II

(Muut kuin lainsäätämisjärjestyksessä hyväksyttävät säädökset)

PÄÄTÖKSET

NEUVOSTON PÄÄTÖS,

tehty 31 päivänä maaliskuuta 2011,

turvallisuussäännöistä EU:n turvallisuusluokiteltujen tietojen suojaamiseksi

(2011/292/EU)

EUROOPAN UNIONIN NEUVOSTO, joka

ottaa huomioon Euroopan unionin toiminnasta tehdyn sopimuksen ja erityisesti sen 240 artiklan 3 kohdan,

ottaa huomioon neuvoston työjärjestyksen vahvistamisesta 1 päivänä joulukuuta 2009 tehdyn neuvoston päätöksen 2009/937/EU ([1]) ja erityisesti sen 24 artiklan,

sekä katsoo seuraavaa:

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

(2) Tätä päätöstä olisi sovellettava, kun neuvosto, sen valmistelevat elimet ja neuvoston pääsihteeristö käsittelevät EU:n turvallisuusluokiteltuja tietoja.

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

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

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

(6) Euroopan unionista tehdyn sopimuksen V osaston 2 luvun nojalla perustetut EU:n virastot ja elimet sekä Europol ja Eurojust soveltavat omassa organisaatiossaan tässä päätöksessä säädettyjä perusperiaatteita ja vähimmäisvaatimuksia EU:n turvallisuusluokiteltujen tietojen suojaamiseksi, siten kuin niiden perustamissäädöksissä säädetään.

(7) Euroopan unionista tehdyn sopimuksen V osaston 2 luvun nojalla perustetut kriisinhallintaoperaatiot ja niiden henkilöstö soveltavat turvallisuussääntöjä, jotka neuvosto on hyväksynyt EU:n turvallisuusluokiteltujen tietojen suojaamiseksi.

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

(9) Tämän päätöksen tekeminen ei rajoita Euroopan unionin toiminnasta tehdyn sopimuksen 15 ja 16 artiklan eikä niiden täytäntöönpanosäädösten soveltamista.

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

ON HYVÄKSYNYT TÄMÄN PÄÄTÖKSEN:

1 artikla

Kohde, soveltamisala ja määritelmät

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

([1]) EUVL L 325, 11.12.2009, s. 35.

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 turvallisuusluokiteltujen tietojen suojaamisessa noudatetaan vastaavaa tasoa.

3. Tässä päätöksessä sovelletaan lisäyksessä A säädettyjä määritelmiä.

2 artikla

EU:n turvallisuusluokiteltujen tietojen määrittely, turvallisuusluokat ja merkinnät

1. 'EU:n turvallisuusluokitelluilla tiedoilla' tarkoitetaan mitä tahansa tietoja tai aineistoja, joille on määritelty EU:n turvallisuusluokka ja joiden luvaton ilmitulo saattaisi vaihtelevassa määrin vahingoittaa Euroopan unionin tai sen yhden tai useamman jäsenvaltion etuja.

2. EU:n turvallisuusluokitellut tiedot jaetaan seuraaviin turvallisuusluokkiin:

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 turvallisuusluokiteltuihin tietoihin lisätään turvallisuusluokitusmerkintä 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

Turvallisuusluokittelun hallinnointi

1. Toimivaltaisten viranomaisten on varmistettava, että EU:n turvallisuusluokitellut tiedot on asianmukaisesti turvallisuusluokiteltu, että ne on selkeästi määritelty turvallisuusluokitelluiksi tiedoiksi ja että niiden turvallisuusluokka säilytetään vain niin kauan kuin se on tarpeen.

2. EU:n turvallisuusluokiteltujen tietojen turvallisuusluokkaa 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 turvallisuusluokiteltujen tietojen tuottamisessa noudatettavat turvallisuusperiaatteet, joihin sisältyy käytännön turvallisuusluokitusopas.

4 artikla

Turvallisuusluokiteltujen tietojen suojaaminen

1. EU:n turvallisuusluokiteltujen tietojen suojaamisessa on noudatettava tätä päätöstä.

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

3. Jäsenvaltioiden tuodessa Euroopan unionin rakenteisiin tai verkostoihin turvallisuusluokiteltuja tietoja, joissa on kansallinen turvallisuusluokitusmerkintä, neuvosto ja pääsihteeristö noudattavat kyseisten tietojen suojaamisessa vastaavan tason EU:n turvallisuusluokiteltuihin tietoihin sovellettavia vaatimuksia lisäyksessä B olevan turvallisuusluokkien vastaavuustaulukon mukaisesti.

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

5 artikla

Turvallisuusriskien hallinta

1. EU:n turvallisuusluokiteltuihin 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 lisäyksessä B määritellyn syvyyssuuntaisen turvallisuuden käsitteen pohjalta. Turvatoimien tehokkuutta on arvioitava jatkuvasti.

2. Turvatoimet EU:n turvallisuusluokiteltujen tietojen suojaamiseksi koko niiden elinkaaren ajan on suhteutettava erityisesti tietojen tai aineistojen turvallisuusluokitukseen, muotoon ja määrään, EU:n turvallisuusluokiteltujen 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 turvallisuusluokitellut tiedot hätätilanteissa, jotta estetään luvaton pääsy tietoihin, tietojen ilmitulo tai niiden eheyden tai käytettävyyden menettäminen.

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

6 artikla

Tämän päätöksen täytäntöönpano

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

2. Turvallisuuskomitean tasolla voidaan hyväksyä turvallisuutta koskevia suuntaviivoja, joilla täydennetään tai tuetaan tätä päätöstä ja neuvoston mahdollisesti hyväksymiä turvallisuusperiaatteita.

7 artikla

Henkilöstöturvallisuus

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

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

— joille on tarvittaessa tehty asianmukaisen tason turvallisuusselvitys;

— joille on tiedotettu heidän vastuustaan.

2. Henkilöturvallisuusselvitystä koskevien menettelyjen tarkoituksena on selvittää, voidaanko henkilölle myöntää pääsy EU:n turvallisuusluokiteltuihin 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 turvallisuusluokiteltuihin tietoihin, on tehtävä asianmukaisen tason turvallisuusselvitys ennen kuin heille myönnetään pääsy kyseisiin EU:n turvallisuusluokiteltuihin tietoihin. Pääsihteeristön virkamiehiä ja muuta henkilöstöä koskeva henkilöturvallisuus-selvitysmenettely 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 turvallisuusluokiteltuihin 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 turvallisuusluokiteltuihin tietoihin.

5. Kaikille henkilöille on selvitettävä heidän vastuunsa ja heidän on annettava vakuutus vastuustaan suojata EU:n turvallisuusluokitellut tiedot tämän päätöksen mukaisesti ennen kuin heille myönnetään pääsy EU:n turvallisuusluokiteltuihin 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 turvallisuusluokiteltuihin 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 turvallisuusluokiteltuihin 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 turvallisuusluokiteltuja tietoja käsitellään tai säilytetään, 10 artiklan 2 kohdassa määritellyt viestintä- ja tietojärjestelmien sijoitusalueet mukaan luettuina.

4. Alueet, joilla säilytetään CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeamman tason EU:n turvallisuusluokiteltuja 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 turvallisuusluokiteltujen tietojen suojaamiseen saa käyttää vain hyväksyttyjä välineitä tai laitteita.

6. Tämän artiklan täytäntöönpanosäännökset vahvistetaan liitteessä II.

9 artikla

Turvallisuusluokiteltujen tietojen hallinnointi

1. Turvallisuusluokiteltujen tietojen hallinnoinnilla tarkoitetaan hallinnollisten toimenpiteiden soveltamista EU:n turvallisuusluokiteltujen 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 vaarantumis- tai katoamistilanne. Tällaiset toimenpiteet liittyvät erityisesti EU:n turvallisuusluokiteltujen tietojen tuottamiseen, kirjaamiseen, jäljentämiseen, kääntämiseen, kuljettamiseen ja hävittämiseen.

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

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

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

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

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

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

ii) 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 turvallisuusluokiteltujen 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 viestintä- ja tietojärjestelmiin, joissa käsitellään EU:n turvallisuusluokiteltuja tietoja.

3. Viestintä- ja tietojärjestelmissä on käsiteltävä EU:n turvallisuusluokiteltuja 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 turvallisuusluokiteltujen tietojen ja viestintä- ja tietojärjestelmän suojaustaso tämän päätöksen säännösten mukaisesti. Hyväksymislausunnossa on määriteltävä niiden tietojen korkein sallittu turvallisuusluokka, 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 turvallisuusluokan tietoja, on suojattava niin, etteivät tahattomat sähkömagneettiset vuodot vaaranna tietoja (TEMPEST-turvatoimet).

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

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

b) CONFIDENTIEL UE/EU CONFIDENTIAL- tai RESTREINT UE/EU RESTRICTED -turvallisuusluokan tietojen luottamuksellisuus on suojattava salaustuotteilla, jotka salauslaitteiden hyväksyntäviranomainen, 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 -turvallisuusluokiteltujen tietojen luottamuksellisuus voidaan suojata jäsenvaltioiden kansallisissa järjestelmissä salaustuotteilla, jotka on hyväksynyt jäsenvaltion salauslaitteiden hyväksyntäviranomainen.

7. Lähetettäessä EU:n turvallisuusluokiteltuja 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) turvallisuusjärjestelyjen hyväksyntäviranomainen;

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 turvallisuusluokiteltujen tietojen suojaamisen sopimusta edeltävissä neuvotteluissa ja turvallisuusluokiteltujen sopimusten koko elinkaaren ajan. Kyseisiin sopimuksiin ei saa kuulua pääsyä TRES SECRET UE/EU TOP SECRET -turvallisuusluokan tietoihin.

2. Pääsihteeristö voi antaa jäsenvaltioon tai sellaiseen kolmanteen valtioon, jonka kanssa EU on tehnyt 12 artiklan 2 kohdan a tai b alakohdan mukaisen sopimuksen tai hallinnollisen järjestelyn, rekisteröidyille yrityksille tai muille yhteisöille sopimuksella toimeksiantoja, joihin sisältyy tai liittyy pääsy EU:n turvallisuusluokiteltuihin tietoihin tai niiden käsittely tai säilyttäminen.

