# KOMISSION PÄÄTÖS (EU, Euratom) 2015/444,

## annettu 13 päivänä maaliskuuta 2015,

## EU:n turvallisuusluokiteltujen tietojen suojaamista koskevista säännöistä

EUROOPAN KOMISSIO, joka

ottaa huomioon Euroopan unionin toiminnasta tehdyn sopimuksen ja erityisesti sen 249 artiklan,

ottaa huomioon Euroopan atomienergiayhteisön perustamissopimuksen ja erityisesti sen 106 artiklan,

ottaa huomioon Euroopan unionin erioikeuksista ja vapauksista tehdyn, perussopimuksiin liitetyn pöytäkirjan N:o 7 ja erityisesti sen 18 artiklan,

sekä katsoo seuraavaa:

(1) Euroopan unionin turvallisuusluokiteltujen tietojen suojaamista koskevia komission määräyksiä on tarkistettava ja päivitettävä institutionaalinen ja organisatorinen kehitys sekä toiminnan ja teknologian kehitys huomioon ottaen.

(2) Komissio on tehnyt Belgian, Luxemburgin ja Italian hallitusten kanssa sopimukset [1] sen pääasiallisia toimipaikkoja koskevista turvallisuusasioista.

(3) Komissio, neuvosto ja Euroopan ulkosuhdehallinto ovat sitoutuneet soveltamaan samanlaisia turvallisuusvaatimuksia EU:n turvallisuusluokiteltujen tietojen suojaamisessa.

(4) On tärkeää, että myös Euroopan parlamentti ja muut EU:n toimielimet, elimet ja laitokset soveltavat tarvittaessa turvallisuusluokiteltujen tietojen suojaamista koskevia periaatteita, vaatimuksia ja sääntöjä, jotka ovat välttämättömiä unionin ja sen jäsenvaltioiden etujen suojaamiseksi.

(5) 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 toimia syvyyssuuntaisen turvallisuuden käsitteen pohjalta. Turvatoimien tehokkuutta on arvioitava jatkuvasti.

(6) Turvallisuusluokiteltujen tietojen suojaamiseen tähtäävällä fyysisellä turvallisuudella tarkoitetaan komissiossa sellaisten fyysisten ja teknisten suojatoimien toteuttamista, joiden tarkoituksena on estää luvaton pääsy EU:n turvallisuusluokiteltuihin tietoihin.

(7) EU:n turvallisuusluokiteltujen tietojen hallinnoinnilla tarkoitetaan hallinnollisten toimien toteuttamista EU:n turvallisuusluokiteltujen tietojen valvomiseksi koko niiden elinkaaren ajan. Kyseisillä toimilla täydennetään tämän päätöksen 2, 3 ja 5 luvussa säädettyjä toimia ja autetaan siten estämään ja havaitsemaan tällaisten tietojen tahallinen tai tahaton vaarantuminen tai häviäminen sekä korjaamaan vaarantumisesta tai häviämisestä aiheutunut tilanne. Tällaiset toimet koskevat erityisesti EU:n turvallisuusluokiteltujen tietojen tuottamista, säilyttämistä, rekisteröintiä, jäljentämistä, kääntämistä, kuljettamista, hävittämistä sekä niiden turvallisuusluokan alentamista ja poistamista, ja ne täydentävät komission asiakirjahallintoa koskevia yleisiä sääntöjä (päätökset 2002/47/EY, EHTY, Euratom [2] ja 2004/563/EY, Euratom [3]).

---

[1] Arrangement entre le Gouvernement belge et le Parlement européen, le Conseil, la Commission, le Comité économique et social européen, le Comité des régions, la Banque européenne d'investissement en matière de sécurité, tehty 31.12.2004, Accord de sécurité signé entre la Commission et le Gouvernement luxembourgeois, tehty 20.1.2007, ja Accordo tra il Governo italiano e la Commissione europea dell'energia atomica (Euratom) per l'istituzione di un Centro comune di ricerche nucleari di competenza generale, tehty 22.7.1959.

[2] Komission päätös 2002/47/EY, EHTY, Euratom, tehty 23 päivänä tammikuuta 2002, työjärjestyksensä muuttamisesta (EYVL L 21, 24.1.2002, s. 23).

[3] Komission päätös 2004/563/EY, Euratom, tehty 7 päivänä heinäkuuta 2004, komission työjärjestyksen muuttamisesta (EUVL L 251, 27.7.2004, s. 9).

(8) Tämän päätöksen säännökset eivät rajoita seuraavien soveltamista:

a) asetus (Euratom) N:o 3 ([1]);

b) Euroopan parlamentin ja neuvoston asetus (EY) N:o 1049/2001 ([2]);

c) Euroopan parlamentin ja neuvoston asetus (EY) N:o 45/2001 ([3]);

d) neuvoston asetus (ETY, Euratom) N:o 354/83 ([4]),

ON HYVÄKSYNYT TÄMÄN PÄÄTÖKSEN:

1 LUKU

**PERUSPERIAATTEET JA VÄHIMMÄISVAATIMUKSET**

*1 artikla*

**Määritelmät**

Tässä päätöksessä tarkoitetaan

1) 'komission osastolla' mitä tahansa komission pääosastoa tai yksikköä taikka komission jäsenen kabinettia;

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

3) 'turvallisuusluokan poistamisella' minkä tahansa turvallisuusluokan poistamista;

4) 'syvyyssuuntaisella turvallisuudella' sellaisten erityyppisten turvatoimien soveltamista, joilla järjestetään monitasoinen puolustus;

5) 'asiakirjalla' mitä tahansa tallennettua tietoa sen fyysisestä muodosta tai ominaisuuksista riippumatta;

6) 'turvallisuusluokan alentamisella' salassapitotason alentamisesta johtuvaa turvallisuusluokan muuttamista;

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

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

9) 'soveltamissäännöillä' mitä tahansa komission päätöksen (EU, Euratom) 2015/443 ([5]) 5 luvun mukaisesti hyväksyttyjä sääntöjä tai turvallisuusohjeita;

10) 'materiaalilla' mitä tahansa viestintä, tiedonsiirtovälinettä, konetta tai laitetta, joka on valmistettu tai jota ollaan valmistamassa;

11) 'luovuttajalla' unionin toimielintä, elintä tai laitosta, jäsenvaltiota, kolmatta valtiota tai kansainvälistä järjestöä, jonka alaisuudessa turvallisuusluokiteltu tieto on tuotettu ja/tai tuotu unionin rakenteisiin;

12) 'tiloilla' mitä tahansa komission kiinteistöä tai siihen rinnastettavissa olevaa kiinteää omaisuutta;

---

([1]) Asetus (Euratom) N:o 3, annettu 31 päivänä heinäkuuta 1958, Euroopan ydinenergiayhteisön perustamissopimuksen 24 artiklan soveltamisesta (EYVL 17, 6.10.1958, s. 406/58).

([2]) Euroopan parlamentin ja neuvoston asetus (EY) N:o 1049/2001, annettu 30 päivänä toukokuuta 2001, Euroopan parlamentin, neuvoston ja komission asiakirjojen saamisesta yleisön tutustuttavaksi (EYVL L 145, 31.5.2001, s. 43).

([3]) Euroopan parlamentin ja neuvoston asetus (EY) N:o 45/2001, annettu 18 päivänä joulukuuta 2000, yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta (EYVL L 8, 12.1.2001, s. 1).

([4]) Neuvoston asetus (ETY, Euratom) N:o 354/83, annettu 1 päivänä helmikuuta 1983, Euroopan talousyhteisön ja Euroopan atomienergiayhteisön historiallisten arkistojen avaamisesta yleisölle (EYVL L 43, 15.2.1983, s. 1).

([5]) Komission päätös (EU, Euratom) 2015/443, annettu 13 päivänä maaliskuuta 2015, turvallisuudesta komissiossa (ks. tämän virallisen lehden sivu 41).

13) 'turvallisuusriskien hallintaprosessilla' sellaisten epävarmojen tapahtumien havaitsemis-, hallinta- ja minimointiprosessia, jotka saattavat vaikuttaa organisaation tai jonkin sen käyttämän järjestelmän turvallisuuteen. Se kattaa kaikki riskeihin liittyvät toiminnot, myös arvioinnin, käsittelyn, hyväksymisen ja viestinnän;

14) 'henkilöstösäännöillä' neuvoston asetuksessa (ETY, Euratom, EHTY) N:o 259/68 ([1]) säädettyjä Euroopan unionin virkamiehiin sovellettavia henkilöstösääntöjä ja unionin muuta henkilöstöä koskevia palvelussuhteen ehtoja;

15) 'uhalla' sellaisen ei-toivotun tapahtuman mahdollista aiheuttajaa, joka voi vahingoittaa organisaatiota tai jotakin sen käyttämää järjestelmää. Tällaiset uhat voivat olla tahattomia tai tahallisia (vihamielisiä), ja niille ovat ominaisia uhkaavat seikat sekä mahdolliset kohteet ja hyökkäysmenetelmät;

16) 'haavoittuvuudella' 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, fyysistä tai organisatorista taikka liittyä menettelyyn tai toimintaan.

*2 artikla*

**Kohde ja soveltamisala**

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

2. Tätä päätöstä sovelletaan kaikkiin komission osastoihin ja kaikissa komission tiloissa.

3. Tätä päätöstä sovelletaan komission jäseniin, henkilöstösääntöjen alaiseen komission henkilöstöön, komission kansallisiin asiantuntijoihin, palveluntarjoajiin ja niiden henkilöstöön, harjoittelijoihin sekä kaikkiin henkilöihin, joilla on pääsy komission rakennuksiin tai muuhun omaisuuteen taikka komission käsittelemiin tietoihin, sanotun kuitenkaan rajoittamatta tiettyjä henkilöstöryhmiä koskevia erityisohjeita.

4. Tämän päätöksen säännökset eivät rajoita päätösten 2002/47/EY, EHTY, Euratom ja 2004/563/EY, Euratom soveltamista.

*3 artikla*

**EU:n turvallisuusluokiteltujen tietojen määritelmä sekä turvallisuusluokat ja -merkinnät**

1. 'EU:n turvallisuusluokitelluilla tiedoilla' tarkoitetaan mitä tahansa tietoa tai materiaalia, jolle on määritelty EU:n turvallisuusluokka ja jonka luvaton ilmitulo saattaisi eriasteisesti vahingoittaa Euroopan unionin tai yhden tai useamman jäsenvaltion etuja.

2. EU:n turvallisuusluokitellut tiedot luokitellaan seuraavasti:

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

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

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

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

3. EU:n turvallisuusluokitellut tiedot on merkittävä 2 kohdan mukaisesti. Niissä voi olla myös muita kuin turvallisuusluokkaa koskevia merkintöjä, joista käy ilmi ala, johon tiedot liittyvät, tietojen luovuttaja ja luovutettavuus sekä jakelun tai käytön rajoitukset.

([1]) Neuvoston asetus (ETY, Euratom, EHTY) N:o 259/68, annettu 29 päivänä helmikuuta 1968, Euroopan yhteisöjen virkamiehiin sovellettavien henkilöstösääntöjen ja näiden yhteisöjen muuta henkilöstöä koskevien palvelussuhteen ehtojen vahvistamisesta ja komission virkamiehiin väliaikaisesti sovellettavista erityistoimenpiteistä (EYVL L 56, 4.3.1968, s. 1).

*4 artikla*

**Luokittelun hallinnointi**

1. Kukin komission jäsen tai osasto varmistaa, että sen tuottamat EU:n turvallisuusluokitellut tiedot on asianmukaisesti luokiteltu, että ne on selvästi merkitty EU:n turvallisuusluokitelluiksi tiedoiksi ja että niiden turvallisuusluokka säilytetään vain niin kauan kuin on tarpeen.

2. EU:n turvallisuusluokiteltujen tietojen turvallisuusluokkaa ei saa alentaa tai poistaa eikä niissä olevia 3 artiklan 2 kohdassa tarkoitettuja turvallisuusluokitusmerkintöjä saa muuttaa tai poistaa ilman niiden luovuttajan kirjallista ennakkosuostumusta, sanotun kuitenkaan rajoittamatta 26 artiklan soveltamista.

3. EU:n turvallisuusluokiteltujen tietojen käsittelyä koskevat soveltamissäännöt, mukaan lukien käytännön luokitteluopas, on tarvittaessa hyväksyttävä 60 artiklan mukaisesti.

*5 artikla*

**Turvallisuusluokiteltujen tietojen suojaaminen**

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

2. Minkä tahansa EU:n turvallisuusluokitellun tiedon haltija on 4 luvussa vahvistettujen sääntöjen mukaisesti vastuussa sen suojaamisesta tämän päätöksen ja sen soveltamissääntöjen mukaisesti.

3. Jäsenvaltioiden tuodessa komission rakenteisiin tai verkostoihin turvallisuusluokiteltuja tietoja, joissa on kansallinen turvallisuusluokitusmerkintä, komissio suojaa kyseiset tiedot vastaavantasoisiin EU:n turvallisuusluokiteltuihin tietoihin sovellettavia vaatimuksia noudattaen liitteeseen I sisältyvän turvallisuusluokkien vastaavuustaulukon mukaisesti.

4. EU:n turvallisuusluokiteltujen tietojen kooste voi edellyttää korkeampaan turvallisuusluokkaan sovellettavaa suojaa kuin koosteen yksittäisten osien suoja.

*6 artikla*

**Turvallisuusriskien hallinta**

1. Turvatoimet EU:n turvallisuusluokiteltujen tietojen suojaamiseksi koko niiden elinkaaren ajan on suhteutettava erityisesti tietojen tai materiaalin turvallisuusluokkaan, muotoon ja määrään, EU:n turvallisuusluokiteltujen tietojen säilytystilojen sijaintiin ja rakenteeseen sekä paikallisesti arvioituun vihamielisen ja/tai rikollisen toiminnan uhkaan, vakoilu, sabotaasi ja terrorismi mukaan lukien.

2. Varautumissuunnitelmissa on otettava huomioon tarve suojata EU:n turvallisuusluokitellut tiedot hätätilanteissa, jotta voidaan estää luvaton pääsy tietoihin, tietojen ilmitulo tai niiden eheyden tai käytettävyyden menetys.

3. Kaikkien yksiköiden on sisällytettävä toiminnan jatkuvuussuunnitelmiin ennalta ehkäiseviä ja korjaavia toimia, jotta voidaan minimoida merkittävien toimintahäiriöiden tai poikkeuksellisten tapahtumien vaikutus EU:n turvallisuusluokiteltujen tietojen käsittelyyn ja säilyttämiseen.

*7 artikla*

**Tämän päätöksen täytäntöönpano**

1. Tätä päätöstä täydentävät tai tukevat soveltamissäännöt hyväksytään tarvittaessa 60 artiklan mukaisesti.

2. Komission osastot toteuttavat kaikki niiden vastuulle kuuluvat tarvittavat toimenpiteet sen varmistamiseksi, että EU:n tai minkä tahansa turvallisuusluokiteltujen tietojen käsittelyssä tai säilytyksessä sovelletaan tätä päätöstä ja asiaankuuluvia soveltamissääntöjä.

3. Tämän päätöksen täytäntöönpanossa toteutettavien turvatoimenpiteiden on oltava päätöksen (EU, Euratom) 2015/443 3 artiklassa vahvistettujen, turvallisuutta komissiossa koskevien periaatteiden mukaisia.

4. Henkilöstöhallinnon ja turvallisuustoiminnan pääjohtaja perustaa johtamaansa pääosastoon komission turvallisuusviranomaisen. Komission turvallisuusviranomainen vastaa tässä päätöksessä ja sen soveltamissäännöissä sille osoitetuista tehtävistä.

5. Päätöksen (EU, Euratom) 2015/443 20 artiklassa tarkoitetulla paikallisella turvavastaavalla on kussakin komission osastossa kokonaisvastuu seuraavista tehtävistä, jotka se suorittaa tiiviissä yhteistyössä henkilöstöhallinnon ja turvallisuustoiminnan pääjohtajan kanssa EU:n turvallisuusluokiteltujen tietojen suojaamiseksi tämän päätöksen mukaisesti:

a) henkilöstöä koskevien turvallisuusselvityspyyntöjen hallinnointi;

b) osallistuminen turvallisuuskoulutusta ja -tietoisuutta käsitteleviin tiedotustilaisuuksiin;

c) osastossa toimivan rekisterin valvontavastaavan ohjaus;

d) tietoturvaloukkauksista ja EU:n turvallisuusluokiteltujen tietojen vaarantumisesta raportointi;

e) vara-avainten ja kunkin numeroyhdistelmän kirjallisen tositteen säilytys;

f) muut EU:n turvallisuusluokiteltujen tietojen suojaamiseen liittyvät tai soveltamissäännöissä määritellyt tehtävät.

*8 artikla*

**Tietoturvaloukkaukset ja EU:n turvallisuusluokiteltujen tietojen vaarantuminen**

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

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

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

4. Jos EU:n turvallisuusluokiteltujen tietojen tiedetään tai voidaan perustellusti olettaa vaarantuneen tai hävinneen, on tehtävä turvallisuustarkastus päätöksen (EU, Euratom) 2015/443 13 artiklan mukaisesti.

5. On toteutettava kaikki aiheelliset toimenpiteet

a) luovuttajalle ilmoittamiseksi;

b) sen varmistamiseksi, että tapausta tutkivat tosiasioiden selvittämiseksi sellaiset henkilöstön jäsenet, joita tietoturvaloukkaus ei koske välittömästi;

c) unionin tai jäsenvaltioiden eduille mahdollisesti aiheutuneen vahingon arvioimiseksi;

d) sellaisten toimien toteuttamiseksi, joilla estetään tapahtuneen toistuminen; ja

e) toteutetuista toimista asiaankuuluville viranomaisille ilmoittamiseksi.

