA	Crypto Distribution Authority
CFSP	Common Foreign and Security Policy
CIS	Communication and Information Systems
DSA	Designated Security Authority
ESDP	European Security and Defence Policy
EUCI	EU Classified Information
EUSR	EU Special Representative
FSC	Facility Security Clearance
GSC	General Secretariat of the Council
IA	Information Assurance
IDS	Intrusion Detection System
IT	Information Technology
NSA	National Security Authority
PSCC	Personnel Security Clearance Certificate
PSI	Programme/Project Security Instructions
SAA	Security Accreditation Authority
SAB	Security Accreditation Board
SAL	Security Aspects Letter
SecOPs	Security Operating Procedures
SCG	Security Classification Guide
SG/HR	Secretary-General of the Council/High Representative for the CFSP
SSRS	System-Specific Security Requirement Statement