3. Pääsihteeristön on hankeviranomaisena varmistettava, että tässä päätöksessä säädettyjä ja sopimuksessa tarkoitettuja yhteisöturvallisuutta koskevia vähimmäisvaatimuksia noudatetaan tehtäessä turvallisuusluokiteltuja 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 turvallisuusluokiteltujen tietojen suojaamiseksi sopimusta edeltävien neuvottelujen aikana tai turvallisuusluokitellun 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 turvallisuusluokitelluissa sopimuksissa tai alihankintasopimuksissa, jotka edellyttävät CONFIDENTIEL UE/EU CONFIDENTIAL- tai SECRET UE/EU SECRET -turvallisuusluokan tietojen saamista niiden toimitiloissa joko sopimusten toimeenpanovaiheessa tai sopimuksia edeltävien neuvottelujen aikana, on asiaankuuluvan turvallisuusluokitustason 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 -turvallisuusluokan tietoihin turvallisuusluokitellun sopimuksen toimeenpanemiseksi, kansallisten lakien ja asetusten sekä liitteessä I säädettyjen vähimmäisvaatimusten mukaisesti.

7. Tämän artiklan täytäntöönpanosäännökset vahvistetaan liitteessä V.

12 artikla

Turvallisuusluokiteltujen 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 turvallisuusluokiteltuja tietoja, tätä varten on perustettava asianmukaiset puitteet.

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

a) neuvosto tekee sopimuksia turvallisuusluokiteltujen 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 turvallisuusluokiteltujen tietojen turvallisuusluokka 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 turvallisuusluokiteltuja tietoja kyseiset tiedot suojataan niiden turvallisuusluokan edellyttämällä tavalla ja vähintään yhtä tiukkojen vaatimusten mukaisesti kuin tässä päätöksessä vahvistetut vähimmäisvaatimukset.

4. Neuvosto tekee päätöksen neuvostosta peräisin olevien EU:n turvallisuusluokiteltujen 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 turvallisuusluokiteltujen tietojen luovuttaja ei ole neuvosto, pääsihteeristön on ensin saatava tietojen luovuttajan kirjallinen suostumus luovutukselle. Jos luovuttajaa ei tiedetä, neuvosto ottaa luovuttajan vastuun itselleen.

5. Luovutettujen tai vaihdettujen EU:n turvallisuusluokiteltujen 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 turvallisuusluokiteltujen tietojen vaarantuminen

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

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

a) ilmoittaakseen tietojen luovuttajalle;

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

c) arvioidakseen EU:n tai jäsenvaltioiden eduille aiheutuneen mahdollisen vahingon;

d) toteuttaakseen tarvittavat toimenpiteet tapahtuneen toistumisen estämiseksi;

e) ilmoittaakseen asianmukaisille viranomaisille toteutetuista toimista.

5. Henkilölle, joka on vastuussa tässä päätöksessä säädettyjen turvallisuussääntöjen rikkomisesta, voidaan määrätä kurinpitoseuraamus asiaankuuluvien sääntöjen ja määräysten mukaisesti. Henkilöön, joka on aiheuttanut EU:n turvallisuusluokiteltujen tietojen vaarantumisen tai katoamisen, 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 yleisesti johdonmukaisen soveltamisen.

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

3. Jäsenvaltioiden on toteutettava kaikki asianmukaiset toimenpiteet kansallisten lakiensa ja asetustensa mukaisesti sen varmistamiseksi, että seuraavat noudattavat tätä päätöstä käsitellessään tai säilyttäessään EU:n turvallisuusluokiteltuja 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 turvallisuusluokiteltuihin tietoihin;

d) jäsenvaltioiden hankeosapuolet riippumatta siitä, ovatko ne kyseisten jäsenvaltioiden alueella vai ulkomailla.

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 turvallisuusluokiteltujen tietojen luovuttaminen kolmansille valtioille ja kansainvälisille järjestöille;

c) pääsihteerin ehdottaman ja turvallisuuskomitean suositteleman vuosittaisen tarkastusohjelman, jonka mukaan tarkastetaan jäsenvaltioiden ja Euroopan unionin toiminnasta tehdyn sopimuksen V osaston 2 luvun nojalla perustettujen EU:n virastojen ja elinten sekä Europolin ja Eurojustin yksiköt ja tilat ja tehdään arviointikäyntejä kolmansiin valtioihin ja kansainvälisiin järjestöihin EU:n turvallisuusluokiteltujen tietojen suojaamiseksi toteutettujen toimenpiteiden tehokkuuden varmistamiseksi;

d) edellä 6 artiklan 1 kohdassa tarkoitetut turvallisuusperiaatteet.

2. Pääsihteeri toimii pääsihteeristön turvallisuusviranomaisena. Siinä ominaisuudessa hän

a) panee täytäntöön neuvoston turvallisuusperiaatteet ja arvioi niitä;

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

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

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

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

f) huolehtii EU:n turvallisuusluokiteltujen tietojen suojaamiseksi toteutettujen turvallisuusjärjestelyjen määräaikaistarkastuksista EU:n virastoissa ja elimissä, Europolissa, Eurojustissa ja Euroopan unionin toiminnasta tehdyn sopimuksen V osaston 2 luvun 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 turvallisuusluokiteltujen tietojen suojaamiseksi toteutettujen turvallisuusjärjestelyjen määräaikaistarkastuksista jäsenvaltioiden yksiköissä ja tiloissa;

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

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

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

Pääsihteeristön turvallisuusyksikkö on pääsihteerin käytettävissä näihin tehtäviin.

3. Jäsenvaltioiden olisi 14 artiklan 3 kohdan täytäntöönpanemiseksi

a) nimettävä kansallinen turvallisuusviranomainen, joka vastaa turvallisuusjärjestelyistä EU:n turvallisuusluokiteltujen tietojen suojaamiseksi niin, että

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

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

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

iv) tarpeelliset turvallisuusohjelmat on laadittu EU:n turvallisuusluokiteltujen tietojen vaarantumis- tai katoamisriskin minimoimiseksi;

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

vi) vastataan Euroopan unionin toiminnasta tehdyn sopimuksen V osaston 2 luvun nojalla perustettujen EU:n virastojen ja elinten, Europolin, Eurojustin ja Euroopan unionin toiminnasta tehdyn sopimuksen V osaston 2 luvun nojalla perustettujen kriisinhallintaoperaatioiden ja EU:n erityisedustajien ja heidän alaisuudessaan työskentelevien henkilöiden esittämiin asianmukaisiin turvallisuusselvityspyyntöihin.

Kansalliset turvallisuusviranomaiset luetellaan lisäyksessä C;

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

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 komission ja Euroopan ulkosuhdehallinnon edustaja osallistuu sen kokouksiin. Komitean puheenjohtajana toimii pääsihteeri tai hänen nimeämänsä henkilö. Se kokoontuu neuvoston toimeksiannosta tai pääsihteerin taikka kansallisen turvallisuusviranomaisen pyynnöstä.

Euroopan unionin toiminnasta tehdyn sopimuksen V osaston 2 luvun nojalla perustettujen EU:n virastojen ja elinten sekä Europolin ja Eurojustin 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 19 päivänä maaliskuuta 2001 tehty neuvoston päätös 2001/264/EY ([1]).

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

18 artikla

Voimaantulo

Tämä päätös tulee voimaan päivänä, jona se julkaistaan *Euroopan unionin virallisessa lehdessä*.

Tehty Brysselissä 31 päivänä maaliskuuta 2011.

Neuvoston puolesta

Puheenjohtaja

VÖLNER P.

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

LIITTEET

LIITE I

Henkilöstöturvallisuus

LIITE II

Fyysinen turvallisuus

LIITE III

Turvallisuusluokiteltujen tietojen hallinnointi

LIITE IV

Viestintä- ja tietojärjestelmissä käsiteltävien EU:n turvallisuusluokiteltujen tietojen suojaaminen

LIITE V

Yhteisöturvallisuus

LIITE VI

Turvallisuusluokiteltujen tietojen vaihto kolmansien valtioiden ja kansainvälisten järjestöjen kanssa

LIITE I

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 turvallisuusluokiteltuihin 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 TURVALLISUUSLUOKITELTUIHIN TIETOIHIN

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

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

   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 turvallisuusluokiteltujen tietojen suojaamista koskevat turvallisuussäännöt ja -menettelyt ja hän on antanut vakuutuksen tällaisten tietojen suojaamista koskevasta vastuustaan.

4. Kunkin jäsenvaltion ja pääsihteeristön on määritettävä omissa hallintorakenteissaan ne tehtävät, jotka edellyttävät pääsyä CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeamman turvallisuusluokan 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 turvallisuusluokan 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 turvallisuusluokan 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 turvallisuusluokan 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 turvallisuuteen liittyviä 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 painostetuksi (esimerkiksi siksi, että hänellä on yksi tai useampi muu kuin EU-kansalaisuus tai siksi, että hänellä on sukulaisia tai läheisiä, 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. Tarvittaessa ja kansallisten lakien ja asetusten mukaisesti puolison, avopuolison tai läheisen perheenjäsenen luonne, käyttäytyminen ja olosuhteet voidaan myös katsoa merkityksellisiksi turvallisuustutkintaa tehtäessä.

Tutkintavaatimukset pääsyn myöntämiseksi EU:n turvallisuusluokiteltuihin tietoihin

Ensimmäisen turvallisuusselvityksen myöntäminen

11. Ensimmäisen turvallisuusselvityksen CONFIDENTIEL UE/EU CONFIDENTIAL- ja SECRET UE/EU SECRET -turvallisuusluokan 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 turvallisuusluokiteltujen tietojen sen turvallisuusluokan 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;

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.

12. Ensimmäisen turvallisuusselvityksen TRES SECRET UE/EU TOP SECRET -turvallisuusluokan tietoihin pääsyä varten on perustuttava turvallisuustutkintaan, joka kattaa vähintään viimeiset kymmenen 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;

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 on haastateltava, 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.

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

Turvallisuusselvityksen uusiminen

14. 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 turvallisuusluokiteltuihin 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.

15. Turvallisuusselvitysten uusimiseksi on tutkittava 11 ja 12 kohdassa esitetyt seikat.

16. Uusimispyynnöt on esitettävä hyvissä ajoin ottaen huomioon turvallisuustutkinnan 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

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

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

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

a) Jos turvallisuustutkinnassa saadaan lausunto 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 turvallisuusluokiteltuihin tietoihin asiaankuuluvaan turvallisuusluokkaan ja määrättyyn päivään asti.

b) Jos turvallisuustutkinnassa ei saada tällaista lausuntoa, 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.