6. Henkilölle, joka on vastuussa tässä päätöksessä vahvistettujen turvallisuussääntöjen rikkomisesta, voidaan määrätä henkilöstösääntöjen mukainen kurinpitoseuraamus. Henkilölle, joka on aiheuttanut EU:n turvallisuusluokiteltujen tietojen vaarantumisen tai häviämisen, on määrättävä kurinpidollisia ja/tai oikeudellisia seuraamuksia asiassa sovellettavien lakien, sääntöjen ja määräysten mukaisesti.

2 LUKU

**HENKILÖSTÖTURVALLISUUS**

*9 artikla*

**Määritelmät**

Tässä luvussa tarkoitetaan

1) ’valtuutuksella EU:n turvallisuusluokiteltuihin tietoihin pääsyä varten’ päätöstä, jonka komission turvallisuusviranomainen tekee jäsenvaltion toimivaltaisen viranomaisen antaman vakuutuksen perusteella ja jonka mukaan komission virkamiehelle, muuhun henkilöstöön kuuluvalle tai kansalliselle asiantuntijalle voidaan myöntää pääsy EU:n turvallisuusluokiteltuihin tietoihin tiettyyn turvallisuusluokkaan (CONFIDENTIEL UE/EU CONFIDENTIAL tai sitä korkeampi) ja tiettyyn päivämäärään asti edellyttäen, että henkilön tiedonsaantitarve on todennettu ja että hänelle on tiedotettu asianmukaisesti hänelle kuuluvasta vastuusta. Henkilön katsotaan tämän jälkeen olevan ”turvallisuusvaltuutettu”;

2) ’henkilöturvallisuusvaltuutuksella’ toimia sen varmistamiseksi, että pääsy EU:n turvallisuusluokiteltuihin tietoihin myönnetään ainoastaan henkilölle,

   a) jolla on tiedonsaantitarve,

   b) jolle on tarvittaessa myönnetty asianmukaisen tason turvallisuusvaltuutus ja

   c) jolle on tiedotettu hänelle kuuluvasta vastuusta;

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

4) ’henkilöturvallisuusselvitykseen perustuvalla todistuksella’ toimivaltaisen viranomaisen antamaa todistusta, jonka mukaan henkilöllä on voimassa oleva turvallisuusselvitys tai komission turvallisuusviranomaisen myöntämä turvallisuusvaltuutus ja josta käy ilmi turvallisuusluokka, johon kuuluviin EU:n turvallisuusluokiteltuihin tietoihin henkilölle voidaan myöntää pääsy (CONFIDENTIEL UE/EU CONFIDENTIAL tai sitä korkeampi), asianomaisen turvallisuusselvityksen tai -valtuutuksen voimassaoloaika ja todistuksen voimassaolon päättymispäivä;

5) ’turvallisuustutkinnalla’ tutkintamenettelyjä, jotka jäsenvaltion toimivaltainen viranomainen suorittaa kansallisten lakien ja asetusten mukaisesti varmistaakseen, että tiedossa ei ole mitään sellaista kielteistä seikkaa, joka estäisi turvallisuusselvityksen myöntämisen henkilölle tiettyyn turvallisuusluokkaan (CONFIDENTIEL UE/EU CONFIDENTIAL tai sitä korkeampi) asti.

*10 artikla*

**Perusperiaatteet**

1. Henkilölle voidaan myöntää pääsy EU:n turvallisuusluokiteltuihin tietoihin vasta sen jälkeen, kun

(1) hänen tiedonsaantitarpeensa on todennettu;

(2) hänelle on selvitetty EU:n turvallisuusluokiteltujen tietojen suojaamista koskevat turvallisuussäännöt sekä asiaankuuluvat turvallisuusvaatimukset ja -ohjeet ja hän on vahvistanut tällaisten tietojen suojaamista koskevan vastuunsa;

(3) hänelle on myönnetty turvallisuusvaltuutus tai hänellä on tehtäviensä vuoksi muu kansallisten lakien ja asetusten mukainen valtuutus CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeamman tason tietoihin pääsyä varten.

2. Kaikilla henkilöillä, joiden tehtävät saattavat edellyttää pääsyä CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeamman tason EU:n turvallisuusluokiteltuihin tietoihin, on oltava asianmukainen turvallisuusvaltuutus ennen kuin heillä voidaan myöntää pääsy kyseisiin tietoihin. Asianomaiselta on saatava kirjallinen suostumus henkilöturvallisuusselvityksen tekemiseen. Ilman suostumusta henkilöä ei voida nimittää toimeen tai tehtävään, joka edellyttää pääsyä CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeammalle tasolle luokiteltuihin tietoihin.

3. Henkilöturvallisuusselvityksen tarkoituksena on selvittää, voidaanko henkilölle myöntää pääsy EU:n turvallisuusluokiteltuihin tietoihin hänen lojaaliutensa, rehellisyytensä ja luotettavuutensa huomioon ottaen.

4. Henkilön lojaalius, rehellisyys ja luotettavuus määritetään turvallisuusselvityksen tekemistä ja pääsyn myöntämistä CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeammalle tasolle luokiteltuihin tietoihin niin, että jäsenvaltion toimivaltaiset viranomaiset suorittavat kansallisten lakien ja asetusten mukaisen turvallisuustutkinnan.

5. Komission turvallisuusviranomainen on yksin vastuussa yhteydenpidosta kansallisiin turvallisuusviranomaisiin tai muihin toimivaltaisiin viranomaisiin kaikissa turvallisuusselvitykseen liittyvissä asioissa. Kaikki yhteydenpito komission yksiköiden ja niiden henkilöstön sekä kansallisten turvallisuusviranomaisten ja muiden toimivaltaisten viranomaisten välillä tapahtuu komission turvallisuusviranomaisen kautta.

*11 artikla*

**Turvallisuusvaltuutusmenettely**

1. Komission sisällä kunkin pääjohtajan tai yksikönpäällikön on nimettävä osastossaan toimet, joiden haltijoilla on tehtäviensä hoitamiseksi oltava pääsy CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeammalle tasolle luokiteltuihin tietoihin ja joilla on siksi oltava turvallisuusvaltuutus.

2. Heti kun on tiedossa, että henkilö aiotaan nimittää tehtävään, joka edellyttää pääsyä CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeammalle tasolle luokiteltuihin tietoihin, komission asianomaisen osaston paikallinen turvavastaava ilmoittaa asiasta komission turvallisuusviranomaiselle, joka toimittaa kyseiselle henkilölle sen jäsenvaltion kansallisen turvallisuusviranomaisen turvallisuusselvityslomakkeen, jonka kansalainen kyseinen EU:n toimielinten henkilöstön jäseneksi nimitetty henkilö on. Asianomaiselta henkilöltä on saatava kirjallinen suostumus turvallisuusselvityksen tekemiseen, ja hänen on palautettava täytetty lomake mahdollisimman pian komission turvallisuusviranomaiselle.

3. Komission turvallisuusviranomainen toimittaa täytetyn turvallisuusselvityslomakkeen sen jäsenvaltion kansalliselle turvallisuusviranomaiselle, jonka kansalainen kyseinen EU:n toimielinten henkilöstön jäseneksi nimitetty henkilö on, ja pyytää sitä tekemään turvallisuustutkinnan sillä EU:n turvallisuusluokiteltujen tietojen tasolla, johon henkilöllä on oltava pääsy.

4. Jos komission turvallisuusviranomaisen tietoon tulee turvallisuustutkinnan kannalta merkityksellisiä tietoja henkilöstä, joka on hakenut turvallisuusselvitystä, komission turvallisuusviranomainen ilmoittaa siitä toimivaltaiselle kansalliselle turvallisuusviranomaiselle asiaankuuluvien sääntöjen ja määräysten mukaisesti.

5. Turvallisuustutkinnan valmistuttua ja mahdollisimman pian sen jälkeen, kun kansallinen turvallisuusviranomainen on ilmoittanut sille kokonaisarvionsa turvallisuustutkinnan tuloksista, komission turvallisuusviranomainen

a) voi myöntää asianomaiselle henkilölle valtuutuksen EU:n turvallisuusluokiteltuihin tietoihin pääsyä varten tiettyyn tasoon ja tiettyyn turvallisuusviranomaisen määrittämään päivämäärään asti mutta enintään viideksi vuodeksi, jos turvallisuustutkinnan johdosta annetaan vakuutus, jonka mukaan ei ole tiedossa mitään sellaista kielteistä seikkaa, joka kyseenalaistaisi henkilön lojaaliuden, rehellisyyden ja luotettavuuden;

b) siinä tapauksessa, että turvallisuustutkinnan johdosta ei anneta tällaista vakuutusta, ilmoittaa siitä asiaankuuluvien sääntöjen ja määräysten mukaisesti asianomaiselle henkilölle, joka voi pyytää, että komission turvallisuusviranomainen kuulee häntä; komission turvallisuusviranomainen voi puolestaan pyytää toimivaltaiselta kansalliselta turvallisuusviranomaiselta lisäselvityksiä, joita se voi antaa kansallisten lakien ja asetusten mukaisesti. Jos turvallisuustutkinnan tulos vahvistetaan, valtuutusta EU:n turvallisuusluokiteltuihin tietoihin pääsyä varten ei myönnetä.

6. Turvallisuustutkintaan ja sen tuloksiin sovelletaan kyseisessä jäsenvaltiossa voimassa olevia asiaa koskevia lakeja ja asetuksia, myös muutoksenhakukeinojen osalta. Komission turvallisuusviranomaisen päätöksiin voi hakea muutosta henkilöstösääntöjen mukaisesti.

7. Komissio hyväksyy muiden unionin toimielinten, elinten tai laitosten antaman valtuutuksen EU:n turvallisuusluokiteltuihin tietoihin pääsyä varten edellyttäen, että valtuutus on voimassa. Valtuutus kattaa kaikki asianomaisen henkilön komissiossa suorittamat tehtävät. Unionin toimielin, elin tai laitos, jossa henkilö ottaa työn vastaan, ilmoittaa asianomaiselle kansalliselle turvallisuusviranomaiselle henkilön työnantajan vaihtumisesta.

8. Jos henkilön palvelusaika ei ala 12 kuukauden kuluessa siitä, kun turvallisuustutkinnan tulokset on ilmoitettu komission turvallisuusviranomaiselle, tai jos henkilön palveluksessaolo keskeytyy 12 kuukaudeksi eikä hän sinä aikana ole komission eikä minkään muun unionin toimielimen, elimen tai laitoksen taikka jäsenvaltion kansallisen hallinnon palveluksessa, komission turvallisuusviranomainen pyytää kansalliselta turvallisuusviranomaiselta vahvistuksen sille, että turvallisuusselvitys on edelleen voimassa ja asianmukainen.

9. Jos komission turvallisuusviranomaisen tietoon tulee seikkoja, joiden perusteella voimassa olevan turvallisuusvaltuutuksen haltija muodostaa turvallisuusriskin, turvallisuusviranomainen ilmoittaa asiasta toimivaltaiselle kansalliselle turvallisuusviranomaiselle asiaankuuluvien sääntöjen ja määräysten mukaisesti.

10. Jos kansallinen turvallisuusviranomainen ilmoittaa komission turvallisuusviranomaiselle EU:n turvallisuusluokiteltuihin tietoihin pääsyä varten myönnetyn ja voimassa olevan valtuutuksen haltijaa koskevan, 5 kohdan a alakohdan mukaisesti annetun vakuutuksen perumisesta, komission turvallisuusviranomainen voi pyytää selvennystä, jonka kansallinen turvallisuusviranomainen voi antaa kansallisten lakien ja asetusten mukaisesti. Jos kansallinen turvallisuusviranomainen vahvistaa kielteisen seikan, turvallisuusvaltuutus on peruttava ja asianomaiselta henkilöltä evättävä pääsy EU:n turvallisuusluokiteltuihin tietoihin ja tehtäviin, joissa niihin on mahdollista päästä tai joissa hän voisi vaarantaa turvallisuuden.

11. Päätös perua tai keskeyttää tämän päätöksen soveltamisalaan kuuluvalle henkilölle myönnetty valtuutus päästä EU:n turvallisuusluokiteltuihin tietoihin ja tarvittaessa päätöksen perusteet on ilmoitettava asianomaiselle, joka voi pyytää tulla komission turvallisuusviranomaisen kuulemaksi. Kansallisen turvallisuusviranomaisen toimittamiin tietoihin sovelletaan kyseisessä jäsenvaltiossa voimassa olevia asiaa koskevia lakeja ja asetuksia. Komission turvallisuusviranomaisen tässä yhteydessä tekemiin päätöksiin voi hakea muutosta henkilöstösääntöjen mukaisesti.

12. Komission osastot varmistavat, että niiden sellaisissa tehtävissä työskentelevät kansalliset asiantuntijat, joissa edellytetään turvallisuusvaltuutusta EU:n turvallisuusluokiteltuihin tietoihin pääsyä varten, esittävät komission turvallisuusviranomaiselle ennen tehtäviensä aloittamista voimassa olevan henkilöturvallisuusselvityksen tai siihen perustuvan todistuksen kansallisten lakien ja asetusten mukaisesti; selvityksen tai todistuksen perusteella komission turvallisuusviranomainen myöntää enintään tehtävän keston ajaksi valtuutuksen päästä EU:n turvallisuusluokiteltuihin tietoihin sellaiseen tasoon asti, joka vastaa kansallisessa turvallisuusselvityksessä mainittua tasoa.

Tehtäviensä vuoksi asianmukaisesti valtuutettujen henkilöiden pääsy EU:n turvallisuusluokiteltuihin tietoihin

13. Komission jäsenille, joilla on tehtäviensä vuoksi perussopimukseen perustuva pääsy EU:n turvallisuusluokiteltuihin tietoihin, on tiedotettava heille kuuluvasta vastuusta kyseisten tietojen suojaamisessa.

Turvallisuusselvitys- ja valtuutusrekisterit

14. Komission turvallisuusviranomainen pitää tämän päätöksen mukaisesti rekisteriä turvallisuusselvityksistä ja EU:n turvallisuusluokiteltuihin tietoihin pääsyä koskevista valtuutuksista. Vähimmäisvaatimuksena rekisteriin on merkittävä korkein taso, johon kuuluviin EU:n turvallisuusluokiteltuihin tietoihin henkilölle voidaan myöntää pääsy, turvallisuusselvityksen myöntämispäivä ja sen voimassaoloaika.

15. Komission turvallisuusviranomainen voi antaa henkilöturvallisuusselvitykseen perustuvan todistuksen, josta käy ilmi taso, johon kuuluviin EU:n turvallisuusluokiteltuihin tietoihin asianomaiselle henkilölle voidaan myöntää pääsy (CONFIDENTIEL UE/EU CONFIDENTIAL tai sitä korkeampi), EU:n turvallisuusluokiteltuihin tietoihin pääsyä koskevan valtuutuksen voimassaoloaika ja itse todistuksen voimassaolon päättymispäivä.

Turvallisuusvaltuutuksen uusiminen

16. Sen jälkeen, kun turvallisuusvaltuutus on ensimmäisen kerran myönnetty, ja edellyttäen, että henkilö on ollut keskeytyksettä Euroopan komission tai muun unionin toimielimen, elimen tai laitoksen palveluksessa ja hänellä on jatkuva tarve päästä EU:n turvallisuusluokiteltuihin tietoihin, turvallisuusvaltuutusta tarkastellaan uudelleen pääsääntöisesti aina viiden vuoden kuluttua edellisen turvallisuustutkinnan, johon myönnetty valtuutus perustuu, tulosten ilmoituspäivästä.

17. Komission turvallisuusviranomainen voi jatkaa voimassa olevan turvallisuusvaltuutuksen voimassaoloa enintään 12 kuukaudella, jos kansallinen turvallisuusviranomainen tai muu toimivaltainen viranomainen ei ole ilmoittanut mitään kielteisiä seikkoja kahden kuukauden kuluessa uusintapyynnön ja siihen liittyvän turvallisuusselvityslomakkeen lähetyspäivästä. Jos kyseisen 12 kuukauden jakson päätyttyä kansallinen turvallisuusviranomainen tai muu toimivaltainen viranomainen ei ole toimittanut komission turvallisuusviranomaiselle lausuntoa, asianomainen henkilö siirretään tehtäviin, joissa ei vaadita turvallisuusvaltuutusta.

*12 artikla*

**Turvallisuusvaltuutuksia koskevat tiedotustilaisuudet**

1. Osallistuttuaan komission turvallisuusviranomaisen turvallisuusvaltuutuksista järjestämään tiedotustilaisuuteen kaikkien valtuutuksen saaneiden on annettava kirjallinen vakuutus siitä, että he ovat ymmärtäneet EU:n turvallisuusluokiteltujen tietojen suojaamista koskevat velvollisuutensa ja tietojen vaarantumisen seuraukset. Komission turvallisuusviranomainen tallentaa nämä kirjalliset vakuutukset.

2. Kaikille henkilöille, joilla on valtuutus päästä EU:n turvallisuusluokiteltuihin tietoihin tai joiden edellytetään käsittelevän niitä, on aluksi selvitettävä turvallisuusuhat, joista on tiedotettava säännöllisin väliajoin, ja heidän on ilmoitettava välittömästi komission turvallisuusviranomaiselle sellaisesta yhteydenotosta tai toiminnasta, jota hän pitää epäilyttävänä tai epätavanomaisena.

3. Kaikille henkilöille, jotka siirtyvät pois tehtävistä, jotka edellyttävät pääsyä EU:n turvallisuusluokiteltuihin tietoihin, on selvitettävä heidän velvollisuutensa EU:n turvallisuusluokiteltujen tietojen jatkuvan suojaamisen osalta, ja heidän on tarvittaessa annettava siitä kirjallinen vakuutus.

*13 artikla*

**Tilapäiset turvallisuusvaltuutukset**

1. Poikkeuksellisissa olosuhteissa komission turvallisuusviranomainen voi sen jäsenvaltion kansallista turvallisuusviranomaista kuultuaan, jonka kansalainen asianomainen henkilö on, ja kielteisten seikkojen olemassaoloa koskevien alustavien tarkastusten tuloksista riippuen myöntää henkilölle tiettyä tehtävää varten tilapäisen valtuutuksen EU:n turvallisuusluokiteltuihin tietoihin pääsyä varten, jos se on yksikön edun mukaista asianmukaisesti perusteltuna ja jos täysimittainen turvallisuustutkinta on kesken, sanotun kuitenkaan rajoittamatta turvallisuusselvityksen uusimista koskevien säännösten soveltamista. Tilapäinen valtuutus EU:n turvallisuusluokiteltuihin tietoihin pääsyä varten on voimassa korkeintaan kuuden kuukauden mittaisen ajanjakson ajan, eikä se oikeuta pääsemään TRES SECRET UE/EU TOP SECRET -turvallisuusluokan tietoihin.

2. Kaikkien henkilöiden, joille on myönnetty tilapäinen valtuutus, on sen jälkeen, kun heille on tiedotettu asiasta 12 artiklan 1 kohdan mukaisesti, vakuutettava kirjallisesti ymmärtäneensä velvollisuutensa EU:n turvallisuusluokiteltujen tietojen suojaamisessa sekä tietojen vaarantumisen seuraukset. Komission turvallisuusviranomainen tallentaa nämä kirjalliset vakuutukset.

*14 artikla*

**Osallistuminen komission järjestämiin luottamuksellisiin kokouksiin**

1. Sellaisten kokousten järjestämisestä vastaavat komission osastot, joissa keskustellaan CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeampaan turvallisuusluokkaan kuuluvista tiedoista, ilmoittavat paikallisen turvavastaavansa tai kokouksen järjestäjän välityksellä komission turvallisuusviranomaiselle hyvissä ajoin tällaisen kokouksen päivämäärän, kellonajan, paikan ja osallistujat.

2. Komission järjestämiin kokouksiin, joissa keskustellaan CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeampaan turvallisuusluokkaan kuuluvista tiedoista, voivat osallistua ainoastaan henkilöt, joiden turvallisuusselvitys tai -valtuutus on vahvistettu, sanotun kuitenkaan rajoittamatta 11 artiklan 13 kohdan soveltamista. Tällaisiin luottamuksellisiin kokouksiin eivät voi osallistua henkilöt, joista komission turvallisuusviranomainen ei ole nähnyt henkilöturvallisuusselvitykseen perustuvaa todistusta tai muuta todistetta turvallisuusselvityksestä, eivätkä komission edustajat, joilla ei ole turvallisuusvaltuutusta.

3. Ennen luottamuksellisen kokouksen järjestämistä vastuullinen järjestäjä tai kokouksen järjestävän komission osaston paikallinen turvavastaava pyytää ulkopuolisia osallistujia toimittamaan komission turvallisuusviranomaiselle henkilöturvallisuusselvitykseen perustuvan todistuksen tai muun todisteen turvallisuusselvityksestä. Komission turvallisuusviranomainen ilmoittaa paikalliselle turvavastaavalle tai kokouksen järjestäjälle saatuaan henkilöturvallisuusselvitykseen perustuvan todistuksen tai muun todisteen henkilöturvallisuusselvityksestä. Tarvittaessa voidaan käyttää nimiluetteloa, johon sisältyy asianmukaisen todiste turvallisuusselvityksestä.

4. Jos toimivaltaiset viranomaiset ilmoittavat komission turvallisuusviranomaiselle, että henkilöturvallisuusselvitys on peruttu henkilöltä, jonka tehtävät edellyttävät osallistumista komission järjestämiin kokouksiin, komission turvallisuusviranomainen ilmoittaa asiasta kokouksen järjestämisestä vastaavan komission osaston paikalliselle turvavastaavalle.

*15 artikla*

**Mahdollinen pääsy EU:n turvallisuusluokiteltuihin tietoihin**

Kuriireilla, vartijoilla ja saattajilla on oltava asiaankuuluvan tason turvallisuusvaltuutus tai heidän on oltava muulla tavoin asianmukaisesti tutkittuja kansallisten lakien ja asetusten mukaisesti, heille on selvitettävä EU:n turvallisuusluokiteltujen tietojen suojaamista koskevat menettelyt ja heille on annettava ohjeet tällaisten heille uskottujen tietojen suojaamiseen liittyvistä tehtävistään.

3 LUKU

**TURVALLISUUSLUOKITELTUJEN TIETOJEN SUOJAAMISEEN TÄHTÄÄVÄ FYYSINEN TURVALLISUUS**

*16 artikla*

**Perusperiaatteet**

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

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

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

b) mahdollistamalla henkilöstön jaottelu EU:n turvallisuusluokiteltuihin tietoihin pääsyä varten heidän tiedonsaantitarpeensa ja tarvittaessa heidän turvallisuusvaltuutustensa perusteella;

c) ehkäisemällä, estämällä ja havaitsemalla luvattomat toimet; ja

d) estämällä salaa tai väkisin tapahtuva tunkeutuminen tai viivyttämällä sitä.

3. Fyysiset turvatoimet on toteutettava kaikissa tiloissa, rakennuksissa, toimistoissa, huoneissa ja muissa paikoissa, joissa EU:n turvallisuusluokiteltuja tietoja käsitellään tai säilytetään, mukaan lukien alueet, joissa 5 luvussa tarkoitetut viestintä- ja tietojärjestelmät sijaitsevat.

4. Alueet, joilla säilytetään CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeamman tason EU:n turvallisuusluokiteltuja tietoja, on tämän luvun mukaisesti määriteltävä turva-alueiksi, ja komission turvallisuusjärjestelyjen hyväksyntäviranomaisen on hyväksyttävä ne.

5. CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeamman tason EU:n turvallisuusluokiteltujen tietojen suojaamiseen saa käyttää vain komission turvallisuusviranomaisen hyväksymiä välineitä ja laitteita.

*17 artikla*

**Fyysiset turvallisuusvaatimukset ja turvatoimet**

1. Fyysiset turvatoimet valitaan komission turvallisuusviranomaisen tekemän uhka-arvion perusteella ja tarvittaessa yhteistyössä muiden komission osastojen, muiden unionin toimielinten, elinten tai virastojen ja/tai jäsenvaltioiden toimivaltaisten viranomaisten kanssa. Komissio soveltaa riskinhallintaprosessia EU:n turvallisuusluokiteltujen tietojen suojaamiseen tiloissaan sen varmistamiseksi, 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 yhdistäminen voi edellyttää tiukempien suojatoimien toteuttamista;

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

d) niiden tiedustelupalvelujen muodostama arvioitu uhka, joiden toiminta kohdistuu unioniin, sen toimielimiin, elimiin ja laitoksiin tai jäsenvaltioihin, sekä sabotaasin, terrorismin taikka kumouksellisen tai muun rikollisen toiminnan uhka.

2. Komission turvallisuusviranomainen tekee päätöksen toteutettavien fyysisten turvatoimien asianmukaisesta yhdistelmästä syvyyssuuntaisen turvallisuuden käsitettä soveltaen. Tätä varten komission turvallisuusviranomainen laatii vähimmäisvaatimukset, normit ja kriteerit, jotka esitetään soveltamissäännöissä.

3. Komission turvallisuusviranomaisella on valtuudet tehdä sisään- ja ulostulotarkastuksia, millä estetään materiaalin luvaton tuonti tai EU:n turvallisuusluokiteltujen tietojen luvaton vienti tiloista tai rakennuksista.

4. Jos EU:n turvallisuusluokiteltuihin tietoihin kohdistuu salakatselun riski, vahingossa tapahtuva salakatselu mukaan lukien, asianomaiset komission osastot toteuttavat komission turvallisuusviranomaisen määrittelemät aiheelliset toimenpiteet tällaisen riskin torjumiseksi.

5. Uusien toimitilojen osalta fyysiset turvallisuusvaatimukset ja niiden toiminnalliset eritelmät on määriteltävä yhteisymmärryksessä komission turvallisuusviranomaisen kanssa osana toimitilojen suunnittelua. Olemassa olevien toimitilojen osalta fyysisiä turvallisuusvaatimuksia sovelletaan soveltamissäännöissä esitettyjen vähimmäisvaatimusten, normien ja kriteerien mukaisesti.

*18 artikla*

**EU:n turvallisuusluokiteltujen tietojen fyysiseen suojeluun tarkoitetut välineet**

1. EU:n turvallisuusluokiteltujen tietojen fyysiseksi suojaamiseksi on perustettava kahdentyyppisiä fyysisesti suojattuja alueita:

a) hallinnollisia alueita; ja

b) turva-alueita (mukaan lukien teknisesti suojatut turva-alueet).

2. Komission turvallisuusjärjestelyjen hyväksyntäviranomainen vahvistaa, että alue täyttää hallinnolliseksi alueeksi, turva-alueeksi tai teknisesti suojatuksi turva-alueeksi nimeämistä koskevat vaatimukset.

3. Hallinnollisiin alueisiin sovelletaan seuraavaa:

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

b) vain komission turvallisuusviranomaisen tai muun toimivaltaisen viranomaisen asianmukaisesti valtuuttamilla henkilöillä on pääsy alueelle ilman saattajaa; ja

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

4. Turva-alueisiin sovelletaan seuraavaa:

a) alueella on oltava selvästi määritellyt, näkyvät ja suojatut rajat, joilla sisään- ja ulostuloa valvotaan kulkuluvin tai henkilöiden tunnistusjärjestelmällä;

b) pääsy alueelle ilman saattajaa myönnetään vain henkilöille, jotka ovat turvallisuusselvitettyjä ja joilla on erityinen valtuutus tulla alueelle tiedonsaantitarpeensa perusteella;

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

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

a) alueella tavallisesti säilytettävien tietojen korkein turvallisuusluokka on ilmoitettava selvästi;

b) kaikilla vierailijoilla on oltava erityinen valtuutus tulla alueelle, heillä on oltava aina saattaja ja heidän on oltava asianmukaisesti turvallisuusselvitettyjä, paitsi jos on toteutettu toimenpiteitä sen varmistamiseksi, ettei EU:n turvallisuusluokiteltuihin tietoihin ole mahdollista päästä.

6. 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 hallinnoitava 20 artiklan mukaisesti;

b) alueille tulevia henkilöitä ja materiaalia on valvottava;

c) komission turvallisuusviranomainen tarkastaa alueet fyysisesti ja/tai teknisesti säännöllisin väliajoin. Tällaiset tarkastukset on suoritettava myös luvattoman sisäänpääsyn tapauksessa tai sitä epäiltäessä; ja

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

7. Sen estämättä, mitä 6 kohdan d alakohdassa säädetään, komission turvallisuusviranomainen tarkastaa tapauksissa, joissa EU:n turvallisuusluokiteltuihin tietoihin kohdistuva uhka arvioidaan suureksi, kaikki viestintä-, sähkö- ja elektroniset laitteet ennen kuin niitä käytetään alueilla, joilla järjestetään SECRET UE/EU SECRET- tai sitä korkeamman turvallisuusluokan tietoihin liittyviä kokouksia tai tehdään niihin liittyvää työtä, ja varmistaa näin, ettei kyseisillä laitteilla voi tahattomasti tai laittomasti välittää ymmärrettävässä muodossa olevia tietoja turva-alueen rajojen ulkopuolelle.

8. Turva-alueet, joilla ei ole päivystävää henkilöstöä vuorokauden ympäri, on tarvittaessa tarkastettava normaalin työajan päätteeksi ja satunnaisin väliajoin sen ulkopuolella, paitsi jos alueelle on asennettu tunkeutumisenhavaitsemisjärjestelmä.

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

10. Komission asianomaisen osaston paikallinen turvavastaava laatii kullekin vastuullaan olevalle turva-alueelle turvallisuusmenettelyt, joissa määrätään tämän päätöksen ja sen soveltamissääntöjen mukaisesti seuraavista:

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

b) toteutettavat valvonta- ja suojatoimet;

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

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

e) muut asiaankuuluvat toimet ja menettelyt.

11. Turva-alueille on rakennettava kassaholveja. Komission turvallisuusviranomainen hyväksyy seinät, lattiat, katot, ikkunat ja lukittavat ovet, joiden on tarjottava sama turvallisuustaso kuin samalle tasolle luokiteltujen EU:n turvallisuusluokiteltujen tietojen säilyttämiseen hyväksytyt turvakaapit.

*19 artikla*

**EU:n turvallisuusluokiteltujen tietojen käsittelyssä ja säilyttämisessä noudatettavat fyysiset suojatoimet**

1. Tasolle RESTREINT UE/EU RESTRICTED luokiteltuja EU:n turvallisuusluokiteltuja tietoja saa 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 haltija kuljettaa EU:n turvallisuusluokiteltuja tietoja 31 artiklan mukaisesti ja on sitoutunut noudattamaan soveltamissäännöissä esitettyjä korvaavia toimia sen varmistamiseksi, että pääsy EU:n turvaluokiteltuihin tietoihin on suojattu sivullisilta.

2. Tasolle RESTREINT UE/EU RESTRICTED kuuluvat EU:n turvallisuusluokitellut tiedot on säilytettävä soveltuvissa lukituissa toimistokalusteissa hallinnollisella alueella tai turva-alueella. Niitä voidaan tilapäisesti säilyttää hallinnollisen alueen tai turva-alueen ulkopuolella, jos haltija on sitoutunut noudattamaan soveltamissäännöissä esitettyjä korvaavia toimenpiteitä.

3. Tasolle CONFIDENTIEL UE/EU CONFIDENTIAL tai SECRET UE/EU SECRET kuuluvia EU:n turvallisuusluokiteltuja tietoja saa 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 haltija

i) on sitoutunut noudattamaan soveltamissäännöissä esitettyjä korvaavia toimenpiteitä sen varmistamiseksi, että pääsy EU:n turvallisuusluokiteltuihin tietoihin on suojattu sivullisilta;

ii) pitää EU:n turvallisuusluokitellut tiedot kaikkina aikoina henkilökohtaisessa valvonnassaan; ja

iii) on ilmoittanut asiaankuuluvalle rekisterille, jos asiakirjat ovat paperimuodossa.

4. Tasolle CONFIDENTIEL UE/EU CONFIDENTIAL ja SECRET UE/EU SECRET luokitellut EU:n turvallisuusluokitellut tiedot on säilytettävä turva-alueella turvakaapissa tai kassaholvissa.

5. Tasolle TRES SECRET UE/EU TOP SECRET luokiteltuja EU:n turvallisuusluokiteltuja tietoja on käsiteltävä turva-alueella, jonka komission turvallisuusviranomainen on perustanut ja jota se ylläpitää, ja jolle komission turvallisuusjärjestelyjen hyväksyntäviranomainen on antanut kyseisen tason hyväksynnän.

6. Tasolle TRES SECRET UE/EU TOP SECRET luokiteltuja EU:n turvallisuusluokiteltuja tietoja on säilytettävä turva-alueella, jolle komission turvallisuusjärjestelyjen hyväksyntäviranomainen on antanut kyseisen tason hyväksynnän, joko

a) turvakaapissa 18 artiklan mukaisesti soveltaen yhtä tai useampaa seuraavista lisävalvontatoimista:

(1) jatkuva suojaus tai varmennus turvallisuusselvitetyn turvahenkilöstön tai päivystävän henkilöstön toimesta;

(2) hyväksytty tunkeutumisenhavaitsemisjärjestelmä ja hälytyksiin vastaava turvallisuushenkilöstö;

tai

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

*20 artikla*

**EU:n turvallisuusluokiteltujen tietojen suojaamisessa käytettävien avainten ja numeroyhdistelmien hallinnointi**

1. Toimistojen, huoneiden, kassaholvien ja turvakaappien avainten ja numeroyhdistelmien hallinnointimenettelyt esitetään soveltamissäännöissä 60 artiklan mukaisesti. Menettelyjen tarkoituksena on estää luvaton pääsy.

2. Numeroyhdistelmät on opeteltava ulkoa, ja ne annetaan mahdollisimman pienelle joukolle ihmisiä, joiden on tarpeen tietää ne. EU:n turvallisuusluokiteltuja tietoja sisältävien turvakaappien ja kassaholvien numeroyhdistelmät on vaihdettava

a) uuden turvallisuuskaapin vastaanoton yhteydessä;

b) aina kun numeroyhdistelmän tuntevassa henkilöstössä tapahtuu muutos;

c) aina kun tiedot ovat vaarantuneet tai niiden epäillään vaarantuneen;

d) kun jokin lukoista on huollettu tai korjattu; ja

e) vähintään 12 kuukauden välein.