20. 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 neuvoston asetuksessa (ETY, Euratom, EHTY) N:o 259/68 ([1]) säädettyjen Euroopan unionin virkamiehiin sovellettavien henkilöstösääntöjen ja Euroopan unionin muuhun henkilöstöön sovellettavien palvelussuhteen ehtojen mukaisesti, jäljempänä ”henkilöstösäännöt ja palvelussuhteen ehdot”.

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

22. 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.

23. 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 19 kohdan a alakohdan mukaisesti annetun lausunnon 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 turvallisuusluokiteltuihin tietoihin ja hänet on siirrettävä pois tehtävistä, joissa niihin pääsy on mahdollista tai joissa turvallisuus voisi hänen vuokseen vaarantua.

24. 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 henkilöstösääntöjen ja palvelussuhteen ehtojen mukaisesti.

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

Turvallisuusselvityksiä koskevat rekisterit

26. Kukin jäsenvaltio rekisteröi ne kansalliset turvallisuusselvitykset ja pääsihteeristö ne EU-turvallisuusselvitykset, jotka ne ovat myöntäneet pääsyn antamiseksi EU:n turvallisuusluokiteltuihin tietoihin. Rekistereihin on merkittävä vähintään korkein turvallisuusluokka, johon kuuluviin EU:n turvallisuusluokiteltuihin tietoihin henkilölle voidaan myöntää pääsy (CONFIDENTIEL UE/EU CONFIDENTIAL tai korkeampi), turvallisuusselvityksen myöntämispäivä ja sen voimassaoloaika.

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

Vapautukset turvallisuusselvitysvaatimuksesta

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

IV TURVALLISUUSKOULUTUS JA -TIETOISUUS

29. Kaikkien henkilöiden, joille on myönnetty turvallisuusselvitys, on kirjallisesti vakuutettava ymmärtävänsä velvollisuutensa suojata EU:n turvallisuusluokitellut tiedot sekä seuraukset, joihin EU:n turvallisuusluokiteltujen tietojen vaarantuminen johtaa. Jäsenvaltiot ja tapauksen mukaan pääsihteeristö rekisteröivät tällaiset kirjalliset vakuutukset.

30. Kaikille henkilöille, joille on myönnetty pääsy EU:n turvallisuusluokiteltuihin 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.

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

([1]) EYVL L 56, 4.3.1968, s. 1.

V POIKKEUKSELLISET OLOSUHTEET

32. Jäsenvaltion toimivaltaisen kansallisen viranomaisen myöntämässä henkilöturvallisuusselvityksessä kansallisten turvallisuusluokiteltujen tietojen saamiseksi voidaan tilapäisesti siihen asti, kunnes kansallinen turvallisuusselvitys pääsystä EU:n turvallisuusluokiteltuihin tietoihin myönnetään, sallia kansallisten virkamiesten pääsy EU:n turvallisuusluokiteltuihin tietoihin lisäyksessä B olevassa vastaavuustaulukossa määriteltyyn vastaavaan turvallisuusluokkaan 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 turvallisuusluokiteltuihin tietoihin ei sallita kansallisissa laeissa ja asetuksissa.

33. 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 turvallisuusluokiteltuihin tietoihin tietyn tehtävän suorittamiseksi. Kyseiset tilapäiset valtuutukset ovat voimassa korkeintaan kuusi kuukautta, eivätkä ne oikeuta pääsemään TRES SECRET UE/EU TOP SECRET -turvallisuusluokan tietoihin. Kaikkien henkilöiden, joille on myönnetty tilapäinen valtuutus, on kirjallisesti vakuutettava ymmärtävänsä velvollisuutensa suojata EU:n turvallisuusluokitellut tiedot sekä seuraukset, jos EU:n turvallisuusluokitellut tiedot vaarantuvat. Pääsihteeristö rekisteröi tällaiset kirjalliset vakuutukset.

34. Jos henkilö on määrä asettaa tehtävään, joka edellyttää yhtä tasoa korkeamman tason turvallisuusselvitystä kuin hänellä tuolloin on, tehtävään asettaminen voidaan tehdä väliaikaisesti edellyttäen, että

a) henkilön esimies perustelee kirjallisesti pakottavan tarpeen päästä korkeamman turvallisuusluokan EU:n turvallisuusluokiteltuihin tietoihin;

b) pääsy rajataan koskemaan tiettyjä erikseen määriteltyjä EU:n turvallisuusluokiteltuja tietoja tehtävään asettamisen 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 asettamisen tehtävään;

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

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

36. Erittäin poikkeuksellisissa olosuhteissa, kuten toteutettaessa operaatioita vihamielisessä ympäristössä tai kasvavien kansainvälisten jännitteiden aikana, jäsenvaltiot ja pääsihteeri voivat kiireellisten toimenpiteiden niin edellyttäessä ja erityisesti ihmishenkien pelastamiseksi myöntää mahdollisuuksien mukaan kirjallisesti pääsyn CONFIDENTIEL UE/EU CONFIDENTIAL- tai SECRET UE/EU SECRET -turvallisuusluokan 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 rekisteri ja kuvaus tiedoista, joihin pääsy hyväksyttiin.

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

38. Turvallisuuskomitealle on ilmoitettava tapauksista, joissa käytetään 36 ja 37 kohdan mukaista menettelyä.

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

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

VI NEUVOSTOSSA PIDETTÄVIIN KOKOUKSIIN OSALLISTUMINEN

41. Jollei 28 kohdasta muuta johdu, henkilöiden, joille on annettu tehtäväksi osallistua neuvoston istuntoihin tai neuvoston valmistelevien elinten kokouksiin, joissa käsitellään CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeamman turvallisuusluokan 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 ajantasaista nimiluetteloa, joka on asianmukainen näyttö turvallisuusselvityksestä.

42. Jos henkilön, jonka tehtävät edellyttävät osallistumista neuvoston tai neuvoston valmistelevien elinten kokouksiin, kansallinen turvallisuusselvitys EU:n turvallisuusluokiteltuihin tietoihin pääsemiseksi perutaan turvallisuussyistä, toimivaltaisen viranomaisen on ilmoitettava asiasta pääsihteeristölle.

VII MAHDOLLINEN PÄÄSY EU:N TURVALLISUUSLUOKITELTUIHIN TIETOIHIN

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

44. 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 turvallisuusluokiteltujen tietojen suojaamista koskevat turvallisuusmenettelyt ja annettava ohjeet heidän mainittujen tietojen suojaamiseen liittyvistä tehtävistään.

LIITE II

FYYSINEN TURVALLISUUS

I JOHDANTO

1. Tässä liitteessä vahvistetaan 8 artiklan täytäntöönpanosäännökset. Siinä vahvistetaan EU:n turvallisuusluokiteltujen 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 turvallisuusluokiteltuihin tietoihin

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

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

   c) ehkäisemällä, estämällä ja havaitsemalla luvattomat toimet;

   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 turvallisuusluokiteltujen tietojen suojaamiseksi tiloissaan, jotta varmistettaisiin, että fyysisen suojelun taso vastaa arvioitua riskiä. Riskinhallintaprosessissa on otettava huomioon kaikki asiaankuuluvat tekijät, erityisesti seuraavat:

   a) EU:n turvallisuusluokiteltujen tietojen turvallisuusluokka;

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

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

   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) kehäsuojaus: fyysinen este, jolla suojattava alue rajataan;

   b) tunkeutumisenhavaitsemisjärjestelmät: kehäsuojauksen tarjoaman turvallisuustason parantamiseksi voidaan käyttää tunkeutumisenhavaitsemisjärjestelmää. 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, turvallisuushenkilöstön ja/tai vastaanottovirkailijan toimesta tai muunlaisin fyysisin keinoin;

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

   e) kameravalvonta: turvallisuushenkilöstö voi käyttää kameravalvontaa tilanteiden ja tunkeutumisenhavaitsemisjärjestelmien 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;

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

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

6. Jos EU:n turvallisuusluokiteltuihin 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 ja rakenteita. Jo olemassa olevien toimitilojen osalta fyysiset turvallisuusvaatimukset on pantava täytäntöön mahdollisimman täydellisesti.

III EU:N TURVALLISUUSLUOKITELTUJEN TIETOJEN FYYSISEEN SUOJELUUN TARKOITETUT LAITTEET

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

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

    a) hallinnollisia alueita;

    b) 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;

    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 kaikkea 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 turvallisuusluokiteltuihin tietoihin, sovelletaan lisäksi seuraavia vaatimuksia:

    a) alueella tavanomaisesti säilytettyjen tietojen korkein turvallisuusluokka 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 turvallisuusluokiteltuihin tietoihin ole pääsyä.

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

    a) alueilla on oltava tunkeutumisenhavaitsemisjärjestelmä, ne on pidettävä lukittuina silloin, kun niitä ei käytetä, ja niitä on vartioitava silloin, kun ne ovat käytössä. Avaimia on valvottava 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 turvallisuusviranomaisen on tarkastettava kaikki viestintä-, sähkö- tai elektroniset laitteet ennen kuin niitä käytetään alueilla, joilla pidetään SECRET UE/EU SECRET- tai sitä korkeamman turvallisuusluokan tietoihin liittyviä kokouksia tai tehdään tällaisiin tietoihin liittyvää työtä, silloin kun EU:n turvallisuusluokiteltuihin tietoihin kohdistuva uhka arvioidaan korkeaksi, ja näin varmistettava, ettei niillä voi tahattomasti eikä laittomasti 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 tunkeutumisenhavaitsemisjärjestelmä.

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

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

    a) EU:n turvallisuusluokiteltujen tietojen, joita alueella voidaan käsitellä ja säilyttää, turvallisuusluokka;

    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 turvallisuusluokiteltujen 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 turvallisuusluokan EU:n turvallisuusluokiteltujen tietojen säilyttämiseen hyväksytyt turvakaapit.

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

23. RESTREINT UE/EU RESTRICTED -turvallisuusluokan EU:n turvallisuusluokiteltuja tietoja voidaan käsitellä

    a) turva-alueella,

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

    c) turva-alueen tai hallinnollisen alueen ulkopuolella, jos tietojen haltija kuljettaa EU:n turvallisuusluokiteltuja tietoja liitteessä III olevan 28–40 kohdan mukaisesti ja hän on sitoutunut noudattamaan toimivaltaisen turvallisuusviranomaisen antamissa turvallisuusohjeissa määrättyjä korvaavia toimenpiteitä sen varmistamiseksi, että pääsy EU:n turvallisuusluokiteltuihin tietoihin on suojattu sivullisilta.