4 LUKU

**EU:N TURVALLISUUSLUOKITELTUJEN TIETOJEN HALLINNOINTI**

*21 artikla*

**Perusperiaatteet**

1. Kaikkia EU:n turvallisuusluokiteltuja tietoja sisältäviä asiakirjoja on hallinnoitava asiakirjahallintoa koskevaa komission politiikkaa noudattaen, ja ne olisi tästä syystä rekisteröitävä, arkistoitava, tallennettava ja lopulta joko hävitettävä taikka siirrettävä historiallisiin arkistoihin joko sellaisenaan tai osana otantaa Euroopan komission tiedostoja koskevan yhteisen säilytysluettelon mukaisesti.

2. CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeamman tason turvallisuusluokitellut tiedot on turvallisuussyistä rekisteröitävä ennen niiden jakelua ja niitä vastaanotettaessa. Tasolle TRÈS SECRET UE/EU TOP SECRET luokitellut tiedot on rekisteröitävä niille tarkoitetuissa rekistereissä.

3. Komissioon perustetaan EU:n turvallisuusluokiteltujen tietojen rekisteröintijärjestelmä 27 artiklan mukaisesti.

4. Komission turvallisuusviranomainen tarkastaa säännöllisesti komission osastot ja tilat, joissa käsitellään tai säilytetään EU:n turvallisuusluokiteltuja tietoja.

5. EU:n turvallisuusluokiteltujen tietojen siirtämisessä yksiköiden ja tilojen välillä fyysisesti suojattujen alueiden ulkopuolella noudatetaan seuraavaa:

a) EU:n turvallisuusluokitellut tiedot siirretään pääsääntöisesti sähköisillä välineillä, jotka on suojattu 5 luvun mukaisesti hyväksytyillä salaustuotteilla;

b) jos a alakohdassa tarkoitettuja välineitä ei käytetä, EU:n turvallisuusluokitellut tiedot on kuljetettava joko

   i) 5 luvun mukaisesti hyväksytyillä salaustuotteilla suojatuilla sähköisillä viestimillä (esim. USB-muistitikut, CD-levyt ja kiintolevyt); tai

   ii) kaikissa muissa tapauksissa soveltamissäännöissä esitetyllä tavalla.

*22 artikla*

**Turvallisuusluokat ja -merkinnät**

1. Tiedot on turvallisuusluokiteltava, jos niiden luottamuksellisuus on suojattava 3 artiklan 1 kohdan mukaisesti.

2. EU:n turvallisuusluokiteltujen tietojen luovuttaja vastaa tietojen turvallisuusluokan määrittelystä asiaankuuluvien soveltamissääntöjen, vaatimusten ja ohjeiden mukaisesti, sekä niiden alustavasta jakelusta.

3. EU:n turvallisuusluokiteltujen tietojen turvallisuusluokka on määritettävä 3 artiklan 2 kohdan ja asiaankuuluvien soveltamissääntöjen mukaisesti.

4. Turvallisuusluokka on merkittävä selvästi ja oikein riippumatta siitä, ovatko EU:n turvallisuusluokitellut tiedot paperilla, suullisia, sähköisiä tai jossakin muussa muodossa.

5. Tietyn asiakirjan yksittäiset osat (kuten sivut, kohdat, jaksot, liitteet, lisäykset ja saatteet) saattavat edellyttää eri turvallisuusluokkia, ja ne voidaan merkitä sen mukaisesti, myös sähköisesti tallennettaessa.

6. Koko asiakirjan tai tiedoston turvallisuusluokan on oltava vähintään yhtä korkea kuin sen korkeimpaan turvallisuusluokkaan määritellyn osan turvallisuusluokka. Jos eri lähteistä peräisin olevia tietoja yhdistetään, lopputuotetta on tarkasteltava sen turvallisuusluokan määrittämiseksi, koska se voi edellyttää korkeampaa turvallisuusluokkaa kuin sen muodostavat osat.

7. Asiakirja, joka sisältää eri turvallisuusluokkiin kuuluvia osia, on mahdollisuuksien mukaan laadittava niin, että eri turvallisuusluokkiin kuuluvat osat voidaan helposti tunnistaa ja tarvittaessa irrottaa.

8. Liitteitä sisältävän kirjeen tai tiedonannon turvallisuusluokan on oltava yhtä korkea kuin sen liitteiden korkein turvallisuusluokka. Luovuttajan on ilmoitettava liitteistään irrotetun asiakirjan turvallisuusluokka selvästi asiaankuuluvalla merkinnällä esimerkiksi näin:

CONFIDENTIEL UE/EU CONFIDENTIAL

Ilman liitteitä: RESTREINT UE/EU RESTRICTED

*23 artikla*

**Merkinnät**

Edellä olevan 3 artiklan 2 kohdassa säädettyjen turvallisuusluokitusmerkintöjen lisäksi EU:n turvallisuusluokitelluissa tiedoissa voi olla muita merkintöjä, esimerkiksi

a) tunniste, josta käy ilmi luovuttaja;

b) varoitus, koodisana tai lyhenne, jolla tarkennetaan asiakirjan aihealue, erityisjakelu tiedonsaantitarpeen perusteella tai käyttörajoitukset;

c) luovutettavuutta koskeva merkintä;

d) tapauksen mukaan päivämäärä tai tietty tapahtuma, jonka jälkeen turvallisuusluokkaa voidaan alentaa tai se voidaan poistaa.

*24 artikla*

**Turvallisuusluokitusmerkintöjen lyhenteet**

1. Tekstin yksittäisten kappaleiden turvallisuusluokan merkitsemiseen voidaan käyttää vakiomuotoisia turvallisuusluokitusmerkintöjen lyhenteitä. Ne eivät korvaa täydellisiä turvallisuusluokitusmerkintöjä.

2. EU:n turvallisuusluokitelluissa asiakirjoissa voidaan käyttää seuraavia vakiomuotoisia lyhenteitä, joilla ilmoitetaan alle sivun mittaisten jaksojen tai tekstiosuuksien 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 |

*25 artikla*

**EU:n turvallisuusluokiteltujen tietojen tuottaminen**

1. EU:n turvallisuusluokiteltua asiakirjaa laadittaessa

a) turvallisuusluokka on merkittävä selvästi jokaiselle sivulle;

b) jokainen sivu on numeroitava;

c) asiakirjalla on oltava rekisteröintinumero ja aihe, joka ei ole turvallisuusluokiteltua tietoa, ellei sitä ole merkitty sellaiseksi;

d) asiakirja on päivättävä;

e) SECRET UE/EU SECRET- tai sitä korkeammalle tasolle luokitellun asiakirjan jokaiselle sivulle on merkittävä jäljennöksen numero, jos asiakirjaa on tarkoitus jakaa useampana kappaleena.

2. Jos 1 kohtaa ei ole mahdollista soveltaa EU:n turvallisuusluokiteltuihin tietoihin, on toteutettava muita aiheellisia toimenpiteitä soveltamissääntöjen mukaisesti.

*26 artikla*

**EU:n turvallisuusluokiteltujen tietojen turvallisuusluokan alentaminen ja poistaminen**

1. EU:n turvallisuusluokiteltuja tietoja tuottaessaan luovuttajan on mahdollisuuksien mukaan ilmoitettava, voidaanko turvallisuusluokkaa alentaa tai voidaanko se poistaa tiettynä päivämääränä tai tietyn tapahtuman jälkeen.

2. Kukin komission osasto tarkistaa säännöllisesti niiden EU:n turvallisuusluokiteltujen tietojen osalta, joiden luovuttaja se on, onko niiden turvallisuusluokka edelleen asianmukainen. Soveltamissäännöillä otetaan käyttöön järjestelmä komission luovuttamien, rekisteröityjen EU:n turvallisuusluokiteltujen tietojen turvallisuusluokan tarkistamiseksi vähintään viiden vuoden välein. Tarkistaminen ei ole tarpeen, jos luovuttaja on alun perin ilmoittanut, että turvallisuusluokkaa alennetaan tai se poistetaan ilman eri toimenpiteitä, ja jos tiedoissa on asiasta merkintä.

3. Tasolle RESTREINT UE/EU RESTRICTED luokiteltujen, komission luovuttamien tietojen turvallisuusluokka poistetaan ilman eri toimenpiteitä 30 vuoden kuluttua asetuksen (ETY, Euratom) N:o 354/83, sellaisena kuin se on muutettuna neuvoston asetuksella (EY, Euratom) N:o 1700/2003 ([1]), mukaisesti.

*27 artikla*

**EU:n turvallisuusluokiteltujen tietojen rekisteröintijärjestelmä komissiossa**

1. Jokaisessa komission osastossa, jossa käsitellään tai säilytetään CONFIDENTIEL UE/EU CONFIDENTIAL- ja SECRET UE/EU SECRET -tason EU:n turvallisuusluokiteltuja tietoja, on nimettävä vastuullinen EU:n turvallisuusluokiteltujen tietojen paikallisrekisteri sen varmistamiseksi, että kyseisiä tietoja käsitellään tämän päätöksen mukaisesti, sanotun kuitenkaan rajoittamatta 52 artiklan 5 kohdan soveltamista.

2. Pääsihteeristön hallinnoima EU:n turvallisuusluokiteltujen tietojen rekisteri toimii komission EU:n turvallisuusluokiteltujen tietojen keskusrekisterinä. Se toimii

— komission pääsihteeristön EU:n turvallisuusluokiteltujen tietojen paikallisrekisterinä;

— komission jäsenten kabinettien EU:n turvallisuusluokiteltujen tietojen rekisterinä, paitsi jos niille on nimetty paikallisrekisteri;

— sellaisten pääosastojen tai yksikköjen EU:n turvallisuusluokiteltujen tietojen rekisterinä, joilla ei ole paikallisrekisteriä;

— pääasiallisena saapumis- ja lähtöpaikkana kaikille RESTREINT UE/EU RESTRICTED -tasolle ja aina SECRET UE/EU SECRET -tasoon asti luokitelluille tiedoille, joita komissio ja sen yksiköt ja, jos asiasta on sovittu erityisjärjestelyin, muut unionin toimielimet, elimet ja laitokset vaihtavat kolmansien maiden ja kansainvälisten järjestöjen kanssa.

3. Komission sisällä komission turvallisuusviranomainen nimeää rekisterin, joka toimii tasolle TRES SECRET UE/EU TOP SECRET luokiteltujen tietojen vastaanotosta ja lähettämisestä vastaavana keskusviranomaisena. Tarvittaessa voidaan nimetä alarekistereitä näiden tietojen käsittelemiseksi rekisteröintiä varten.

4. Alarekisterit eivät saa siirtää TRES SECRET UE/EU TOP SECRET -tason asiakirjoja suoraan toisiin saman TRES SECRET UE/EU TOP SECRET -keskusrekisterin alarekistereihin tai niiden ulkopuolelle ilman keskusrekisterin nimenomaista kirjallista suostumusta.

5. EU:n turvallisuusluokiteltujen tietojen rekisterit on määriteltävä turva-alueiksi 3 luvussa esitetyn mukaisesti, ja komission turvallisuusjärjestelyjen hyväksyntäviranomainen hyväksyy ne.

*28 artikla*

**Rekisterin valvontavastaava**

1. Jokaisella EU:n turvallisuusluokiteltujen tietojen rekisterillä on oltava valvontavastaava.

2. Rekisterin valvontavastaavan on oltava asianmukaisesti turvallisuusselvitetty.

3. Rekisterin valvontavastaava toimii komission osastossa paikallisen turvavastaavan alaisuudessa siltä osin kuin on kyse EU:n turvallisuusluokiteltuja tietoja sisältävien asiakirjojen käsittelyä koskevien säännösten soveltamisesta sekä asiaankuuluvien turvallisuussääntöjen, -vaatimusten ja -ohjeiden noudattamisesta.

4. Rekisterin valvontavastaava suorittaa hänelle osoitetun, EU:n turvallisuusluokiteltujen tietojen rekisterin hallinnointivastuun puitteissa seuraavat tehtävät tämän päätöksen ja asiaankuuluvien soveltamissääntöjen, vaatimusten ja ohjeiden mukaisesti:

— EU:n turvallisuusluokiteltujen tietojen rekisteröintiin, säilyttämiseen, jäljentämiseen, kääntämiseen, siirtämiseen, lähettämiseen ja hävittämiseen tai historiallisiin arkistoihin siirtämiseen liittyvät toiminnot;

— tietojen turvallisuusluokan säilyttämistarpeen tarkistaminen määräajoin;

— muut EU:n turvallisuusluokiteltujen tietojen suojaamiseen liittyvät, soveltamissäännöissä määritellyt tehtävät.

*29 artikla*

**EU:n turvallisuusluokiteltujen tietojen rekisteröinti turvallisuustarkoituksia varten**

1. Tässä päätöksessä turvallisuustarkoituksia varten tapahtuvalla rekisteröinnillä, jäljempänä 'rekisteröinti', tarkoitetaan menettelyjä, joilla tallennetaan EU:n turvallisuusluokiteltujen tietojen elinkaari, mukaan lukien niiden jakelu.

([1]) Neuvoston asetus (EY, Euratom) N:o 1700/2003, annettu 22 päivänä syyskuuta 2003, Euroopan talousyhteisön ja Euroopan atomienergiayhteisön historiallisten arkistojen avaamisesta yleisölle annetun asetuksen (ETY, Euratom) N:o 354/83 muuttamisesta (EUVL L 243, 27.9.2003, s. 1).

2. Kaikki CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeammalle tasolle luokiteltu tieto tai materiaali on rekisteröitävä sille tarkoitetussa rekisterissä, kun se saapuu organisaatioyksikköön tai lähetetään sieltä.

3. Kun EU:n turvallisuusluokiteltuja tietoja käsitellään tai säilytetään viestintä- ja tietojärjestelmässä, rekisteröintimenettelyt voidaan suorittaa järjestelmän omien prosessien avulla.

4. Soveltamissäännöissä on yksityiskohtaisempia säännöksiä turvallisuustarkoituksiin tapahtuvasta EU:n turvallisuusluokiteltujen tietojen rekisteröinnistä.

*30 artikla*

**EU:n turvallisuusluokiteltujen asiakirjojen jäljentäminen ja kääntäminen**

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

2. Jos SECRET UE/EU SECRET- ja sitä alemman turvallisuusluokan asiakirjan luovuttaja ei ole kieltänyt jäljentämästä tai kääntämästä asiakirjaa, se voidaan jäljentää tai kääntää niiden haltijan pyynnöstä.

3. Jäljennöksiin ja käännöksiin on sovellettava alkuperäistä asiakirjaa koskevia turvatoimia.

*31 artikla*

**EU:n turvallisuusluokiteltujen tietojen kuljetus**

1. EU:n turvallisuusluokiteltuja tietoja on kuljetettava niin, että ne suojataan luvattomalta ilmitulolta.

2. EU:n turvallisuusluokiteltujen tietojen kuljettamiseen on sovellettava suojatoimia, jotka on

— suhteutettu kuljetettavien EU:n turvallisuusluokiteltujen tietojen turvallisuusluokkaan;

— mukautettu niiden kuljetusolosuhteisiin erityisesti sen perusteella, kuljetetaanko niitä

  — yhden komission rakennuksen sisällä vai komission rakennuksista muodostuvan suljetun ryhmän sisällä,

  — samassa jäsenvaltioissa sijaitsevien komission rakennusten välillä,

  — unionin alueella,

  — unionista kolmannen valtion alueelle; ja

  — mukautettu EU:n turvallisuusluokiteltujen tietojen luonteeseen ja muotoon.

3. Näistä suojatoimista säädetään yksityiskohtaisesti soveltamissäännöissä tai, 42 artiklassa tarkoitettujen hankkeiden ja ohjelmien tapauksessa, asianomaisen ohjelman tai hankkeen turvallisuusohjeissa.

4. Soveltamissääntöihin tai turvallisuusohjeisiin on sisällyttävä EU:n turvallisuusluokiteltujen tietojen turvallisuusluokkaan suhteutettuja säännöksiä seuraavista:

— kuljetustapa, esimerkiksi henkilökohtaisesti, diplomaatti- tai sotilaskuriirin välityksellä taikka postipalveluja tai kaupallisia lähettipalveluja käyttäen;

— EU:n turvallisuusluokiteltujen tietojen pakkaaminen;

— sähköisillä viestimillä kuljetettavien EU:n turvallisuusluokiteltujen tietojen tekniset vastatoimet;

— muut menettelyä koskevat taikka fyysiset tai sähköiset toimet;

— rekisteröintimenettelyt;

— turvallisuusvaltuutuksen omaavan henkilöstön käyttö.

5. Jos EU:n turvallisuusluokiteltuja tietoja kuljetetaan sähköisillä viestimillä ja sen estämättä, mitä 21 artiklan 5 kohdassa säädetään, soveltamissäännöissä esitettyjä suojatoimia voidaan täydentää komission turvallisuusviranomaisen hyväksymillä asianmukaisilla teknisillä vastatoimilla häviämisen tai vaarantumisen riskin minimoimiseksi.

*32 artikla*

**EU:n turvallisuusluokiteltujen tietojen hävittäminen**

1. EU:n turvallisuusluokitellut asiakirjat, joita ei enää tarvita, voidaan hävittää ottaen huomioon arkistoja koskevat määräykset, asiakirjojen hallinnointia ja arkistointia koskevat komission säännöt ja määräykset sekä varsinkin Euroopan komission tiedostoja koskevan yhteisen säilytysluettelon.

2. CONFIDENTIEL UE/EU CONFIDENTIAL- ja sitä korkeamman tason EU:n turvallisuusluokitellut tiedot hävittää vastuullisen EU:n turvallisuusluokiteltujen tietojen rekisterin valvontavastaava haltijan tai toimivaltaisen viranomaisen pyynnöstä. Hävittämisen jälkeen rekisterin valvontavastaava päivittää lokikirjat ja muut rekisteröintitiedot.

3. Rekisterin valvontavastaajan on hävitettävä SECRET UE/EU SECRET- tai TRES SECRET UE/EU TOP SECRET -tasolle luokitellut asiakirjat todistajan läsnä ollessa; todistajan on oltava turvallisuusselvitetty vähintään hävitettävän asiakirjan turvallisuusluokkaa vastaavalle tasolle.

4. Sekä rekisterinpitäjän että todistajan, jos jälkimmäisen läsnäoloa edellytetään, on allekirjoitettava hävittämistodistus, joka tallennetaan rekisteriin. EU:n turvallisuusluokiteltujen tietojen vastuullisen rekisterin valvontavastaava säilyttää 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.

5. Turvallisuusluokitellut asiakirjat, myös RESTREINT UE/EU RESTRICTED -tason asiakirjat, on hävitettävä käyttäen menetelmiä, jotka määritellään soveltamissäännöissä ja jotka täyttävät asiaa koskevat EU:n vaatimukset tai vastaavat.

6. EU:n turvallisuusluokiteltuja tietoja sisältävät ATK-tallennevälineet on hävitettävä soveltamissäännöissä vahvistettujen menettelyjen mukaisesti.

*33 artikla*

**EU:n turvallisuusluokiteltujen tietojen hävittäminen hätätilanteissa**

1. EU:n turvallisuusluokiteltuja tietoja hallussaan pitävät komission osastot laativat paikallisiin olosuhteisiin perustuvat suunnitelmat EU:n turvaluokitellun materiaalin suojaamiseksi kriisitilanteessa, tarvittaessa myös suunnitelmat hävittämistä ja evakuointia varten hätätapauksissa. Ne julkistavat ohjeet, joita pidetään tarpeellisina EU:n turvallisuusluokiteltujen tietojen sivullisille joutumisen estämiseksi.

2. Järjestelyt CONFIDENTIEL UE/EU CONFIDENTIAL- ja SECRET UE/EU SECRET -tasolle luokitellun materiaalin suojaamiseksi ja/tai hävittämiseksi kriisitilanteessa eivät saa missään tapauksessa vaikuttaa haitallisesti TRÈS SECRET UE/EU TOP SECRET -tasolle luokitellun materiaalin suojaamiseen tai hävittämiseen, mukaan lukien salauslaitteisto, jonka käsittely on kaikkia muita tehtäviä kiireellisempi.

3. Hätätapauksessa, jos on olemassa EU:n turvallisuusluokiteltujen tietojen luvattoman ilmitulon välitön vaara, haltijan on tuhottava tiedot niin, ettei niitä voida palauttaa ennalleen kokonaan eikä osittain. Luovuttajalle ja luovuttavalle rekisterille on ilmoitettava rekisteröityjen EU:n turvallisuusluokiteltujen tietojen hävittämisestä hätätapauksessa.

4. Yksityiskohtaisempia säännöksiä EU:n turvallisuusluokiteltujen tietojen hävittämisestä annetaan soveltamissäännöissä.

5 LUKU

**EU:N TURVALLISUUSLUOKITELTUJEN TIETOJEN SUOJAAMINEN VIESTINTÄ- JA TIETOJÄRJESTELMISSÄ**

*34 artikla*

**Tietojen turvaamisen perusperiaatteet**

1. Tietojen turvaamisella tarkoitetaan viestintä- ja tietojärjestelmien alalla varmuutta siitä, että järjestelmät suojaavat niissä käsiteltävät tiedot ja toimivat siten kuin ja silloin kun niiden kuuluu toimia oikeutettujen käyttäjien valvonnassa.

2. Tietojen tehokkaalla turvaamisella varmistetaan seuraavien asianmukainen taso:

Aitous: tae siitä, että tiedot ovat aitoja ja vilpittömässä mielessä toimivista lähteistä;

Käytettävyys: tiedot ovat valtuutetun yksikön pyynnöstä saatavilla ja käytettävissä;

Luottamuksellisuus: tiedot eivät tule ilmi sivullisille henkilöille, yksiköille eikä prosesseille;

Eheys: omaisuuden ja tietojen oikeellisuus ja täydellisyys turvataan;

Kiistattomuus: tietty toimi tai tapahtuma voidaan todistaa tapahtuneeksi niin, ettei sitä voida myöhemmin kiistää.

3. Tietojen turvaamisen on perustuttava riskinhallintaprosessiin.

*35 artikla*

**Määritelmät**

Tässä luvussa tarkoitetaan

a) 'hyväksynnällä' turvallisuusjärjestelyjen hyväksyntäviranomaisen viestintä- ja tietojärjestelmälle antamaa muodollista valtuutusta ja hyväksyntää muokata EU:n turvallisuusluokiteltuja tietoja toimintaympäristössään sen jälkeen, kun turvallisuussuunnitelma on muodollisesti vahvistettu ja pantu asianmukaisesti täytäntöön;

b) 'hyväksyntämenettelyllä' toimenpiteitä ja tehtäviä, jotka on suoritettava ennen turvallisuusjärjestelyjen hyväksyntäviranomaisen hyväksyntää. Nämä toimenpiteet ja tehtävät on määriteltävä hyväksyntämenettelystandardissa;

c) 'viestintä- ja tietojärjestelmällä' järjestelmää, joka mahdollistaa tietojen käsittelyn sähköisessä muodossa. Viestintä- ja tietojärjestelmä käsittää kaikki toimintansa edellyttämät resurssit, myös infrastruktuurin, organisaation, henkilöstön ja tietoresurssit;

d) 'jäännösriskillä' riskiä, joka jää jäljelle, kun turvatoimet on toteutettu, ottaen huomioon, että kaikkia uhkia ei voida torjua eikä kaikkea haavoittuvuutta poistaa;

e) 'riskillä' mahdollisuutta, että tietty uhka hyötyy organisaation tai minkä tahansa sen käyttämän järjestelmän sisäisestä ja ulkoisesta haavoittuvuudesta ja aiheuttaa siten vahinkoa organisaatiolle ja sen aineelliselle tai aineettomalle omaisuudelle. Sen mittana on uhkien toteutumisen todennäköisyys yhdistettynä niiden vaikutuksiin;

f) 'riskin hyväksynnällä' päätöstä hyväksyä jäännösriskin olemassaolo riskin käsittelyn jälkeen;

g) 'riskinarvioinnilla' uhkien ja haavoittuvuuden tunnistamista ja niihin liittyvän riskianalyysin eli todennäköisyyden ja vaikutusten analyysin tekemistä;

h) 'riskiviestinnällä' viestintä- ja tietojärjestelmien käyttäjäyhteisöjen riskitietoisuuden lisäämistä sekä riskeistä tiedottamista hyväksyntäviranomaisille ja niistä raportoimista toiminnasta vastaaville viranomaisille;

i) 'riskin käsittelyllä' riskin lieventämistä, poistamista, vähentämistä (teknisiä, fyysisiä, organisatorisia tai menettelyyn liittyviä toimenpiteitä tarkoituksenmukaisesti yhdistämällä), siirtämistä ja seuraamista.

*36 artikla*

**EU:n turvallisuusluokiteltujen tietojen käsittely viestintä- ja tietojärjestelmissä**

1. EU:n turvallisuusluokiteltuja tietoja viestintä- ja tietojärjestelmissä käsiteltäessä on noudatettava tietojen turvaamisperiaatetta.

2. EU:n turvallisuusluokiteltuja tietoja käsittelevien viestintä- ja tietojärjestelmien osalta tietojärjestelmien turvallisuutta koskevan komission politiikan, sellaisena kuin se esitetään komission päätöksessä C(2006) 3602 ([1]), noudattamisella tarkoitetaan, että

a) tietojärjestelmiä koskevan turvallisuuspolitiikan täytäntöönpanoon on sovellettava tietojärjestelmän koko elinkaaren ajan "suunnittele/toteuta/tarkista/toimi" -lähestymistapaa;

b) turvatarpeet on määriteltävä toimintaan kohdistuvien vaikutusten arvioinnin avulla;

c) tietojärjestelmälle ja sen sisältämille tiedoille on tehtävä muodollinen resurssiluokittelu;

([1]) C(2006) 3602 concerning the security of information systems used by the European Commission, 16.8.2006.

d) kaikki tietojärjestelmien turvallisuuspolitiikassa määritellyt pakolliset turvatoimet on toteutettava;

e) on sovellettava riskinhallintaprosessia, joka käsittää seuraavat vaiheet: uhkan ja haavoittuvuuden tunnistaminen, riskinarviointi, riskin käsittely, riskin hyväksyntä ja riskiviestintä;

f) laaditaan, pannaan täytäntöön, tarkistetaan ja uudelleenarvioidaan turvallisuussuunnitelma, joka käsittää myös turvallisuuspolitiikan ja -menettelyt.

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

4. Jos EU:n turvallisuusluokiteltujen tietojen suojaamiseen käytetään salaustuotteita, ne on hyväksyttävä seuraavasti:

a) etusija on annettava tuotteille, jotka neuvosto tai sen pääsihteeri on hyväksynyt neuvoston salauslaitteiden hyväksyntäviranomaisena komission turvallisuusasiantuntijaryhmän suosituksesta;

b) komission salauslaitteiden hyväksyntäviranomainen voi komission turvallisuusasiantuntijaryhmän suosituksesta luopua a alakohdassa esitetyistä vaatimuksista ja myöntää tilapäisen hyväksynnän tietyksi ajanjaksoksi, jos se on perusteltua erityisistä toiminnallisista syistä.

5. EU:n turvallisuusluokiteltuja tietoja sähköisesti siirrettäessä, muokattaessa ja säilytettäessä on käytettävä hyväksyttyjä salaustuotteita. Hätätilanteissa tai tiettyjen teknisten määritysten osalta voidaan tästä vaatimuksesta poiketen soveltaa erityisiä menettelyjä sen jälkeen, kun salauslaitteiden hyväksyntäviranomainen on antanut hyväksyntänsä.

6. CONFIDENTIEL UE/EU CONFIDENTIAL- ja sitä korkeamman turvallisuusluokan tietoja käsittelevien viestintä- ja tietojärjestelmien suojaamiseksi on toteutettava turvatoimia, joilla estetään tietojen vaarantuminen tahattoman sähkömagneettisen säteilyn takia (nk. TEMPEST-turvatoimet). Nämä turvatoimet on suhteutettava tietojen hyväksikäytön vaaraan ja turvallisuusluokkaan.

7. Komission turvallisuusviranomainen toimii seuraavissa tehtävissä:

— tiedonturvaamisviranomainen;

— turvallisuusjärjestelyjen hyväksyntäviranomainen;

— TEMPEST-viranomainen;

— salauslaitteiden hyväksyntäviranomainen;

— salatun aineiston jakelusta vastaava viranomainen.

8. Komission turvallisuusviranomainen nimittää kullekin järjestelmälle operatiivisen tiedonturvaamisviranomaisen.

9. Soveltamissäännöissä määritellään 7 ja 8 kohdassa mainittuihin tehtäviin kuuluvat vastuut.

*37 artikla*

**EU:n turvallisuusluokiteltuja tietoja käsittelevien viestintä- ja tietojärjestelmien hyväksyntä**

1. Kaikkien EU:n turvallisuusluokiteltuja tietoja käsittelevien viestintä- ja tietojärjestelmien on käytävä läpi tietojen turvaamisperiaatteisiin perustuva hyväksyntämenettely, jonka yksityiskohdat on suhteutettava vaaditun suojan tasoon.

2. Hyväksyntämenettelyyn kuuluu komission turvallisuusjärjestelyjen hyväksyntäviranomaisen antama muodollinen vahvistus asianomaisen viestintä- ja tietojärjestelmän turvallisuussuunnitelmalle sen varmistamiseksi, että

a) 36 artiklan 2 kohdassa kuvattu riskinhallintaprosessi on suoritettu asianmukaisesti;

b) järjestelmävastaava on tietoisesti hyväksynyt jäännösriskin; ja

c) viestintä- ja tietojärjestelmän ja siinä käsiteltävien EU:n turvallisuusluokiteltujen tietojen suojaamisessa on saavutettu tämän päätöksen mukainen riittävä taso.

3. Komission turvallisuusjärjestelyjen hyväksyntäviranomainen antaa hyväksymislausunnon, jossa määritetään niiden EU:n turvallisuusluokiteltujen tietojen korkein taso, joita viestintä- ja tietojärjestelmässä voidaan käsitellä, ja vastaavat toimintaedellytykset. Tämä ei kuitenkaan rajoita Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 512/2014 ([1]) 11 artiklassa määritellylle turvallisuusjärjestelyjen hyväksyntälautakunnalle uskottuja tehtäviä.

4. Yhteinen turvallisuusjärjestelyjen hyväksyntälautakunta vastaa sellaisten komission viestintä- ja tietojärjestelmien hyväksymisestä, joissa on useampi osapuoli. Lautakunta muodostuu kunkin osapuolen turvallisuusjärjestelyjen hyväksyntäviranomaisen edustajasta, ja sen puheenjohtajana toimii komission turvallisuusjärjestelyjen hyväksyntäviranomaisen edustaja.

5. Hyväksyntämenettely muodostuu useista osapuolten suorittamista tehtävistä. Vastuu hyväksyntäasiakirjojen laatimisesta on yksin viestintä- ja tietojärjestelmän vastaavalla.

6. Hyväksynnästä vastaa komission turvallisuusjärjestelyjen hyväksyntäviranomainen, jolla on missä tahansa viestintä- ja tietojärjestelmän elinkaaren vaiheessa oikeus

a) vaatia hyväksyntämenettelyn soveltamista;

b) tarkastaa viestintä- ja tietojärjestelmä;

c) vaatia turvallisuuden parantamissuunnitelman laatimista ja tehokasta täytäntöönpanoa tarkkaan määritetyssä aikataulussa, jos toimintaedellytykset eivät enää täyty, ja mahdollisesti perua viestintä- ja tietojärjestelmän toimilupa, kunnes toimintaedellytykset taas täyttyvät.

7. Hyväksyntämenettely määritellään EU:n turvallisuusluokiteltuja tietoja käsittelevien viestintä- ja tietojärjestelmien hyväksyntämenettelystandardissa, joka vahvistetaan päätöksen C(2006) 3602 10 artiklan 3 kohdan mukaisesti.

*38 artikla*

**Hätätilanteet**

1. Jäljempänä kuvattuja erityismenettelyjä voidaan soveltaa hätätapauksessa, esimerkiksi kriisi-, konflikti- tai sotatilanteen uhatessa tai toteutuessa taikka poikkeuksellisissa toimintaolosuhteissa, sanotun kuitenkaan rajoittamatta tämän luvun säännösten soveltamista.

2. EU:n turvallisuusluokiteltujen tietojen siirtämisessä voidaan käyttää alempaa turvallisuusluokkaa varten hyväksyttyjä salaustuotteita tai ne voidaan siirtää ilman salausta toimivaltaisen viranomaisen suostumuksella, jos mahdollinen viive aiheuttaisi selvästi suuremman vahingon kuin turvallisuusluokitellun materiaalin ilmitulon aiheuttama vahinko ja jos

a) lähettäjällä ja vastaanottajalla ei ole vaadittua salauslaitetta; ja

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

3. Edellä 1 kohdassa esitetyissä olosuhteissa siirrettävissä turvallisuusluokitelluissa tiedoissa ei saa olla mitään merkintöjä tai mainintoja, jotka erottavat ne turvallisuusluokittelemattomista tiedoista tai tiedoista, jotka voidaan suojata käytettävissä olevalla salaustuotteella. Tietojen turvallisuusluokka on ilmoitettava muulla tavoin viipymättä vastaanottajille.

4. Asiasta on tämän jälkeen laadittava raportti toimivaltaiselle viranomaiselle ja komission turvallisuusasiantuntijaryhmälle.

6 LUKU

**YHTEISÖTURVALLISUUS**

*39 artikla*

**Perusperiaatteet**

1. Yhteisöturvallisuudella tarkoitetaan toimenpiteitä, joilla varmistetaan EU:n turvallisuusluokiteltujen tietojen suojaaminen

a) turvallisuusluokiteltujen hankintasopimusten nojalla

   i) ehdokkaiden tai tarjoajien toimesta koko tarjouskilpailu- ja sopimuksentekomenettelyn ajan,

   ii) toimeksisaajien tai alihankkijoiden toimesta turvallisuusluokiteltujen hankintasopimusten koko elinkaaren ajan;

([1]) Euroopan parlamentin ja neuvoston asetus (EU) N:o 512/2014, annettu 16 päivänä huhtikuuta 2014, Euroopan GNSS-viraston perustamisesta annetun asetuksen (EU) N:o 912/2010 muuttamisesta (EUVL L 150, 20.5.2014, s. 72).

b) turvallisuusluokiteltujen avustussopimusten nojalla

i) hakijoiden toimesta avustuksen myöntämismenettelyn aikana,

ii) avunsaajien toimesta turvallisuusluokiteltujen avustussopimusten koko elinkaaren ajan.

2. Tällaiset hankinta- tai avustussopimukset eivät saa koskea TRES SECRET UE/EU TOP SECRET -tasolle luokiteltuja tietoja.

3. Jollei toisin säädetä, turvallisuusluokiteltuja hankintasopimuksia ja toimeksisaajia koskevia tämän luvun säännöksiä on sovellettava myös turvallisuusluokiteltuihin alihankintasopimuksiin ja alihankkijoihin.