24. RESTREINT UE/EU RESTRICTED -turvallisuusluokan EU:n turvallisuusluokiteltuja 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 -turvallisuusluokan EU:n turvallisuusluokiteltuja tietoja voidaan käsitellä

    a) turva-alueella,

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

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

        i) kuljettaa EU:n turvallisuusluokiteltuja tietoja liitteessä III olevan 28–40 kohdan mukaisesti;

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

        iii) pitää EU:n turvallisuusluokitellut 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 -turvallisuusluokan EU:n turvallisuusluokitellut tiedot on säilytettävä turva-alueella turvakaapissa tai kassaholvissa.

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

28. TRES SECRET UE/EU TOP SECRET -turvallisuusluokan EU:n turvallisuusluokiteltuja 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 päivystyshenkilöstön säännölliset tarkastukset;

        ii) hyväksytty tunkeutumisenhavaitsemisjärjestelmä ja hälytyksiin vastaava turvallisuushenkilöstö;

    tai

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

29. Säännöt EU:n turvallisuusluokiteltujen tietojen kuljettamisesta fyysisesti suojattujen alueiden ulkopuolella vahvistetaan liitteessä III.

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

30. Toimivaltaisen turvallisuusviranomaisen on määriteltävä toimistojen, huoneiden, kassaholvien ja turvakaappien avainten ja numeroyhdistelmien hallinnointimenettelyt. Tällaisilla menettelyillä on suojattava ne luvattomalta pääsyltä.

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

    a) aina, kun numeroyhdistelmän tuntevassa henkilöstössä tapahtuu muutos;

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

    c) kun jokin lukoista on huollettu tai korjattu;

    d) vähintään 12 kuukauden välein.

LIITE III

TURVALLISUUSLUOKITELTUJEN TIETOJEN HALLINNOINTI

I JOHDANTO

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

II TURVALLISUUSLUOKITTELUN HALLINNOINTI

Turvallisuusluokat ja merkinnät

2. Tiedot turvallisuusluokitellaan, jos niiden luottamuksellisuus on suojattava.

3. EU:n turvallisuusluokiteltujen tietojen luovuttajan on vastattava tietojen turvallisuusluokan määrittelystä turvallisuusluokittelua koskevien asiaankuuluvien ohjeiden mukaisesti sekä niiden alustavasta jakelusta.

4. EU:n turvallisuusluokiteltujen tietojen turvallisuusluokka määritellään 2 artiklan 2 kohdan mukaisesti ja soveltaen turvallisuusperiaatteita, jotka hyväksytään 3 artiklan 3 kohdan mukaisesti.

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

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

7. Koko asiakirjan tai tiedoston turvallisuusluokan on oltava vähintään yhtä korkea kuin sen korkeimpaan turvallisuusluokkaan määritellyn osan turvallisuusluokka. Jos eri lähteistä peräisin olevia tietoja yhdistetään, lopputuote on tarkistettava sen kokonaisturvallisuusluokan määrittämiseksi, koska asiakirja voi edellyttää korkeampaa turvallisuusluokkaa kuin sen muodostavat osat.

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

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

CONFIDENTIEL UE/EU CONFIDENTIAL

Ilman liitteitä RESTREINT UE/EU RESTRICTED

Merkinnät

10. 2 artiklan 2 kohdassa säädettyjen turvallisuusluokitusmerkintöjen lisäksi EU:n turvallisuusluokitelluissa 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 turvallisuusluokka voidaan alentaa tai poistaa.

Turvallisuusluokitusmerkintöjen lyhenteet

11. Tekstiin kuuluvien yksittäisten kappaleiden turvallisuusluokan merkitsemiseen voidaan käyttää vakiomuotoisia turvallisuusluokitusmerkintöjen lyhenteitä. Täydellisiä turvallisuusluokitusmerkintöjä ei saa korvata lyhenteillä.

12. EU:n turvallisuusluokitelluissa asiakirjoissa voidaan käyttää seuraavia vakiomuotoisia lyhenteitä, joilla ilmoitetaan alle yhden sivun mittaisten jaksojen tai tekstin osien turvallisuusluokka:

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 turvallisuusluokiteltujen tietojen tuottaminen

13. Tuotettaessa EU:n turvallisuusluokiteltua asiakirjaa

a) turvallisuusluokka on merkittävä selvästi jokaiselle sivulle;

b) jokainen sivu on numeroitava;

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

d) asiakirja on päivättävä;

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

14. Jos EU:n turvallisuusluokiteltuihin tietoihin ei voida soveltaa 13 kohtaa, on toteutettava muita asianmukaisia toimenpiteitä 6 artiklan 2 kohdan nojalla laadittavien turvallisuutta koskevien suuntaviivojen mukaisesti.

EU:n turvallisuusluokiteltujen tietojen turvallisuusluokan alentaminen ja poistaminen

15. Tietoja tuottaessaan luovuttajan on mahdollisuuksien mukaan ja erityisesti RESTREINT UE/EU RESTRICTED -turvallisuusluokan tietojen osalta ilmoitettava, voidaanko EU:n turvallisuusluokiteltujen tietojen turvallisuusluokkaa alentaa tai turvallisuusluokitus poistaa tiettynä päivänä tai tietyn tapahtuman jälkeen.

16. Pääsihteeristön on tarkistettava hallussaan olevat EU:n turvallisuusluokitellut tiedot säännöllisin väliajoin sen selvittämiseksi, onko turvallisuusluokka edelleen asianmukainen. Pääsihteeristön on perustettava järjestelmä sen luovuttamien kirjattujen EU:n turvallisuusluokiteltujen tietojen turvallisuusluokan tarkistamiseksi vähintään joka viides vuosi. Tarkistaminen ei ole tarpeen, jos tietojen luovuttaja on alun perin ilmoittanut, että tietojen turvallisuusluokkaa alennetaan tai että se poistetaan ilman eri toimenpiteitä, ja jos tiedot on merkitty tämän mukaisesti.

III EU:N TURVALLISUUSLUOKITELTUJEN TIETOJEN KIRJAAMINEN TURVALLISUUSTARKOITUKSIIN

17. Kaikille pääsihteeristön ja jäsenvaltioiden kansallisten hallintojen organisaatioyksiköille, joissa EU:n turvallisuusluokiteltuja 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 turvallisuustarkoituksiin, jäljempänä 'kirjaaminen', tarkoitetaan sellaisten menettelyjen soveltamista, joilla rekisteröidään aineiston elinkaari, myös sen jakelu ja hävittäminen.

19. Kaikki CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeamman turvallisuusluokan aineisto on kirjattava sille tarkoitetuissa kirjaamoissa, kun aineisto saapuu organisaatioyksikköön tai lähtee siitä.

20. Pääsihteeristön keskuskirjaamo rekisteröi kaikki neuvoston ja pääsihteeristön kolmansille valtioille ja kansainvälisille järjestöille luovuttamat turvallisuusluokitellut tiedot sekä kaikki kolmansilta valtioilta tai kansainvälisiltä järjestöiltä vastaanotetut turvallisuusluokitellut tiedot.

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

22. Neuvosto hyväksyy turvallisuustarkoituksiin kirjattavia EU:n turvallisuusluokiteltuja tietoja koskevat turvallisuusperiaatteet.

TRES SECRET UE/EU TOP SECRET -turvallisuusluokan tietojen kirjaamot

23. Jäsenvaltioihin ja pääsihteeristöön on nimettävä kirjaamo, joka toimii TRES SECRET UE/EU TOP SECRET -turvallisuusluokan 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 niiden ulkopuolelle ilman keskuskirjaamon nimenomaista kirjallista hyväksyntää.

IV EU:N TURVALLISUUSLUOKITELTUJEN 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 turvallisuusluokan 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 TURVALLISUUSLUOKITELTUJEN TIETOJEN KULJETTAMINEN

28. EU:n turvallisuusluokiteltujen tietojen fyysiseen kuljettamiseen sovelletaan 30–40 kohdassa esitettyjä suojatoimenpiteitä. Jos EU:n turvallisuusluokiteltuja tietoja siirretään sähköisillä tallennusvälineillä ja sen estämättä, mitä 9 artiklan 4 kohdassa säädetään, jäljempänä 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 turvallisuusluokiteltujen tietojen kuljettamisesta tämän päätöksen mukaisesti.

Rakennuksen tai suljetun rakennusryhmän sisällä

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

31. TRES SECRET UE/EU TOP SECRET -turvallisuusluokan 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 turvallisuusluokitellut tiedot on pakattava niin, että ne on suojattu luvattomalta ilmitulolta.

33. SECRET UE/EU SECRET- tai sitä alemman turvallisuusluokan tiedot on kuljetettava EU:n alueella jollakin seuraavista tavoista:

a) sotilaskuriirilla, valtion kuriirilla tai diplomaattikuriirilla tapauksen mukaan;

b) henkilökohtaisesti, jos

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

ii) EU:n turvallisuusluokiteltuja tietoja ei avata matkalla eikä lueta julkisilla paikoilla;

iii) henkilöille selvitetään heidän turvallisuutta koskeva vastuunsa;

iv) henkilöille annetaan tarvittaessa kuriiritodistus;

c) postipalvelujen tai kaupallisten kuriiripalvelujen välityksellä, jos

i) asiaankuuluva kansallinen turvallisuusviranomainen on hyväksynyt ne kansallisten lakien ja asetusten mukaisesti;

ii) ne soveltavat asianmukaisia suojatoimenpiteitä 6 artiklan 2 kohdan nojalla laadittavissa turvallisuutta koskevissa suuntaviivoissa asetettavien vähimmäisvaatimusten mukaisesti.

Kuljetettaessa tietoja jäsenvaltiosta toiseen c alakohdan säännökset koskevat korkeintaan CONFIDENTIEL UE/EU CONDIFENTIAL -turvallisuusluokan tietoja.

34. CONFIDENTIEL UE/EU CONFIDENTIAL- ja SECRET UE/EU SECRET -turvallisuusluokkiin kuuluva aineisto (esimerkiksi laitteet tai koneet), joita ei voida kuljettaa 33 kohdassa tarkoitetuilla tavoilla, on kuljetettava rahtina kaupallisten rahdinkuljettajien välityksellä liitteen V mukaisesti.