*40 artikla*

**Määritelmät**

Tätä lukua sovellettaessa tarkoitetaan

a) 'turvallisuusluokitellulla hankintasopimuksella' neuvoston asetuksessa (EY, Euratom) N:o 1605/2002 ([1]) tarkoitettua puitesopimusta tai sopimusta, jonka komissio tai jokin sen osasto tekee toimeksisaajan kanssa irtaimen tai kiinteän omaisuuden, työsuoritusten tai palveluiden hankkimiseksi ja jonka täyttäminen edellyttää tai siihen kuuluu EU:n turvallisuusluokiteltujen tietojen tuottamista, käsittelyä tai säilyttämistä;

b) 'turvallisuusluokitellulla alihankintasopimuksella' sopimusta, jonka komissio tai joku sen osasto tekee toisen toimeksisaajan (eli alihankkijan) kanssa irtaimen tai kiinteä omaisuuden, työsuoritusten tai palveluiden hankkimiseksi ja jonka täyttäminen edellyttää tai siihen kuuluu EU:n turvallisuusluokiteltujen tietojen tuottamista, käsittelyä tai säilyttämistä;

c) 'turvallisuusluokitellulla avustussopimuksella' sopimusta, jolla komissio myöntää asetuksen (EY, Euratom) N:o 1605/2002 VI osaston I osassa tarkoitetun avustuksen ja jonka täyttäminen edellyttää tai siihen kuuluu EU:n turvallisuusluokiteltujen tietojen tuottamista, käsittelyä tai säilyttämistä;

d) 'nimetyllä turvallisuusviranomaisella' jäsenvaltion kansalliselle turvallisuusviranomaiselle vastuussa olevaa viranomaista, jonka vastuulla on tiedottaa yhteisöille tai muille yksiköille kaikkiin yhteisöturvallisuutta koskeviin asioihin sovellettavasta kansallisesta politiikasta sekä antaa ohjausta ja apua kyseisen politiikan täytäntöönpanossa. Kansallinen turvallisuusviranomainen tai mikä tahansa muu toimivaltainen viranomainen voi hoitaa nimetyn turvallisuusviranomaisen tehtävää.

*41 artikla*

**Turvallisuusluokiteltuihin hankinta- ja avustussopimuksiin sovellettava menettely**

1. Kukin komission osasto varmistaa hankintaviranomaisen ominaisuudessa, että hankintasopimuksessa viitataan tässä luvussa säädettyihin yhteisöturvallisuutta koskeviin vähimmäisvaatimuksiin tai että ne sisältyvät siihen ja että niitä noudatetaan turvallisuusluokiteltuja hankinta- tai avustussopimuksia tehtäessä.

2. Komission toimivaltaiset yksiköt pyytävät 1 kohdan soveltamiseksi neuvoa henkilöstöhallinnon ja turvallisuustoiminnan pääosastolta ja erityisesti sen turvallisuudesta vastaavalta linjalta ja varmistavat, että hankinta-, alihankinta- ja avustussopimusten malleihin sisältyy määräyksiä EU:n turvallisuusluokiteltujen tietojen suojaamista koskevista perusperiaatteista ja vähimmäisvaatimuksista, joita toimeksisaajien, alihankkijoiden ja avunsaajien on noudatettava.

3. Komissio tekee tiivistä yhteistyötä asianomaisen jäsenvaltion kansallisen turvallisuusviranomaisen, nimetyn turvallisuusviranomaisen tai muun toimivaltaisen viranomaisen kanssa.

4. Kun hankintaviranomainen aikoo käynnistää menettelyn turvallisuusluokitellun hankinta- tai avustussopimuksen tekemiseksi, se pyytää komission turvallisuusviranomaiselta neuvoa menettelyn luottamuksellisuutta ja turvallisuusluokiteltuja osia koskevissa asioissa menettelyn kaikissa vaiheissa.

5. Yhteisöturvallisuutta koskevissa soveltamissäännöissä esitetään turvallisuusluokiteltujen hankinta-, alihankinta- ja avustussopimusten sekä hankintailmoitusten mallit, ohjeet olosuhteista, joissa edellytetään yhteisöturvallisuusselvitystä, ohjelman tai hankkeen turvallisuusohjeet, turvallisuutta koskevat lisälausekkeet samoin kuin vierailuja sekä EU:n turvallisuusluokiteltujen tietojen siirtoa ja kuljetusta turvallisuusluokiteltujen hankinta- tai avustussopimusten nojalla koskevat säännöt sen jälkeen, kun asiassa on kuultu komission turvallisuusasiantuntijaryhmää.

([1]) Neuvoston asetus (EY, Euratom) N:o 1605/2002, annettu 25 päivänä kesäkuuta 2002, Euroopan yhteisöjen yleiseen talousarvioon sovellettavasta varainhoitoasetuksesta (EYVL L 248, 16.9.2002, s. 1).

6. Komissio voi tehdä turvallisuusluokitellun hankinta- tai avustussopimuksen, jolla jäsenvaltioon tai sellaiseen kolmanteen valtioon, jonka kanssa on tehty sopimus tai sovittu hallinnollisesta järjestelystä tämän päätöksen 7 luvun mukaisesti, rekisteröityneelle talouden toimijalle annetaan tehtäviä, joihin liittyy pääsy EU:n turvallisuusluokiteltuihin tietoihin tai niiden käsittelyä tai säilytystä.

*42 artikla*

**Turvallisuusluokitellun hankinta- tai avustussopimuksen turvallisuutta koskevat osat**

1. Turvallisuusluokiteltuun hankinta- tai avustussopimukseen on sisällyttävä seuraavat turvallisuutta koskevat osat:

Ohjelman tai hankkeen turvallisuusohjeet

a) 'Ohjelman tai hankkeen turvallisuusohjeilla' tarkoitetaan luetteloa turvallisuusmenettelyistä, joita sovelletaan tiettyyn ohjelmaan tai hankkeeseen turvallisuusmenettelyjen yhdenmukaistamiseksi. Niitä voidaan tarkistaa missä tahansa ohjelman tai hankkeen vaiheessa.

b) Henkilöstöhallinnon ja turvallisuustoiminnan pääosasto laatii ohjelman tai hankkeen yleiset turvallisuusohjeet. Sellaisista ohjelmista ja hankkeista vastaavat komission osastot, joihin liittyy EU:n turvallisuusluokiteltujen tietojen käsittelyä tai säilyttämistä, voivat tarvittaessa laatia ohjelman tai hankkeen erityiset turvallisuusohjeet, jotka perustuvat yleisiin turvallisuusohjeisiin.

c) Ohjelman tai hankkeen erityiset turvallisuusohjeet on laadittava varsinkin sellaisia ohjelmia tai hankkeita varten, jotka ovat huomattavan laaja-alaisia tai monimutkaisia tai joissa on mukana monia ja/tai esimerkiksi oikeudelliselta asemaltaan erityyppisiä toimeksisaajia, avunsaajia sekä muita kumppaneita ja sidosryhmiä. Ohjelmaa tai hanketta hallinoiva(t) komission osasto(t) laatii(vat) ohjelman tai hankkeen erityiset turvallisuusohjeet tiiviissä yhteistyössä henkilöstöhallinnon ja turvallisuustoiminnan pääosaston kanssa.

d) Henkilöstöhallinnon ja turvallisuustoiminnan pääosasto toimittaa sekä yleiset että erityiset turvallisuusohjeet komission turvallisuusasiantuntijaryhmälle neuvojen saamiseksi.

Turvallisuutta koskeva lisälauseke

a) 'Turvallisuutta koskevalla lisälausekkeella' tarkoitetaan hankintaviranomaisen määräämien erityissopimusehtojen kokonaisuutta, joka on erottamaton osa pääsyä EU:n turvallisuusluokiteltuihin tietoihin tai niiden tuottamista edellyttävää turvallisuusluokiteltua hankintasopimusta ja jossa yksilöidään turvallisuusvaatimukset ja ne sopimuksen osat, jotka edellyttävät turvallisuuden suojaamista.

b) Turvallisuutta koskevassa lisälausekkeessa on kuvattava sopimuskohtaiset turvallisuusvaatimukset. Se on erottamaton osa turvallisuusluokiteltua hankinta-, alihankinta- tai avustussopimusta, ja siihen on tarvittaessa sisällytettävä turvallisuusluokitteluopas.

c) Turvallisuutta koskevaan lisälausekkeeseen on sisällyttävä määräykset, joilla toimeksisaaja tai avunsaaja velvoitetaan noudattamaan tässä päätöksessä säädettyjä vähimmäisvaatimuksia. Hankintaviranomainen varmistaa, että turvallisuutta koskevasta lisälausekkeesta käy ilmi, että vähimmäisvaatimusten noudattamatta jättäminen voi olla riittävä peruste hankinta- tai avustussopimuksen irtisanomiselle.

2. Sekä ohjelman tai hankkeen turvallisuusohjeisiin että turvallisuutta koskeviin lisälausekkeisiin on sisällyttävä turvallisuusluokitteluopas pakollisena turvallisuutta koskevana osana:

a) 'Turvallisuusluokitteluopas' on asiakirja, jossa kuvataan ohjelman, hankkeen taikka hankinta- tai avustussopimuksen turvallisuusluokiteltavat osat ja eritellään sovellettavat turvallisuusluokat. Turvallisuusluokitteluopasta voidaan laajentaa koko ohjelman tai hankkeen elinkaaren taikka hankinta- tai avustussopimuksen voimassaolon ajan, ja niiden sisältämiä tietoja voidaan luokitella uudelleen tai niiden luokkaa voidaan alentaa; jos turvallisuusluokitteluopas on olemassa, sen on oltava osa turvallisuutta koskevaa lisälauseketta.

b) Ennen tarjouskilpailun käynnistämistä tai turvallisuusluokitellun sopimuksen tekemistä hankintaviranomaisena toimiva komission osasto määrittelee ehdokkaille ja tarjoajille tai toimeksisaajille annettavien tietojen turvallisuusluokan sekä toimeksisaajan tuottamien tietojen turvallisuusluokan. Tätä varten se laatii komission turvallisuusviranomaista kuultuaan turvallisuusluokitteluoppaan, jota käytetään hankintasopimuksen täytäntöönpanossa tämän päätöksen ja sen soveltamissääntöjen mukaisesti.

c) Turvallisuusluokitellun hankintasopimuksen eri osien turvallisuusluokan määrittämisessä sovelletaan seuraavia periaatteita:

i) turvallisuusluokitteluopasta laatiessaan komission osasto ottaa huomioon kaikki asiaankuuluvat turvallisuusnäkökohdat, myös annetuille tiedoille, joiden käytön sopimuksessa niiden luovuttaja on hyväksynyt, määritetyn turvallisuusluokan;

ii) hankintasopimuksen turvallisuusluokka ei voi olla alempi kuin yhdenkään sen osan korkein turvallisuusluokka; ja

iii) hankintaviranomaisen on tarvittaessa ja komission turvallisuusviranomaisen välityksellä oltava yhteydessä jäsenvaltioiden kansalliseen, nimettyyn tai muuhun toimivaltaiseen turvallisuusviranomaiseen siinä tapauksessa, että hankintasopimusta täytettäessä toimeksisaajien tuottamien tai niille annettujen tietojen turvallisuusluokkaa muutetaan ja turvallisuusluokitteluoppaaseen tehdään tämän vuoksi muutoksia.

*43 artikla*

**Toimeksisaajien ja avunsaajien henkilöstön pääsy EU:n turvallisuusluokiteltuihin tietoihin**

Hankintaviranomainen tai avustuksen myöntävä viranomainen varmistaa, että turvallisuusluokiteltuun hanke- tai avustussopimukseen sisältyy määräyksiä siitä, että toimeksisaajan, alihankkijan tai avunsaajan henkilöstölle, jolla on osana sopimuksen täytäntöönpanoa oltava pääsy EU:n turvallisuusluokiteltuihin tietoihin, myönnetään pääsy kyseisiin tietoihin vain, jos

a) henkilöllä on asiaankuuluvan tason turvallisuusvaltuutus tai hänet on muuten asianmukaisesti valtuutettu todennetun tiedonsaantitarpeen perusteella;

b) henkilölle on selvitetty EU:n turvallisuusluokiteltujen tietojen suojaamiseen sovellettavat turvallisuussäännöt ja hän on vahvistanut tällaisten tietojen suojaamista koskevan vastuunsa;

c) kansallinen tai nimetty turvallisuusviranomainen taikka muu toimivaltainen viranomainen on myöntänyt henkilölle turvallisuusselvityksen CONFIDENTIEL UE/EU CONFIDENTIAL- tai SECRET UE/EU SECRET -tasolle luokiteltujen tietojen osalta.

*44 artikla*

**Yhteisöturvallisuusselvitys**

1. 'Yhteisöturvallisuusselvityksellä' tarkoitetaan kansallisen, nimetyn tai muun toimivaltaisen turvallisuusviranomaisen hallinnollista päätöstä, jonka mukaan toimitila tarjoaa turvallisuusnäkökulmasta riittävän suojan tiettyyn turvallisuusluokkaan kuuluville EU:n turvallisuusluokitelluille tiedoille.

2. Jäsenvaltion kansallisen, nimetyn tai muun toimivaltaisen turvallisuusviranomaisen myöntämä yhteisöturvallisuusselvitys, josta käy kansallisten lakien ja asetusten mukaisesti ilmi, että talouden toimija pystyy suojaamaan EU:n turvallisuusluokitellut tiedot asianmukaisella tasolla (CONFIDENTIEL UE/EU CONFIDENTIAL tai SECRET UE/EU SECRET) toimitiloissaan, on esitettävä komission turvallisuusviranomaiselle, joka toimittaa selvityksen hankeviranomaisena tai avustuksen myöntävänä viranomaisena toimivalle komission osastolle ennen kuin ehdokkaalle, tarjoajalle tai toimeksisaajalle taikka avustuksen hakijalle tai saajalle voidaan antaa EU:n turvallisuusluokiteltuja tietoja tai myöntää pääsy niihin.

3. Hankintaviranomainen ilmoittaa tarvittaessa ja komission turvallisuusviranomaisen välityksellä asianmukaiselle kansalliselle, nimetylle tai muulle toimivaltaiselle turvallisuusviranomaiselle, että sopimuksen täytäntöönpano edellyttää yhteisöturvallisuusselvityksen tekemistä. Yhteisö- tai henkilöturvallisuusselvitys vaaditaan, jos hankintamenettelyn tai avustuksen myöntämismenettelyn aikana on annettava CONFIDENTIEL UE/EU CONFIDENTIAL- tai SECRET UE/EU SECRET -tasolle luokiteltuja EU:n turvallisuusluokiteltuja tietoja.

4. Hankintaviranomainen tai avustuksen myöntävä viranomainen ei tee turvallisuusluokiteltua hankinta- tai avustussopimusta valitun tarjoajan tai osallistujan kanssa ennen kuin se on saanut sen jäsenvaltion kansalliselta, nimetyltä tai muulta toimivaltaiselta turvallisuusviranomaiselta, johon asianomainen toimeksisaaja tai alihankkija on rekisteröity, vahvistuksen siitä, että mahdollisesti vaadittava yhteisöturvallisuusselvitys on myönnetty asianmukaisella tasolla.

5. Kun yhteisöturvallisuusselvityksen myöntänyt kansallinen, nimetty tai muu toimivaltainen turvallisuusviranomainen on ilmoittanut komission turvallisuusviranomaiselle selvitykseen vaikuttavista muutoksista, komission turvallisuusviranomainen ilmoittaa asiasta hankintaviranomaisena tai avustuksen myöntävänä viranomaisena toimivalle komission osastolle. Kun kyseessä on alihankintasopimus, asiasta on ilmoitettava kansalliselle, nimetylle tai muulle toimivaltaiselle turvallisuusviranomaiselle.

6. Jos kansallinen, nimetty tai muu toimivaltainen turvallisuusviranomainen peruu yhteisöturvallisuusselvityksen, tämä on hankintaviranomaiselle tai avustuksen myöntävälle viranomaiselle riittävä peruste irtisanoa turvallisuusluokiteltu hankintasopimus tai sulkea ehdokas, tarjoaja tai hakija kilpailun ulkopuolelle. Tätä koskeva määräys on sisällytettävä myöhemmin laadittaviin hankinta- ja avustussopimusten malleihin.

*45 artikla*

**Turvallisuusluokiteltuja hankinta- ja avustussopimuksia koskevat säännökset**

1. Jos ehdokkaalle, tarjoajalle tai hakijalle annetaan EU:n turvallisuusluokiteltuja tietoja hankintamenettelyn aikana, tarjous- tai ehdotuspyynnössä on oltava määräys, jolla ehdokas, tarjoaja tai hakija, joka ei esitä tarjousta tai ehdotusta tai jota ei valita, velvoitetaan palauttamaan kaikki turvallisuusluokitellut asiakirjat ilmoitetussa määräajassa.

2. Hankintaviranomainen tai avustuksen myöntävä viranomainen ilmoittaa komission turvallisuusviranomaisen välityksellä kansalliselle, nimetylle tai muulle toimivaltaiselle turvallisuusviranomaiselle siitä, että turvallisuusluokiteltu hankinta- tai avustussopimus on tehty, samoin kuin asiaankuuluvat tiedot, kuten toimeksisaajan/-saajien tai avunsaajan/-saajien nimen/nimet, sopimuksen keston ja korkeimman turvallisuusluokan.

3. Tällaisen hankinta- tai avustussopimuksen päättyessä hankintaviranomainen tai avustuksen myöntävä viranomainen ilmoittaa asiasta viipymättä komission turvallisuusviranomaisen välityksellä sen jäsenvaltion kansalliselle, nimitetylle tai muulle toimivaltaiselle turvallisuusviranomaiselle, jossa toimeksisaaja tai avunsaaja on rekisteröity.

4. Yleensä toimeksisaajan tai avunsaajan edellytetään palauttavan hankintaviranomaiselle tai avustuksen myöntävälle viranomaiselle turvallisuusluokitellun hankinta- tai avustussopimuksen voimassaolon tai avunsaajan osallistumisen päättyessä kaikki hallussaan olevat EU:n turvallisuusluokitellut tiedot.

5. Turvallisuutta koskevaan lisälausekkeeseen on sisällytettävä erityismääräyksiä EU:n turvallisuusluokiteltujen tietojen hävittämisestä turvallisuusluokitellun hankinta- tai avustussopimuksen täytäntöönpanon aikana tai sen voimassaolon päättyessä.

6. Jos toimeksisaaja tai avunsaaja saa luvan säilyttää EU:n turvallisuusluokiteltuja tietoja turvallisuusluokitellun hankinta- tai avustussopimuksen voimassaolon päätyttyä, tässä päätöksessä säädettyjä vähimmäisvaatimuksia on edelleen noudatettava ja toimeksisaajan tai avunsaajan on huolehdittava EU:n turvallisuusluokiteltujen tietojen luottamuksellisuuden säilymisestä.

*46 artikla*

**Turvallisuusluokiteltuja hankintasopimuksia koskevat erityissäännökset**

1. Tarjouspyynnössä ja turvallisuusluokitellussa hankintasopimuksessa on määriteltävä EU:n turvallisuusluokiteltujen tietojen suojaamista koskevat ehdot, joiden mukaisesti toimeksisaaja voi tehdä alihankintasopimuksia.

2. Toimeksisaajan on saatava hankintaviranomaiselta lupa ennen yhdenkään turvallisuusluokitellun sopimuksen osan antamista alihankkijan toteutettavaksi. Kolmanteen maahan rekisteröityneen alihankkijan kanssa ei voi tehdä alihankintasopimusta, johon liittyy pääsy EU:n turvallisuusluokiteltuihin tietoihin, ellei tietojen turvallisuudesta ole 7 luvussa tarkoitettua sääntelykehystä.

3. Toimeksisaajan tehtävänä on varmistaa, että kaikki alihankintatoiminnot suoritetaan tässä päätöksessä säädettyjen vähimmäisvaatimusten mukaisesti, eikä se saa antaa EU:n turvallisuusluokiteltuja tietoja alihankkijalle ilman hankintaviranomaisen kirjallista etukäteissuostumusta.

4. Jos toimeksisaaja tuottaa tai käsittelee EU:n turvallisuusluokiteltuja tietoja, komission katsotaan olevan niiden luovuttaja, ja tietojen luovuttajan oikeudet kuuluvat hankintaviranomaiselle.

*47 artikla*

**Turvallisuusluokiteltuihin hankintasopimuksiin liittyvät vierailut**

1. Jos komission henkilöstön jäsenellä tai toimeksisaajan tai avunsaajan henkilöstöllä on oltava pääsy CONFIDENTIEL UE/EU CONFIDENTIAL- tai SECRET UE/EU SECRET -tasolle luokiteltuihin tietoihin toistensa tiloissa osana turvallisuusluokitellun hankinta- tai avustussopimuksen täytäntöönpanoa, vierailuista on sovittava asianomaisen kansallisen, nimetyn tai muun toimivaltaisen turvallisuusviranomaisen kanssa. Tällaisista vierailusta on ilmoitettava komission turvallisuusviranomaiselle. Kun on kyse erityisistä ohjelmista tai hankkeista, kansallinen, nimetty tai muu toimivaltainen turvallisuusviranomainen voi kuitenkin sopia menettelystä, jossa vierailut voidaan järjestää suoraan.

2. Kaikilla vierailijoilla on oltava asianmukainen turvallisuusselvitys ja tiedonsaantitarve, jotta heille voidaan myöntää pääsy sellaisiin EU:n turvallisuusluokiteltuihin tietoihin, jotka liittyvät turvallisuusluokiteltuun sopimukseen.

3. Vierailijoille on annettava pääsy vain vierailun tarkoitukseen liittyviin EU:n turvallisuusluokiteltuihin tietoihin.

4. Yksityiskohtaisempia ohjeita annetaan soveltamissäännöissä.

5. Tähän päätökseen ja 4 kohdassa tarkoitettuihin soveltamissääntöihin sisältyvien, turvallisuusluokiteltuihin hankintasopimuksiin liittyviä vierailuja koskevien säännösten noudattaminen on pakollista.

*48 artikla*

**Turvallisuusluokiteltuihin hankinta- tai avustussopimuksiin liittyvien EU:n turvallisuusluokiteltujen tietojen siirto ja kuljetus**

1. EU:n turvallisuusluokiteltujen tietojen siirtämiseen sähköisesti sovelletaan tämän päätöksen 5 luvun asiaankuuluvia säännöksiä.

2. EU:n turvallisuusluokiteltujen tietojen kuljetukseen sovelletaan tämän päätöksen 4 luvun asiaankuuluvia säännöksiä ja päätöksen soveltamissääntöjä kansallisten lakien ja asetusten mukaisesti.

3. Turvallisuusluokitellun materiaalin rahtina kuljettamiseen sovelletaan turvallisuusjärjestelyjä määriteltäessä seuraavia periaatteita:

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

b) lähetyksen suojan taso on määriteltävä sen sisältämän materiaalin korkeimman turvallisuusluokan mukaan;

c) lähettäjän on ennen CONFIDENTIEL UE/EU CONFIDENTIAL- tai SECRET UE/EU SECRET -tasolle luokitellun materiaalin kuljettamista yli rajojen laadittava kuljetussuunnitelma, joka kansallisen, nimetyn tai muun toimivaltaisen turvallisuusviranomaisen on hyväksyttävä;

d) kuljetuksen on tapahduttava mahdollisuuksien mukaan suoraan lähtöpaikasta määräpaikkaan, ja se on suoritettava niin nopeasti kuin olosuhteet sallivat;

e) reittien olisi mahdollisuuksien mukaan kuljettava ainoastaan jäsenvaltioiden kautta. Muiden kuin jäsenvaltioiden kautta kulkevia reittejä olisi käytettävä ainoastaan, kun siihen on sekä lähettäjän että vastaanottajan valtion kansallisen, nimetyn tai muun toimivaltaisen turvallisuusviranomaisen lupa.

*49 artikla*

**EU:n turvallisuusluokiteltujen tietojen siirto kolmansissa valtioissa sijaitseville toimeksisaajille tai avunsaajille**

Siirrettäessä EU:n turvallisuusluokiteltuja tietoja kolmansissa valtioissa sijaitseville toimeksisaajille tai avunsaajille on noudatettava komission turvallisuusviranomaisen, hankintaviranomaisena tai avustuksen myöntävänä viranomaisena toimivan komission osaston sekä sen kolmannen maan, johon toimeksisaaja tai avunsaaja on rekisteröity, kansallisen, nimetyn tai muun toimivaltaisen turvallisuusviranomaisen kesken sovittuja turvatoimia.

*50 artikla*

**RESTREINT UE/EU RESTRICTED -tasolle luokiteltujen tietojen käsittely turvallisuusluokiteltujen hanke- tai avustussopimusten yhteydessä**

1. Turvallisuusluokiteltujen hankinta- tai avustussopimusten nojalla käsiteltävien, RESTREINT UE/EU RESTRICTED -luokkaan kuuluvien tietojen suojaamisen on perustuttava suhteellisuusperiaatteeseen ja kustannustehokkuuden periaatteeseen.

2. Sellaisten turvallisuusluokiteltujen hankinta- tai avustussopimusten yhteydessä, joihin liittyy RESTREINT UE/EU RESTRICTED -luokkaan kuuluvien tietojen käsittelyä, ei edellytetä yhteisö- eikä henkilöturvallisuusselvitystä.

3. Jos hankinta- tai avustussopimukseen kuuluu RESTREINT UE/EU RESTRICTED -luokkaan kuuluvien tietojen käsittelyä toimeksisaajan tai avunsaajan operoimassa viestintä- ja tietojärjestelmässä, hankintaviranomainen tai avustuksen myöntävä viranomainen varmistaa komission turvallisuusviranomaista kuultuaan, että hankinta- tai avustussopimuksessa määrätään viestintä- ja tietojärjestelmän hyväksymistä koskevista tarvittavista teknisistä ja hallinnollisista vaatimuksista, jotka on suhteutettu arvioituun riskiin ja joissa on otettu huomioon kaikki asiaankuuluvat tekijät. Tällaisen viestintä- ja tietojärjestelmän hyväksymisen laajuudesta on sovittava komission turvallisuusviranomaisen ja asianomaisen kansallisen tai nimetyn turvallisuusviranomaisen kesken.

7 LUKU

**TURVALLISUUSLUOKITELTUJEN TIETOJEN VAIHTO MUIDEN UNIONIN TOIMIELINTEN, ELINTEN JA LAITOSTEN, JÄSENVALTIOIDEN, KOLMANSIEN VALTIOIDEN JA KANSAINVÄLISTEN JÄRJESTÖJEN KANSSA**

*51 artikla*

**Perusperiaatteet**

1. Jos komissio tai jokin sen osasto katsoo, että EU:n turvallisuusluokiteltuja tietoja on tarpeen vaihtaa toisen unionin toimielimen, elimen tai laitoksen taikka kolmannen valtion tai kansainvälisen järjestön kanssa, se ryhtyy tarvittaviin toimiin luodakseen asianmukaisen oikeudellisen tai hallinnollisen kehyksen, johon voi kuulua myös asiaankuuluvien määräysten mukaisesti tehtyjä tietoturvasopimuksia tai hallinnollisia järjestelyjä.

2. EU:n turvallisuusluokiteltuja tietoja voidaan vaihtaa toisen unionin toimielimen, elimen tai laitoksen taikka kolmannen valtion tai kansainvälisen järjestön kanssa vain, jos asianmukainen oikeudellinen tai hallinnollinen kehys on luotu ja on olemassa riittävät takeet siitä, että asianomainen unionin toimielin, elin tai laitos taikka kolmas valtio tai kansainvälinen järjestö soveltaa turvallisuusluokiteltujen tietojen suojaamiseen samantasoisia perusperiaatteita ja vähimmäisvaatimuksia, sanotun kuitenkaan rajoittamatta 57 artiklan soveltamista.

*52 artikla*

**EU:n turvallisuusluokiteltujen tietojen vaihto muiden unionin toimielinten, elinten ja laitosten kanssa**

1. Ennen kuin komissio sopii EU:n turvallisuusluokiteltujen tietojen vaihdossa käytettävästä hallinnollisesta järjestelystä toisen unionin toimielimen, elimen tai laitoksen kanssa, se hankkii vahvistuksen sille, että asianomainen unionin toimielin, elin tai laitos

a) soveltaa EU:n turvallisuusluokiteltujen tietojen suojaamiseen sääntelykehystä, jossa määrätään vastaavista perusperiaatteista ja vähimmäisvaatimuksista kuin tässä päätöksessä ja sen soveltamissäännöissä;

b) soveltaa henkilöstöturvallisuutta, fyysistä turvallisuutta, EU:n turvallisuusluokiteltujen tietojen hallinnointia ja viestintä- ja tietojärjestelmien turvallisuutta koskevia turvallisuusvaatimuksia ja -ohjeita, joilla taataan vastaava EU:n turvallisuusluokiteltujen tietojen suojan taso kuin komissiossa;

c) merkitsee tuottamansa turvallisuusluokitellut tiedot EU:n turvallisuusluokitelluiksi tiedoiksi.

2. Henkilöstöhallinnon ja turvallisuustoiminnan pääosasto toimii komission vastuuyksikkönä tiiviissä yhteistyössä muiden toimivaltaisten komission osastojen kanssa, kun muiden unionin toimielinten, elinten tai laitosten kanssa sovitaan EU:n turvallisuusluokiteltujen tietojen vaihtoa koskevista hallinnollisista järjestelyistä.

3. Hallinnollisista järjestelyistä sovitaan yleensä kirjeenvaihdolla; kirjeet allekirjoittaa komission puolesta henkilöstöhallinnon ja turvallisuustoiminnan pääjohtaja.

4. Ennen EU:n turvallisuusluokiteltujen tietojen vaihtoa koskevasta hallinnollisesta järjestelystä sopimista komission turvallisuusviranomainen tekee arviointikäynnin, jonka tarkoituksena on arvioida EU:n turvallisuusluokiteltujen tietojen suojaamiseen sovellettava sääntelykehys ja varmistua suojatoimien tehokkuudesta. Hallinnollinen järjestely tulee voimaan ja EU:n turvallisuusluokiteltuja tietoja vaihdetaan vain, jos arviointikäynnin tulos on tyydyttävä ja sen johdosta annettuja suosituksia on noudatettu. Säännöllisiä seurantakäyntejä on tehtävä sen varmistamiseksi, että hallinnollista järjestelyä noudatetaan ja että käytössä olevat turvatoimet ovat edelleen sovittujen perusperiaatteiden ja vähimmäisvaatimusten mukaisia.

5. Pääsihteeristön hallinnoima EU:n turvallisuusluokiteltujen tietojen rekisteri toimii pääsääntöisesti unionin muiden toimielinten, elinten ja laitosten kanssa vaihdettavien turvallisuusluokiteltujen tietojen saapumis- ja lähtöpaikkana komissiossa. Komission osastoihin perustetut EU:n turvallisuusluokiteltujen tietojen paikallisrekisterit toimivat tämän päätöksen ja sen soveltamissääntöjen mukaisesti turvallisuusluokiteltujen tietojen saapumis- ja lähtöpaikkana asioissa, jotka kuuluvat asianomaisten osastojen toimivaltaan, siinä tapauksessa, että se on EU:n turvallisuusluokiteltujen tietojen suojaamisen kannalta ja turvallisuuteen, organisaatioon tai toimintaan liittyvistä syistä tarkoituksenmukaisempaa.

6. Komission turvallisuusasiantuntijaryhmälle on tiedotettava 2 kohdan mukaisesta hallinnollisten järjestelyjen sopimisprosessista.

*53 artikla*

**EU:n turvallisuusluokiteltujen tietojen vaihto jäsenvaltioiden kanssa**

1. EU:n turvallisuusluokiteltuja tietoja voidaan vaihtaa jäsenvaltioiden kanssa ja luovuttaa niille edellyttäen, että ne suojaavat tiedot sellaisiin turvallisuusluokiteltuihin tietoihin sovellettavien vaatimusten mukaisesti, joilla on samantasoinen kansallinen turvallisuusluokka liitteeseen I sisältyvän turvallisuusluokkien vastaavuustaulukon mukaisesti.

2. Jäsenvaltioiden tuodessa Euroopan unionin rakenteisiin tai verkostoihin turvallisuusluokiteltuja tietoja, joissa on kansallinen turvallisuusluokitusmerkintä, komissio noudattaa kyseisten tietojen suojaamisessa vastaavantasoisiin EU:n turvallisuusluokiteltuihin tietoihin sovellettavia vaatimuksia liitteeseen I sisältyvän turvallisuusluokkien vastaavuustaulukon mukaisesti.

*54 artikla*

**EU:n turvallisuusluokiteltujen tietojen vaihto kolmansien valtioiden ja kansainvälisten järjestöjen kanssa**

1. Jos komissio katsoo, että sillä on pitkäkestoinen tarve vaihtaa turvallisuusluokiteltuja tietoja kolmansien valtioiden tai kansainvälisten järjestöjen kanssa, se ryhtyy tarvittaviin toimiin luodakseen asianmukaisen oikeudellisen tai hallinnollisen kehyksen, johon voi kuulua myös asiaankuuluvien määräysten mukaisesti tehtyjä tietoturvasopimuksia tai hallinnollisia järjestelyjä.

2. Edellä 1 kohdassa tarkoitettuihin tietoturvasopimuksiin ja hallinnollisiin järjestelyihin on sisällytettävä määräyksiä sen varmistamiseksi, että kolmansien valtioiden tai kansainvälisten järjestöjen vastaanottaessa EU:n turvallisuusluokiteltuja tietoja kyseiset tiedot suojataan niiden turvallisuusluokan edellyttämällä ja tässä päätöksessä vahvistettuja vähimmäisvaatimuksia vastaavien vaatimusten mukaisesti.

3. Komissio voi 56 artiklan mukaisesti sopia hallinnollisista järjestelyistä, kun EU:n turvallisuusluokiteltujen tietojen turvallisuusluokka on pääsääntöisesti korkeintaan RESTREINT UE/EU RESTRICTED.

4. Edellä 3 kohdassa tarkoitettuihin turvallisuusluokiteltujen tietojen vaihtoa koskeviin hallinnollisiin järjestelyihin on sisällyttävä määräyksiä sen varmistamiseksi, että kolmansien valtioiden tai kansainvälisten järjestöjen vastaanottaessa EU:n turvallisuusluokiteltuja tietoja kyseiset tiedot suojataan niiden turvallisuusluokan edellyttämällä tasolla ja tässä päätöksessä vahvistettuja vähimmäisvaatimuksia vastaavien vaatimusten mukaisesti. Komission turvallisuusasiantuntijaryhmää on kuultava ennen tietoturvasopimusten tekemistä tai hallinnollisista järjestelyistä sopimista.