35. TRES SECRET UE/EU TOP SECRET -turvallisuusluokan tiedot on kuljetettava rakennusten tai tilojen välillä EU:n alueella tapauksen mukaan sotilaskuriirilla, valtion kuriirilla tai diplomaattikuriirilla.

EU:sta kolmannen valtion alueelle

36. EU:sta kolmannen valtion alueelle kuljetettavat EU:n turvallisuusluokitellut tiedot on pakattava niin, että ne on suojattu luvattomalta ilmitulolta.

37. CONFIDENTIEL UE/EU CONFIDENTIAL- ja SECRET UE/EU SECRET -turvallisuusluokkien tiedot on kuljetettava EU:sta kolmannen valtion alueelle 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;

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

iv) EU:n turvallisuusluokiteltuja tietoja ei avata matkalla eikä lueta julkisilla paikoilla;

v) henkilöille selvitetään heidän turvallisuutta koskeva vastuunsa.

38. Kuljetettaessa EU:n kolmannelle valtiolle tai kansainväliselle järjestölle luovuttamia CONFIDENTIEL UE/EU CONFIDENTIAL- ja SECRET UE/EU SECRET -turvallisuusluokkien tietoja on noudatettava 12 artiklan 2 kohdan a alakohdan mukaisen tietoturvallisuussopimuksen tai b alakohdan mukaisen hallinnollisen järjestelyn asiaankuuluvia määräyksiä.

39. RESTREINT UE/EU RESTRICTED -turvallisuusluokan tietoja voidaan kuljettaa myös postipalvelujen tai kaupallisten kuriiripalvelujen välityksellä.

40. TRES SECRET UE/EU TOP SECRET -turvallisuusluokan tiedot on kuljetettava EU:sta kolmannen valtion alueelle sotilas- tai diplomaattikuriirilla.

VI EU:N TURVALLISUUSLUOKITELTUJEN TIETOJEN HÄVITTÄMINEN

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

42. 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.

43. SECRET UE/EU SECRET- tai TRES SECRET UE/EU TOP SECRET -turvallisuusluokan asiakirjojen hävittäminen on suoritettava todistajan läsnä ollessa. Todistajalla on oltava vähintään hävitettävän asiakirjan turvallisuusluokkaa vastaava turvallisuusselvitys.

44. Sekä kirjaajan että todistajan, jos jälkimmäisen läsnäoloa vaaditaan, 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.

45. Turvallisuusluokiteltujen asiakirjojen, myös RESTREINT UE/EU RESTRICTED -turvallisuusluokan 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.

46. EU:n turvallisuusluokiteltujen tietojen tallentamiseen käytetyt atk-tallennevälineet on hävitettävä liitteessä IV olevan 36 kohdan mukaisesti.

VII TARKASTUKSET JA ARVIOINTIKÄYNNIT

47. ”Tarkastuksella” tarkoitetaan jäljempänä

a) 9 artiklan 3 kohdan ja 15 artiklan 2 kohdan e, f ja g alakohdan mukaista tarkastusta tai

b) 12 artiklan 5 kohdan mukaista arviointikäyntiä,

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

48. Tarkastuksia tehdään muun muassa

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

b) turvallisuuden ja tehokkaan riskinhallinnan merkityksen korostamiseksi tarkastetuissa yksiköissä;

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

d) turvallisuusviranomaisten jatkuvan turvallisuuskoulutuksen ja tiedotusohjelmien tehostamiseksi.

49. 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

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

51. 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 turvallisuusluokiteltuja tietoja käsitellään, erityisesti kirjaamoihin ja viestintä- ja tietojärjestelmien sijoituspaikkoihin.

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

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

54. Euroopan unionin toiminnasta tehdyn sopimuksen V osaston 2 luvun nojalla perustettujen EU:n virastojen ja elinten sekä Europolin ja Eurojustin tarkastukset suorittaa pääsihteeristön turvallisuusyksikkö käyttäen viraston tai elimen sijaintijäsenvaltion kansallisen turvallisuusviranomaisen asiantuntija-apua. Euroopan komission turvallisuusosasto voi osallistua toimintaan, jos se vaihtaa säännöllisesti EU:n turvallisuusluokiteltuja tietoja kyseisen viraston tai elimen kanssa.

55. Kun tarkastuksia tehdään Euroopan unionin toiminnasta tehdyn sopimuksen V osaston 2 luvun nojalla perustetuissa EU:n virastoissa ja elimissä, Europolissa ja Eurojustissa sekä kolmansissa valtioissa ja kansainvälisissä järjestöissä, kansallisilta turvallisuusviranomaisilta pyydetään apua turvallisuuskomitean päättämien yksityiskohtaisten järjestelyjen mukaisesti.

Tarkastusraportit

56. 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.

57. Jäsenvaltioiden kansallisissa hallinnoissa suoritettavien tarkastusten osalta

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

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

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

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

59. Raportti Euroopan unionin toiminnasta tehdyn sopimuksen V osaston 2 luvun nojalla perustettuihin EU:n virastoihin ja elimiin sekä Europoliin ja Eurojustiin 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 -turvallisuusluokkaan kuuluvia tietoja. Mahdollisten korjaavien toimien toteuttaminen tarkistetaan seurantakäynnillä, ja siitä raportoidaan turvallisuuskomitealle.

60. Pääsihteeristön turvallisuusviranomainen suorittaa säännöllisin väliajoin pääsihteeristön organisaatioyksiköiden tarkastuksia 48 kohdan soveltamiseksi.

Tarkastusluettelo

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

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

LIITE IV

VIESTINTÄ- JA TIETOJÄRJESTELMISSÄ KÄSITELTÄVIEN EU:N TURVALLISUUSLUOKITELTUJEN 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 vilpittömässä mielessä toimivista lähteistä;

Käytettävyys: ominaisuus, että tiedot ovat pyynnöstä valtuutetun yksikön saatavilla ja käytettävissä;

Luottamuksellisuus: ominaisuus, että tiedot eivät paljastu sivullisille henkilöille, yksiköille eikä prosesseille;

Eheys: ominaisuus, että tietojen ja resurssien oikeellisuus ja täydellisyys turvataan;

Kiistämättömyys: kyky todistaa tietty toimi tai tapahtuma tapahtuneeksi niin, ettei tapahtumaa tai toimea voida myöhemmin kiistää.

II TIEDONTURVAAMISPERIAATTEET

3. Jäljempänä esitetyt säännökset muodostavat kaikkien EU:n turvallisuusluokiteltuja 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 turvallisuusjärjestelyjen hyväksyntäviranomaisen 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 turvallisuusluokiteltujen tietojen turvallisuusluokka. Hyväksyntään on liitettävä vastuuviranomaisen 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. Käyttöajan 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 turvallisuusasiakirjoja on kehitettävä 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 turvallisuusluokiteltujen 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 turvallisuusluokiteltujen tietojen suojaamisessa on hyödynnettävä tietojen turvaamiseen 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 turvallisuusluokiteltuja 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 torjumaan mahdolliset vihamieliset suunnitelmat viestintä- ja tietojärjestelmään kohdistuvasta hyökkäyksestä;

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 hyökkäyksen vaikutukset mahdollisimman pieneen osaan tietoja tai viestintä- ja tietojärjestelmän resursseja ja estämään muut vahingot;

e) *tilanteen 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 (tietotekniset hätävalmiudet).

Vähimmäistoimintojen ja pienimmän mahdollisen etuoikeuden periaate

18. Tarpeettoman riskin välttämiseksi on otettava käyttöön 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;

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

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

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 turvallisuusluokiteltujen 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 turvallisuusluokasta, johon kuuluvia EU:n turvallisuusluokiteltuja 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 turvallisuusluokiteltujen tietojen suojaamiseen tarkoitettujen salaustuotteiden toinen arviointi.

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

Tietojen lähettäminen turva-alueilla

30. Sen estämättä, mitä tässä päätöksessä säädetään, jos EU:n turvallisuusluokiteltujen tietojen lähettäminen tapahtuu turva-alueilla, salaamatonta jakelua tai alemman tason salausta voidaan käyttää riskinhallintaprosessin tulosten perusteella ja turvallisuusjärjestelyjen hyväksyntäviranomaisen 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 turvallisuusluokiteltujen 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 turvallisuusjärjestelyjen hyväksyntäviranomaisella;

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 turvallisuusjärjestelyjen hyväksyntäviranomaisen 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 -turvallisuusluokiteltujen tietojen käsittelyyn hyväksytyn viestintä- ja tietojärjestelmän välitön tai porrastettu yhteenliitäntä suojaamattoman tai julkisen verkon kanssa on kiellettyä.

Atk-tallennevälineet

36. Atk-tallennevälineet on hävitettävä toimivaltaisen turvallisuusviranomaisen hyväksymien menettelyjen mukaisesti.

37. Atk-tallennevälineitä voidaan käyttää uudelleen, niiden turvallisuusluokkaa voidaan alentaa tai se voidaan poistaa 6 artiklan 1 kohdan nojalla vahvistettavien turvallisuutta koskevien periaatteiden mukaisesti.

Hätätilanteet

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

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

a) lähettäjällä ja vastaanottajalla ei ole vaadittua salauslaitetta tai ei mitään salauslaitetta; ja

b) turvallisuusluokiteltua aineistoa ei voida toimittaa perille ajoissa muulla tavoin.

40. Edellä 38 kohdassa esitetyissä olosuhteissa lähetetyissä turvallisuusluokitelluissa tiedoissa ei saa olla mitään merkintöjä eikä mainintoja, jotka erottavat ne turvallisuusluokittelemattomista tiedoista tai tiedoista, jotka voidaan suojata käytettävissä olevalla salaustuotteella. Tietojen vastaanottajille on ilmoitettava turvallisuusluokasta viipymättä muulla tavoin.

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

III TIEDONTURVAAMISTEHTÄVÄT JA -VIRANOMAISET

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

Tiedonturvaamisviranomainen

43. 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 turvallisuusluokiteltujen 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 tietoisuuden koordinoinnista;

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

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

TEMPEST-viranomainen

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

Salauslaitteiden hyväksyntäviranomainen

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

Salatun aineiston jakelusta vastaava viranomainen

46. 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;

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

Turvallisuusjärjestelyjen hyväksyntäviranomainen

47. Kunkin järjestelmän turvallisuusjärjestelyjen hyväksyntäviranomainen 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 turvallisuusluokiteltuja tietoja voidaan käsitellä tiettyyn turvallisuusluokkaan 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;

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

48. Pääsihteeristön turvallisuusjärjestelyjen hyväksyntäviranomainen vastaa kaikkien pääsihteeristön toimivallan puitteissa käytettävien viestintä- ja tietojärjestelmien hyväksymisestä.

49. Jäsenvaltion asiaankuuluva turvallisuusjärjestelyjen hyväksyntäviranomainen vastaa jäsenvaltion toimivallan puitteissa käytettävien viestintä- ja tietojärjestelmien ja niiden osien hyväksymisestä.

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

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

Operatiivinen tiedonturvaamisviranomainen

51. 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 sekä tarvittaessa operatiivisen turvallisuusvastuun siirtämisestä 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 turvallisuusjärjestelyjen hyväksyntäviranomaisen vaatimien asiaankuuluvien riskiraporttien laatimiseksi;

g) viestintä- ja tietojärjestelmäkohtaisen tiedonturvaamiskoulutuksen antamisesta;

h) viestintä- ja tietojärjestelmäkohtaisten turvatoimien toteuttamisesta ja käytöstä.

LIITE V

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 turvallisuusluokiteltujen sopimusten koko elinkaaren ajan.

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

II TURVALLISUUSLUOKITELLUN SOPIMUKSEN TURVALLISUUTTA KOSKEVAT OSAT

Turvallisuusluokitusopas

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

4. Turvallisuusluokitellun sopimuksen eri osien turvallisuusluokan määrittämiseksi sovelletaan seuraavia periaatteita:

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

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

   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 turvallisuusluokkaa muutetaan ja että turvallisuusluokitusoppaaseen tehdään tämän vuoksi muutoksia.

Turvallisuutta koskeva lisälauseke

5. Sopimuskohtaiset turvallisuusvaatimukset on ilmoitettava turvallisuutta koskevassa lisälausekkeessa. Turvallisuutta koskevan lisälausekkeen on tarvittaessa sisällettävä turvallisuusluokitusopas, ja sen on oltava erottamaton osa turvallisuusluokiteltua 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 turvallisuusluokiteltuihin 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 turvallisuusluokkaan (CONFIDENTIEL UE/EU CONFIDENTIAL- tai SECRET UE/EU SECRET) kuuluvat EU:n turvallisuusluokitellut tiedot toimitiloissaan. Yhteisöturvallisuusselvitys on esitettävä hankeviranomaisena toimivalle pääsihteeristölle ennen kuin hankeosapuolelle tai alihankkijalle taikka mahdolliselle hankeosapuolelle tai alihankkijalle voidaan luovuttaa EU:n turvallisuusluokiteltuja 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 toimipaikassaan käyttöön turvallisuusjärjestelmän, joka kattaa kaikki asianmukaiset CONFIDENTIEL UE/EU CONFIDENTIAL- tai SECRET UE/EU SECRET -turvallisuusluokan tietojen tai aineistojen suojaamisen edellyttämät turvatoimet tässä päätöksessä säädettyjen vaatimusten mukaisesti;

d) tarkistettava, että johtohenkilöstön, omistajien ja työntekijöiden, joiden tehtävät edellyttävät pääsyä CONFIDENTIEL UE/EU CONFIDENTIAL- tai SECRET UE/EU SECRET -turvallisuusluokkaan kuuluviin tietoihin, henkilöstöturvallisuus on selvitetty tämän päätöksen 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 -turvallisuusluokan tietoja.

11. Hankeviranomainen ei saa tehdä turvallisuusluokiteltua sopimusta valitun tarjoajan kanssa ennen kuin se on saanut sen jäsenvaltion kansalliselta tai nimetyltä turvallisuus-viranomaiselta 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 yhteisöturvallisuus-selvitykseen vaikuttavista muutoksista. Kun kyseessä on alihankintasopimus, kansalliselle tai nimetylle turvallisuusviranomaiselle tai muulle toimivaltaiselle turvallisuus-viranomaiselle on ilmoitettava vastaavasti.

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

IV TURVALLISUUSLUOKITELLUT SOPIMUKSET JA ALIHANKINTASOPIMUKSET

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

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

16. Kun tällaiset sopimukset irtisanotaan, 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 turvallisuusluokitellun sopimuksen tai alihankintasopimuksen päättyessä kaikki hallussaan olevat EU:n turvallisuusluokitellut tiedot.

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

19. Jos hankeosapuoli tai alihankkija saa luvan säilyttää EU:n turvallisuusluokiteltuja tietoja sopimuksen päätyttyä, tässä päätöksessä säädettyjä vähimmäisvaatimuksia on yhä noudatettava, ja hankeosapuolen tai alihankkijan on suojattava EU:n turvallisuusluokiteltujen 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 turvallisuusluokitellun 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 turvallisuusluokiteltuja tietoja alihankkijalle ilman hankeviranomaisen kirjallista etukäteissuostumusta.

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

V TURVALLISUUSLUOKITELTUIHIN SOPIMUKSIIN LIITTYVÄT VIERAILUT

24. Jos pääsihteeristön, hankeosapuolien tai alihankkijoiden on saatava CONFIDENTIEL UE/EU CONFIDENTIAL- tai SECRET UE/EU SECRET -turvallisuusluokan tietoja toistensa toimitiloissa turvallisuusluokitellun 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 turvallisuusluokiteltuihin tietoihin.

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

VI EU:N TURVALLISUUSLUOKITELTUJEN TIETOJEN LÄHETTÄMINEN JA KULJETTAMINEN

27. EU:n turvallisuusluokiteltujen tietojen lähettämiseen sähköisesti sovelletaan 10 artiklassa ja liitteessä IV olevia asiaankuuluvia säännöksiä.

28. EU:n turvallisuusluokiteltujen tietojen kuljettamiseen sovelletaan liitteessä III olevia asiaankuuluvia säännöksiä kansallisten lakien ja asetusten mukaisesti.

29. Kuljetettaessa turvallisuusluokiteltua aineistoa rahtina sovelletaan seuraavia periaatteita turvallisuusjärjestelyjä määritettäessä:

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

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

c) kuljetuksen suorittaville yrityksille on hankittava asianmukaisen tason yhteisöturvallisuusselvitys. Tällaisissa tapauksissa lähetystä käsittelevällä henkilöstöllä on oltava liitteen I mukainen turvallisuusselvitys;

d) lähettäjän on ennen CONFIDENTIEL UE/EU CONFIDENTIAL- tai SECRET UE/EU SECRET -turvallisuusluokitellun 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 lähettäjän valtion että vastaanottajan valtion kansallisen tai nimetyn turvallisuusviranomaisen tai muun toimivaltaisen turvallisuusviranomaisen lupa.

VII EU:N TURVALLISUUSLUOKITELTUJEN TIETOJEN LÄHETTÄMINEN KOLMANSISSA VALTIOISSA SIJAITSEVILLE HANKEOSAPUOLILLE

30. EU:n turvallisuusluokiteltuja 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 -TURVALLISUUSLUOKAN 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 -turvallisuusluokan EU:n turvallisuusluokiteltujen tietojen suojaamiseksi on toteutettu.

32. Hankeviranomaisena toimivan pääsihteeristön on annettava kansallisille tai nimetyille turvallisuusviranomaisille tai muulle toimivaltaiselle turvallisuusviranomaiselle tiedoksi RESTREINT UE/EU RESTRICTED -turvallisuusluokan tietoja sisältävät sopimukset tai alihankintasopimukset siinä laajuudessa kuin 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 -turvallisuusluokan tietoja.

34. Hankeviranomaisena toimivan pääsihteeristön on tutkittava tarjouspyyntöihin saadut vastaukset, jos sopimuksen tekeminen edellyttää RESTREINT UE/EU RESTRICTED -turvallisuusluokan tietojen saamista, sellaisten vaatimusten estämättä, 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 -turvallisuusluokan 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 asianomaisen kansallisen tai nimetyn turvallisuusviranomaisen kesken.

LIITE VI

TURVALLISUUSLUOKITELTUJEN TIETOJEN VAIHTO KOLMANSIEN VALTIOIDEN JA KANSAINVÄLISTEN JÄRJESTÖJEN KANSSA

I JOHDANTO

1. Tässä liitteessä vahvistetaan 12 artiklan täytäntöönpanosäännökset.

II TURVALLISUUSLUOKITELTUJEN TIETOJEN VAIHDON PUITTEET

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

— tehdään tietoturvallisuussopimus, tai

— sovitaan hallinnollisesta järjestelystä

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

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

— osallistumista koskevaa puitesopimusta;

— osallistumista koskevaa erillissopimusta; tai

— jos kumpaakaan edellä mainituista ei ole tehty, hallinnollista erillisjärjestelyä.

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

III TIETOTURVALLISUUSSOPIMUKSET

5. Tietoturvallisuussopimuksissa on määrättävä perusperiaatteista ja vähimmäisvaatimuksista, joita sovelletaan turvallisuusluokiteltujen 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 turvallisuus-viranomaisen kesken. Täytäntöönpanojärjestelyissä on otettava huomioon asianomaisessa kolmannessa valtiossa tai kansainvälisessä järjestössä sovellettavien turvallisuussääntöjen, -rakenteiden ja -menettelyjen tarjoaman suojan taso. Ne on hyväksyttävä turvallisuus-komiteassa.

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

8. Tietoturvallisuussopimuksissa on määrättävä, että ennen sopimuksen mukaista turvallisuusluokiteltujen 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 turvallisuusluokiteltujen tietojen vaihtoa varten.

10. Asianomaisen kolmannen valtion tai kansainvälisen järjestön turvallisuussääntöjen, -rakenteiden ja -menettelyjen toimivuuden arvioimiseksi pääsihteeristön turvallisuus-yksikön 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) turvallisuusluokiteltujen tietojen suojaamiseen sovellettavia sääntelypuitteita;

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

c) tosiasiallisesti käytössä olevia turvatoimia ja turvallisuusmenettelyjä;

d) luovutettavien EU:n turvallisuusluokiteltujen tietojen turvallisuusluokkaan 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 turvallisuusluokitellut tiedot määrätyssä turvallisuusluokassa.

12. Arviointikäyntien havainnot on esitettävä raportissa, jonka perusteella turvallisuuskomitea määrittelee korkeimman turvallisuusluokan, johon kuuluvia EU:n turvallisuusluokiteltuja 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 turvallisuus-järjestelmän 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 turvallisuusluokiteltuja tietoja ei saa luovuttaa ennen kuin arviointikäynnin tulosten tarkastelu on saatu päätökseen, tai että niitä saa luovuttaa vain tiettyyn turvallisuusluokkaan asti. Se voi myös määrätä muita erityisiä ehtoja EU:n turvallisuusluokiteltujen 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 turvallisuusluokiteltuja tietoja, turvallisuuskomitea voi päättää muuttaa korkeinta turvallisuusluokkaa, johon kuuluvia EU:n turvallisuusluokiteltuja 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 turvallisuusluokka 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 turvallisuusluokiteltujen tietojen vaihtoa varten on kiireellisistä toiminnallisista syistä perustettava puitteet nopeasti, neuvosto voi poikkeuksellisesti päättää, että korkeampaan turvallisuusluokkaan kuuluvien tietojen vaihtoon voidaan käyttää hallinnollista järjestelyä.

19. Hallinnollisista järjestelyistä sovitaan pääsääntöisesti kirjeenvaihtona.

20. EU:n turvallisuusluokiteltuja 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 turvallisuusluokiteltuja tietoja saa kuitenkin luovuttaa, jos turvallisuusluokiteltujen tietojen kiireelliseen vaihtoon on poikkeuksellisia syitä, joista neuvostolle on ilmoitettu, edellyttäen, että tällainen arviointikäynti pyritään kaikin tavoin tekemään mahdollisimman pian.

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

V TURVALLISUUSLUOKITELTUJEN 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 turvallisuusluokiteltujen tietojen luovuttamisesta osallistuville kolmansille valtioille tai kansainvälisille järjestöille. Korkein turvallisuusluokka, johon kuuluvia EU:n turvallisuusluokiteltuja tietoja voidaan vaihtaa, saa olla RESTREINT UE/EU RESTRICTED ETPP-siviilioperaatioiden osalta ja CONFIDENTIEL UE/EU CONFIDENTIAL ETPP-sotilasoperaatioiden osalta, jollei kyseisen ETPP-operaation perustamista koskevassa päätöksessä toisin määrätä.

23. Tiettyä ETPP-operaatiota varten tehtyihin osallistumista koskeviin erillissopimuksiin on sisällytettävä määräyksiä kyseistä operaatiota varten tuotettujen EU:n turvallisuusluokiteltujen tietojen luovuttamisesta osallistuvalle kolmannelle valtiolle tai kansainväliselle järjestölle. Korkein turvallisuusluokka, johon kuuluvia EU:n turvallisuusluokiteltuja tietoja voidaan vaihtaa, saa olla RESTREINT UE/EU RESTRICTED ETPP-siviilioperaatioiden osalta ja CONFIDENTIEL UE/EU CONFIDENTIAL ETPP-sotilasoperaatioiden osalta, jollei kyseisen ETPP-operaation perustamista koskevassa päätöksessä toisin määrätä.

24. Kolmannen valtion tai kansainvälisen järjestön osallistumista määrättyyn ETPP-operaatioon koskevissa hallinnollisissa erillisjärjestelyissä voidaan määrätä muun muassa operaatiota varten tuotettujen EU:n turvallisuusluokiteltujen tietojen luovuttamisesta kyseiselle kolmannelle valtiolle tai kansainväliselle järjestölle. Tällaisista hallinnollisista erillisjärjestelyistä on sovittava edellä IV jaksossa olevassa 17 ja 18 kohdassa säädettyjen menettelyjen mukaisesti. Korkein turvallisuusluokka, johon kuuluvia EU:n turvallisuusluokiteltuja tietoja voidaan vaihtaa, saa olla RESTREINT UE/EU RESTRICTED ETPP-siviilioperaatioiden osalta ja CONFIDENTIEL UE/EU CONFIDENTIAL ETPP-sotilasoperaatioiden osalta, jollei kyseisen ETPP-operaation perustamista koskevassa päätöksessä toisin määrätä.

25. Ennen EU:n turvallisuusluokiteltujen 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 turvallisuusluokiteltujen tietojen vaihtoa varten, voidaan perustaa hallinnollinen erillisjärjestely siinä tapauksessa, että siihen on erityinen ja välitön toiminnallinen tarve. Tästä mahdollisuudesta on määrättävä ETPP-operaation perustamista koskevassa päätöksessä. Kyseisissä olosuhteissa luovutettavat EU:n turvallisuusluokitellut tiedot on rajoitettava ETPP-operaatiota varten tuotettuihin tietoihin, jotka kuuluvat korkeintaan RESTREINT UE/EU RESTRICTED -turvallisuusluokkaan. Isäntävaltion on tällaisessa hallinnollisessa erillisjärjestelyssä sitouduttava suojaamaan EU:n turvallisuusluokitellut 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 erillissopimusten ja hallinnollisten erillisjärjestelyjen turvallisuusluokiteltuja tietoja koskevissa osissa on määrättävä, että kyseisen kolmannen valtion tai kansainvälisen järjestön on varmistettava, että sen mihin tahansa operaatioon lähettämä henkilöstö suojaa EU:n turvallisuusluokitellut tiedot neuvoston turvallisuus-sääntöjen 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 erillissopimuksen tai hallinnollisen erillisjärjestelyn EU:n turvallisuusluokiteltujen tietojen vaihdon ja käsittelyn osalta.

29. EU:n turvallisuusluokiteltuja tietoja ei saa vaihtaa sähköisesti kolmannen valtion tai kansainvälisen järjestön kanssa tehdyn osallistumista koskevan puitesopimuksen, osallistumista koskevan erillissopimuksen eikä hallinnollisen erillisjärjestelyn nojalla, ellei siitä nimenomaisesti määrätä kyseisessä sopimuksessa tai järjestelyssä.

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

VI EU:N TURVALLISUUSLUOKITELTUJEN 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 turvallisuusluokiteltujen 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 turvallisuusluokiteltujen 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 turvallisuusluokiteltuja tietoja on tarkoitus luovuttaa.

32. Jos turvallisuuskomitea antaa suosituksen EU:n turvallisuusluokiteltujen tietojen luovuttamiseksi, asia siirretään pysyvien edustajien komitealle (Coreper), joka päättää tietojen luovuttamisesta.

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

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

b) kaikissa muissa asioissa Coreper keskustelee ja päättää asiasta.

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

35. Kun EU:n turvallisuusluokiteltujen 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 turvallisuusluokitellut tiedot tässä päätöksessä säädettyjen perusperiaatteiden ja vähimmäisvaatimusten mukaisesti.

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

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

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

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

Lisäykset

Lisäys A

Määritelmät

Lisäys B

Turvallisuusluokkien vastaavuus

Lisäys C

Luettelo kansallisista turvallisuusviranomaisista

Lisäys D

Lyhenneluettelo

Lisäys A

MÄÄRITELMÄT

Tässä päätöksessä sovelletaan seuraavia määritelmiä:

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

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

”ETPP-operaatiolla” tarkoitetaan Euroopan unionin toiminnasta tehdyn sopimuksen V osaston 2 luvun nojalla toteutettavaa sotilas- tai siviilikriisinhallintaoperaatiota.

”Turvallisuusluokan poistamisella” tarkoitetaan minkä tahansa turvallisuusluokan poistamista.

”EU:n turvallisuusluokitellut tiedot” – ks. 2 artiklan 1 kohta.

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

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

”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.

”Hankeosapuolella” tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, joka on oikeudellisesti kelpoinen tekemään sopimuksia.

”Henkilöstöturvallisuus” – ks. 7 artiklan 1 kohta.

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

”Henkilöturvallisuusselvityksellä” tarkoitetaan jompaakumpaa seuraavista tai molempia:

— ”EU:n henkilöturvallisuusselvityksellä” (EU-turvallisuusselvitys) EU:n turvallisuusluokiteltujen tietojen saamista varten tarkoitetaan pääsihteeristön nimitysvallan käyttäjän valtuutusta, joka annetaan tämän päätöksen mukaisesti jäsenvaltion toimivaltaisten viranomaisten tekemän turvallisuustutkinnan jälkeen ja jonka nojalla henkilölle voidaan myöntää oikeus saada EU:n turvallisuusluokiteltuja tietoja määrättyyn turvallisuusluokkaan (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 turvallisuusluokiteltujen tietojen saamista varten tarkoitetaan jäsenvaltion toimivaltaisen viranomaisen lausuntoa, joka annetaan jäsenvaltion toimivaltaisten viranomaisten tekemän turvallisuustutkinnan jälkeen ja jonka nojalla henkilölle voidaan myöntää oikeus saada EU:n turvallisuusluokiteltuja tietoja määrättyyn turvallisuusluokkaan (CONFIDENTIEL UE/EU CONFIDENTIAL tai korkeampi) ja tiettyyn päivämäärään saakka edellyttäen, että hänen tiedonsaantitarpeensa on todettu. Henkilön katsotaan tämän jälkeen olevan ”turvallisuusselvitetty”.

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

”Jäännösriskillä” tarkoitetaan riskiä, joka jää jäljelle, kun turvatoimet on toteutettu, ottaen huomioon, että kaikkia uhkia ei pystytä torjumaan eikä kaikkea haavoittuvuutta voida poistaa.

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

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

”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.

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

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

”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.

— ”Riskinarviointi” koostuu uhkien ja haavoittuvuuden tunnistamisesta ja niihin liittyvän riskianalyysin eli todennäköisyyden ja vaikutusten analyysin tekemisestä.

— ”Riskin hyväksyminen” on päätös hyväksyä jäännösriskin olemassaolo riskin käsittelyn jälkeen.

— ”Riskin käsittely” muodostuu riskin lieventämisestä, poistamisesta, vähentämisestä (yhdistämällä asianmukaisesti teknisiä, fyysisiä, organisatorisia tai menettelyyn liittyviä toimenpiteitä), siirtämisestä ja seurannasta.

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

”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.

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

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

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

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

— ”Korkean turvallisuustason toimintatavalla” tarkoitetaan toimintatapaa, jossa kaikille viestintä- ja tietojärjestelmään pääseville henkilöille tehdään turvallisuusselvitys järjestelmässä käsiteltävien tietojen korkeimman turvallisuusluokan mukaan, mutta kaikilla järjestelmään pääsevillä henkilöillä ei ole yhteistä tarvetta saada järjestelmässä käsiteltäviä tietoja. Henkilöt voivat myöntää pääsyn tietoihin.

— ”Monitasoisella toimintatavalla” tarkoitetaan toimintatapaa, jossa kaikille viestintä- ja tietojärjestelmään pääseville henkilöille ei tehdä turvallisuusselvitystä järjestelmässä käsiteltävien tietojen korkeimman turvallisuusluokan mukaan, ja kaikilla järjestelmään pääsevillä henkilöillä ei ole yhteistä tarvetta saada järjestelmässä käsiteltäviä tietoja.

— ”Osastokohtaisella toimintatavalla” tarkoitetaan toimintatapaa, jossa kaikille viestintä- ja tietojärjestelmään pääseville henkilöille tehdään turvallisuusselvitys järjestelmässä käsiteltävien tietojen korkeimman turvallisuusluokan 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.

— ”Yleisvaltuutuksella” tarkoitetaan toimintatapaa, jossa kaikille viestintä- ja tietojärjestelmään pääseville henkilöille tehdään turvallisuusselvitys järjestelmässä käsiteltävien tietojen korkeimman turvallisuusluokan mukaan ja henkilöillä on yhteinen tarve saada KAIKKI järjestelmässä käsiteltävät tiedot.

”Turvallisuusluokan alentamisella” tarkoitetaan turvallisuusluokituksen tason alentamista.

”Turvallisuusluokitellulla 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 turvallisuusluokiteltuihin tietoihin pääsemistä tai niiden tuottamista.

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

”Turvallisuusluokiteltujen tietojen hallinnointi” – ks. 9 artiklan 1 kohta.

”Turvallisuusluokitusoppaalla” tarkoitetaan asiakirjaa, jossa kuvataan turvallisuusluokitellun ohjelman tai sopimuksen osat ja eritellään sovellettavat turvallisuusluokat. Turvallisuus-luokitusopasta voidaan laajentaa ohjelman tai sopimuksen koko keston ajan, ja sen sisältämien tietojen turvallisuusluokat voidaan määritellä uudelleen tai niitä voidaan alentaa. Jos turvallisuusluokitusopas on olemassa, sen on oltava osa turvallisuutta koskevaa lisälauseketta.

”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.

”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 turvallisuusluokiteltujen tietojen saamista varten tiettyyn turvallisuusluokkaan saakka (CONFIDENTIEL UE/EU CONFIDENTIAL tai korkeampi).

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

”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.

”Viestintä- ja tietojärjestelmä” – ks. 10 artiklan 2 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.

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

”Yhteisöturvallisuus” – ks. 11 artiklan 1 kohta.

”Yhteisöturvallisuusselvityksellä” tarkoitetaan kansallisen tai nimetyn turvallisuusviranomaisen hallinnollista päätöstä, jonka mukaan yhteisö tarjoaa turvallisuuden kannalta riittävän suojan tiettyyn turvallisuusluokkaan kuuluville EU:n turvallisuusluokitelluille tiedoille ja jonka mukaan kyseisessä yhteisössä työskentelevälle henkilöstölle, jonka tehtävät edellyttävät EU:n turvallisuusluokiteltuihin tietoihin pääsemistä, on tehty asianmukainen turvallisuusselvitys ja selvitetty EU:n turvallisuusluokiteltuihin tietoihin pääsemisen ja niiden suojaamisen edellyttämät asiaankuuluvat turvallisuusvaatimukset.

”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.

Lisäys B

TURVALLISUUSLUOKKIEN 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
Tšekki	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
Irlanti	Top Secret	Secret	Confidential	Restricted
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*
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-Oġħla 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	Strict secret de importanţă deosebită	Strict secret	Secret	Secret de serviciu

EU	TRES SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
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	Confidential	Restricted

([1]) Diffusion Restreinte/Beperkte Verspreiding ei ole Belgiassa turvallisuusluokka. 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 turvallisuusluokkaa 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 turvallisuusluokitusmerkintöjä käyttävät puolustusviranomaiset, ja alemmalla rivillä olevia merkintöjä käyttävät muut viranomaiset.

Lisäys C

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
Faksi: + 32 2 501 45 96
Sähköposti: nvo-ans@diplobel.fed.be

BULGARIA
State Commission on Information Security
90 Cherkovna Str.
BG-1505 Sofia

Puhelin: + 359 2 921 5911
Faksi: + 359 2 987 3750
Sähköposti: dksi@government.bg
Verkkosivut: www.dksi.bg

TŠEKKI
Národní bezpečnostní úřad
(National Security Authority)
Na Popelce 2/16
CZ-150 06 Praha 56

Puhelin: + 420 257 28 33 35
Faksi: + 420 257 28 31 10
Sähköposti: czech.nsa@nbu.cz
Verkkosivut: www.nbu.cz

IRLANTI
National Security Authority
Department of Foreign Affairs
76 - 78 Harcourt Street
Dublin 2 Ireland

Puhelin: + 353 1 478 08 22
Faksi: + 353 1 408 29 59

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

TANSKA
Politiets Efterretningstjeneste
(Danish Security Intelligence Service)
Klausdalsbrovej 1
DK-2860 Søborg

Puhelin: + 45 33 14 88 88
Faksi: + 45 33 43 01 90

Forsvarets Efterretningstjeneste
(Danish Defence Intelligence Service)
Kastellet 30
DK-2100 Copenhagen Ø

Puhelin: + 45 33 32 55 66
Faksi: + 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
Faksi: + 49 30 18 681 1441
Sähköposti: oesIII3@bmi.bund.de

VIRO
National Security Authority Department
Estonian Ministry of Defence
Sakala 1
EE-15094 Tallinn

Puhelin: +372 7170 113, +372 7170 117
Faksi: +372 7170 213
Sähköposti: nsa@kmin.ee

ESPANJA
Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
E-28023 Madrid

Puhelin: + 34 91 372 50 00
Faksi: + 34 91 372 58 08
Sähköposti: nsa-sp@areatec.com

RANSKA
Secrétariat général de la défense et de la sécurité nationale
Sous-direction Protection du secret (SGDSN/PSD)
51 Boulevard de la Tour-Maubourg
F-75700 Paris 07 SP

Puhelin: + 33 1 71 75 81 77
Faksi: + 33 1 71 75 82 00

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
Faksi: + 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
Faksi: + 357 22 30 23 51
Sähköposti: cynsa@mod.gov.cy

LUXEMBURG
Autorité nationale de Sécurité
Boîte postale 2379
L-1023 Luxembourg

Puhelin: + 352 2478 22 10 keskus
+ 352 2478 22 53 ohivalinta
Faksi: + 352 2478 22 43

UNKARI
Nemzeti Biztonsági Felügyelet
(National Security Authority)
P.O. Box 2
HU-1357 Budapest

Puhelin: + 361 346 96 52
Faksi: + 361 346 96 58
Sähköposti: nbf@nbf.hu
Verkkosivut: www.nbf.hu

MALTA
Ministry of Justice and Home Affairs
P.O. Box 146
MT-Valletta

Puhelin: + 356 21 24 98 44
Faksi: + 356 25 69 53 21

LATVIA
National Security Authority
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
Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija
The Commission for Secrets Protection Coordination of the Republic of Lithuania
(National Security Authority)
Gedimino 40/1
LT-01110 Vilnius

Puhelin: + 370 5 266 32 01,
+370 5 266 32 02
Faksi: + 370 5 266 32 00
Sähköposti: nsa@vsd.lt

ALANKOMAAT
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20010
NL-2500 EA Den Haag

Puhelin: + 31 70 320 44 00
Faksi: + 31 70 320 07 33

Ministerie van Defensie
Beveiligingsautoriteit
Postbus 20701
NL-2500 ES Den Haag

Puhelin: + 31 70 318 70 60
Faksi: + 31 70 318 75 22

ITÄVALTA
Informationssicherheitskommission
Bundeskanzleramt
Ballhausplatz 2
A-1014 Wien

Puhelin: + 43 1 531 15 25 94
Faksi: + 43 1 531 15 26 15
Sähköposti: ISK@bka.gv.at

PUOLA
Agencja Bezpieczeństwa Wewnętrznego – ABW
(Internal Security Agency)
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

Służba Kontrwywiadu Wojskowego
(Military Counter-Intelligence Service)
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

ROMANIA
Oficiul Registrului Național al Informațiilor Secrete de Stat
(Romanian NSA – ORNISS
National Registry Office for Classified Information)
4 Mures Street
RO-012275 Bucharest

Puhelin: + 00 4 0 21 224 58 30
Faksi: + 00 4 0 21 224 07 14
Sähköposti: nsa.romania@nsa.ro
Verkkosivut: www.orniss.ro

PORTUGALI
Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Rua da Junqueira, 69
P-1300-342 Lisboa

Puhelin: +351 213 031 710
Faksi: +351 213 031 711

SLOVENIA
Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
SVN-1000 Ljubljana

Puhelin: + 386 1 478 13 90
Faksi: + 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
Faksi: + 421 2 63 82 40 05
Verkkosivut: www.nbusr.sk

RUOTSI
Utrikesdepartementet
(Ministry for Foreign Affairs)
SSSB
S-103 39 Stockholm

Puhelin: + 46 8 405 10 00
Faksi: + 46 8 723 11 76
Sähköposti: ud-nsa@foreign.ministry.se

SUOMI
Ulkoasiainministeriö
Kansallinen turvallisuusviranomainen
PL 453
00023 Valtioneuvosto

Puhelin 1: + 358 916056487
Puhelin 2: +358 916056484
Faksi: + 358 916055140
Sähköposti: NSA@formin.fi

YHDISTYNYT KUNINGASKUNTA
UK National Security Authority
Room 335, 3rd Floor
70 Whitehall
London
SW1A 2AS

Puhelin 1: + 44 20 7276 5649
Puhelin 2: + 44 20 7276 5497
Faksi: + 44 20 7276 5651
Sähköposti: UK-NSA@cabinet-office.x.gsi.gov.uk

Lisäys D

LYHENNELUETTELO

Lyhenne	Merkitys
AQUA-viranomainen	asianmukaisesti pätevä viranomainen
Coreper	Pysyvien edustajien komitea
ETPP	Euroopan turvallisuus- ja puolustuspolitiikka
YUTP	yhteinen ulko- ja turvallisuuspolitiikka