5. Komission osasto tekee EU:n turvallisuusluokiteltujen tietojen luovuttajana päätöksen kyseisten komissiosta peräisin olevien tietojen luovuttamisesta kolmannelle valtiolle tai kansainväliselle järjestölle tapauskohtaisesti tietojen luonteen ja sisällön, vastaanottajan tiedonsaantitarpeen ja unionille koituvan edun arvioinnin perusteella. Jos komissio ei ole luovutuspyynnön kohteena olevien turvallisuusluokiteltujen tietojen tai niiden mahdollisesti sisältämän lähdeaineiston luovuttaja, komission osasto, jonka hallussa kyseiset tiedot ovat, pyytää ensin luovuttajalta kirjallisen suostumuksen tietojen luovuttamiselle. Jos luovuttaja ei ole tiedossa, komission osasto, jonka hallussa turvallisuusluokitellut tiedot ovat, ottaa luovuttajalle kuuluvan vastuun komission turvallisuusasiantuntijaryhmää kuultuaan.

*55 artikla*

**Tietoturvasopimukset**

1. Tietoturvasopimukset kolmansien valtioiden tai kansainvälisten järjestöjen kanssa on tehtävä Euroopan unionin toiminnasta tehdyn sopimuksen 218 artiklan mukaisesti.

2. Tietoturvasopimuksissa on määrättävä

a) perusperiaatteista ja vähimmäisvaatimuksista, joita sovelletaan turvallisuusluokiteltujen tietojen vaihtoon unionin ja kolmannen valtion tai kansainvälisen järjestön välillä;

b) teknisistä täytäntöönpanojärjestelyistä, joista sovitaan asianomaisten unionin toimielinten ja elinten toimivaltaisten turvallisuusviranomaisten sekä kyseisen kolmannen valtion tai kansainvälisen järjestön toimivaltaisen turvallisuusviranomaisen kesken. Tällaisissa järjestelyissä on otettava huomioon asianomaisessa kolmannessa valtiossa tai kansainvälisessä järjestössä sovellettavien turvallisuusmääräysten, -rakenteiden ja -menettelyjen tarjoaman suojan taso;

c) siitä, että ennen sopimuksen mukaista turvallisuusluokiteltujen tietojen vaihtoa varmistetaan, että vastaanottava osapuoli pystyy suojaamaan sille annettavat turvallisuusluokitellut tiedot asianmukaisella tavalla.

3. Jos tarve vaihtaa turvallisuusluokiteltuja tietoja on todettu 51 artiklan 1 kohdan mukaisesti, komissio kuulee tarvittaessa Euroopan ulkosuhdehallintoa, neuvoston pääsihteeristöä sekä muita unionin toimielimiä ja elimiä sen määrittämiseksi, olisiko annettava Euroopan unionin toiminnasta tehdyn sopimuksen 218 artiklan 3 kohdan mukainen suositus.

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

5. Pääsihteeristön hallinnoima EU:n turvallisuusluokiteltujen tietojen rekisteri toimii pääsääntöisesti kolmansien valtioiden ja kansainvälisten järjestöjen kanssa vaihdettavien turvallisuusluokiteltujen tietojen saapumis- ja lähtöpaikkana komissiossa. Komission osastoihin perustetut EU:n turvallisuusluokiteltujen tietojen paikallisrekisterit toimivat tämän päätöksen ja sen soveltamissääntöjen mukaisesti turvallisuusluokiteltujen tietojen saapumis- ja lähtöpaikkana asioissa, jotka kuuluvat asianomaisten komission osastojen toimivaltaan, siinä tapauksessa, että se on EU:n turvallisuusluokiteltujen tietojen suojaamisen kannalta ja turvallisuuteen, organisaatioon tai toimintaan liittyvistä syistä tarkoituksenmukaisempaa.

6. Asianomaisen kolmannen valtion tai kansainvälisen järjestön turvallisuusmääräysten, -rakenteiden ja -menettelyjen tehokkuuden arvioimiseksi tehdään arviointikäyntejä, joihin komissio osallistuu yhdessä muiden unionin toimielinten, elinten tai laitosten kanssa ja joista on sovittava asianomaisen kolmannen valtion tai kansainvälisen järjestön kanssa. Arviointikäynneillä arvioidaan

a) turvallisuusluokiteltujen tietojen suojaamiseen sovellettavaa sääntelykehystä;

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

c) käytössä olevia turvatoimia ja turvallisuusmenettelyjä; ja

d) luovutettavien EU:n turvallisuusluokiteltujen tietojen turvallisuusluokkaan sovellettavia turvallisuusselvitysmenettelyjä.

*56 artikla*

**Hallinnolliset järjestelyt**

1. Jos unionin poliittisen tai oikeudellisen kehyksen puitteissa on olemassa pitkäkestoinen tarve vaihtaa kolmannen valtion tai kansainvälisen järjestön kanssa tietoja, joiden turvallisuusluokka on pääsääntöisesti korkeintaan RESTREINT UE/EU RESTRICTED, ja varsinkin jos komission turvallisuusviranomainen on komission turvallisuusasiantuntijaryhmää kuultuaan katsonut, ettei kyseisen osapuolen turvallisuusjärjestelmä ole riittävän kehittynyt tietoturvallisuussopimuksen tekemiseksi, komissio voi sopia hallinnollisesta järjestelystä kyseisen kolmannen valtion viranomaisten tai kansainvälisen järjestön kanssa.

2. Hallinnollisista järjestelyistä sovitaan yleensä kirjeenvaihtona.

3. Ennen järjestelystä sopimista on tehtävä arviointikäynti. Komission turvallisuusasiantuntijaryhmälle on tiedotettava arviointikäynnin tuloksesta. EU:n turvallisuusluokiteltuja tietoja saa luovuttaa, jos niiden kiireelliseen vaihtoon on poikkeuksellisia syitä, edellyttäen, että arviointikäynti pyritään järjestämään mahdollisimman pian.

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

*57 artikla*

**EU:n turvallisuusluokiteltujen tietojen poikkeuksellinen luovuttaminen tapauskohtaisesti**

1. Jos tietoturvasopimusta ei ole tehty eikä hallinnollisesta järjestelystä sovittu ja komissio tai jokin sen osasto katsoo, että unionin poliittisen tai oikeudellisen kehyksen puitteissa on poikkeuksellinen tarve luovuttaa EU:n turvallisuusluokiteltuja tietoja kolmannelle valtiolle tai kansainväliselle järjestölle, komission turvallisuusviranomainen varmistaa mahdollisuuksien mukaan kyseisen kolmannen valtion tai kansainvälisen järjestön turvallisuusviranomaisilta, että sen turvallisuusmääräykset, -rakenteet ja -menettelyt ovat sellaiset, että sille luovutettuja EU:n turvallisuusluokiteltuja tietoja suojataan vähintään yhtä tiukkojen vaatimusten mukaisesti kuin joista säädetään tässä päätöksessä.

2. Komissio tekee komission turvallisuusasiantuntijaryhmää kuultuaan päätöksen EU:n turvallisuusluokiteltujen tietojen luovuttamisesta asianomaiselle kolmannelle valtioille tai kansainväliselle järjestölle turvallisuusasioista vastaavan komission jäsenen ehdotuksen pohjalta.

3. Sen jälkeen, kun komissio on tehnyt päätöksen EU:n turvallisuusluokiteltujen tietojen luovuttamisesta ja luovuttajalta, myös tietojen mahdollisesti sisältämän lähdeaineiston luovuttajalta, on saatu kirjallinen ennakkosuostumus, toimivaltainen komission osasto toimittaa asianomaiset tiedot, joissa on oltava luovutettavuutta koskeva merkintä ja maininta kolmannesta valtiosta tai kansainvälisestä järjestöstä, jolle tiedot 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.

8 LUKU

**LOPPUSÄÄNNÖKSET**

*58 artikla*

**Aiemman päätöksen korvaaminen**

Tällä päätöksellä kumotaan ja korvataan komission päätös 2001/844/EY, EHTY, Euratom ([1]).

*59 artikla*

**Ennen tämän päätöksen voimaantuloa tuotetut turvallisuusluokitellut tiedot**

1. Kaikki päätöksen 2001/844/EY, EHTY, Euratom mukaisesti luokitellut EU:n turvallisuusluokitellut tiedot suojataan edelleen tämän päätöksen säännösten mukaisesti.

2. Kaikki komission hallussa päivänä, jona päätös 2001/844/EY, EHTY, Euratom tuli voimaan, olleet turvallisuusluokitellut tiedot Euratomin turvallisuusluokiteltuja tietoja lukuun ottamatta

a) katsotaan edelleen, jos ne on tuotettu komissiossa, luokitellun automaattisesti uudelleen RESTRAINT EU -tasolle, paitsi jos niiden kirjoittaja oli 31 päivään tammikuuta 2002 mennessä päättänyt antaa niille eri luokituksen ja oli ilmoittanut asiasta kaikille asianomaisen asiakirjan vastaanottajille;

b) säilyttävät, jos ne on tuotettu komission ulkopuolella, alkuperäisen turvallisuusluokkansa, eli niitä pidetään samantasoisina EU:n turvallisuusluokiteltuina tietoina, paitsi jos kirjoittaja suostuu niiden turvallisuusluokan poistamiseen tai alentamiseen.

*60 artikla*

**Soveltamissäännöt ja turvallisuusohjeet**

1. Tämän päätöksen soveltamissääntöjen hyväksyntä voi edellyttää erillistä valtuutuspäätöstä, jonka komissio antaa turvallisuusasioista vastaavalle komission jäsenelle sisäisiä menettelysääntöjä täysimääräisesti noudattaen.

2. Turvallisuusasioista vastaava komission jäsen voi edellä mainitulla komission päätöksellä valtuutuksen saatuaan laatia turvallisuusohjeita, joissa esitetään turvallisuutta koskevat suuntaviivat ja parhaat käytännöt tämän päätöksen ja sen soveltamissääntöjen soveltamisalalla.

3. Komissio voi siirtää tämän artiklan 1 ja 2 kohdassa mainitut tehtävät erillisellä päätöksellä henkilöstöhallinnon ja turvallisuustoiminnan pääjohtajalle sisäisiä menettelysääntöjä täysimääräisesti noudattaen.

*61 artikla*

**Voimaantulo**

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

Tehty Brysselissä 13 päivänä maaliskuuta 2015.

*Komission puolesta*

*Puheenjohtaja*

Jean-Claude JUNCKER

([1]) Komission päätös 2001/844/EY, EHTY, Euratom, tehty 29 päivänä marraskuuta 2001, komission sisäisten menettelysääntöjen muuttamisesta (EYVL L 317, 3.12.2001, s. 1).

*LIITE I*

**TURVALLISUUSLUOKKIEN VASTAAVUUS**

| EU | TRES SECRET UE/EU TOP SECRET | SECRET UE/EU SECRET | CONFIDENTIEL UE/EU CONFIDENTIAL | RESTREINT UE/EU RESTRICTED |
|---|---|---|---|---|
| Euratom | EURA TOP SECRET | EURA SECRET | EURA CONFIDENTIAL | EURA RESTRICTED |
| Belgia | Très Secret (Loi 11.12.1998)<br>Zeer Geheim (Wet 11.12.1998) | Très Secret (Loi 11.12.1998)<br>Zeer Geheim (Wet 11.12.1998) | Très Secret (Loi 11.12.1998)<br>Zeer Geheim (Wet 11.12.1998) | ks. alaviite (1) |
| 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<br>(ΑΑΠ) | Απόρρητο<br>(ΑΠ) | Εμπιστευτικό<br>(ΕΜ) | Περιορισμένης Χρήσης<br>(ΠΧ) |
| Espanja | Secreto | Reservado | Confidencial | Difusión Limitada |
| Ranska | Très Secret Défense | Secret Défense | Confidentiel Défense | ks. alaviite (3) |
| Kroatia | VRLO TAJNO | TAJNO | POVJERLJIVO | OGRANIČENO |
| Italia | Segretissimo | Segreto | Riservatissimo | Riservato |
| Kypros | Άκρως Απόρρητο<br>(ΑΑΠ) | Απόρρητο<br>(ΑΠ) | Εμπιστευτικό<br>(ΕΜ) | Περιορισμένης Χρήσης<br>(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-Għola 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 |

| EU | TRES SECRET UE/EU TOP SECRET | SECRET UE/EU SECRET | CONFIDENTIEL UE/EU CONFIDENTIAL | RESTREINT UE/EU RESTRICTED |
|---|---|---|---|---|
| Romania | Strict secret de importanță deosebită | Strict secret | Secret | Secret de serviciu |
| Slovenia | Strogo tajno | Tajno | Zaupno | Interno |
| Slovakia | Prísne tajné | Tajné | Dôverné | Vyhradené |
| Suomi | ERITTÄIN SALAINEN<br>YTTERST HEMLIG | SALAINEN<br>HEMLIG | LUOTTAMUKSELLINEN<br>KONFIDENTIELL | KÄYTTÖ RAJOITETTU<br>BEGRÄNSAD TILLGÅNG |
| Ruotsi ([4]) | HEMLIG/TOP SECRET<br>HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET | HEMLIG/SECRET<br>HEMLIG | HEMLIG/CONFIDENTIAL<br>HEMLIG | HEMLIG/RESTRICTED<br>HEMLIG |
| Yhdistynyt kuningaskunta | UK TOP SECRET | UK SECRET | ei ole ([5]) | UK OFFICIAL – SENSITIVE |

([1]) ”Diffusion Restreinte”/”Beperkte Verspreiding” ei ole turvallisuusluokka Belgiassa. 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, alemmalla rivillä olevia muut viranomaiset.

([5]) Yhdistynyt kuningaskunta käsittelee ja suojaa EU:n turvallisuusluokan ”CONFIDENTIEL UE/EU CONFIDENTIAL” tietoja ”UK SECRET” -turvallisuusluokkaan sovellettavien vaatimusten mukaisesti.

*LIITE II*

**LYHENNELUETTELO**

| Lyhenne | Merkitys |
|---|---|
| CA | Salausasioista vastaava viranomainen (Crypto Authority) |
| CAA | Salauslaitteiden hyväksyntäviranomainen (Crypto Approval Authority) |
| CCTV | Kameravalvonta (Closed Circuit Television) |
| CDA | Salatun aineiston jakelusta vastaava viranomainen (Crypto Distribution Authority) |
| CIS | EU:n turvallisuusluokiteltuja tietoja käsittelevät viestintä- ja tietojärjestelmät (Communication and Information Systems handling EUCI) |
| DSA | Nimetty turvallisuusviranomainen (Designated Security Authority) |
| EUCI | EU:n turvallisuusluokitellut tiedot (EU Classified Information) |
| FSC | Yhteisöturvallisuusselvitys (Facility Security Clearance) |
| IA | Turvallisuusohje (Information Assurance) |
| IAA | Tiedonturvaamisviranomainen (Information Assurance Authority) |
| IDS | Tietomurtohälytin (Intrusion Detection System) |
| IT | Tietotekniikka (Information Technology) |
| LSO | Paikallinen turvavastaava (Local Security Officer) |
| NSA | Kansallinen turvallisuusviranomainen (National Security Authority) |
| PSC | Henkilöturvallisuusselvitys (Personnel Security Clearance) |
| PSCC | Henkilöturvallisuusselvitystodistus (Personnel Security Clearance Certificate) |
| PSI | Ohjelman tai hankkeen turvallisuusohjeet (Programme/Project Security Instructions) |
| RCO | Rekisterin valvontavastaava (Registry Control Officer) |
| SAA | Turvallisuusjärjestelyjen hyväksyntäviranomainen (Security Accreditation Authority) |
| SAL | Turvallisuutta koskeva lisälauseke (Security Aspects Letter) |
| SCG | Turvaluokitusohjeet (Security Classification Guide) |
| SecOPs | Turvallisuusmenettely (Security Operating Procedures) |
| TA | TEMPEST-viranomainen (TEMPEST Authority) |
| TFEU | Sopimus Euroopan unionin toiminnasta (Treaty on the Functioning of the EU) |

*LIITE III*

**LUETTELO KANSALLISISTA TURVALLISUUSVIRANOMAISISTA**

BELGIA

Autorité nationale de Sécurité
SPF Affaires étrangères, Commerce extérieur et Coopération au Développement
15 rue des Petits Carmes
BE-1000 Bruxelles
P. (sihteeristö): +32 25014542
Faksi: +32 25014596
Sähköposti: nvo-ans@diplobel.fed.be

BULGARIA

State Commission on Information Security
90 Cherkovna Str.
1505 Sofia
Puhelin: +359 29333600
Faksi: +359 29873750
Sähköposti: dksi@government.bg
Kotisivu: www.dksi.bg

TŠEKKI

Národní bezpečnostní úřad
(National Security Authority)
Na Popelce 2/16
150 06 Praha 56
Puhelin: +420 257283335
Faksi: +420 257283110
Sähköposti: czech.nsa@nbu.cz
Kotisivu: www.nbu.cz

TANSKA

Politiets Efterretningstjeneste
(Danish Security Intelligence Service)
Klausdalsbrovej 1
DK-2860 Søborg
Puhelin: +45 33148888
Faksi: +45 33430190

Forsvarets Efterretningstjeneste
(Danish Defence Intelligence Service)
Kastellet 30
2100 København
Puhelin: +45 33325566
Faksi: +45 33931320

SAKSA

Bundesministerium des Innern
Referat ÖS III 3
Alt-Moabit 101 D
D-11014 Berlin
Puhelin: +49 30186810
Faksi: +49 30186811441
Sähköposti: oesIII3@bmi.bund.de

VIRO

National Security Authority Department
Estonian Ministry of Defence
Sakala 1
EE-15094 Tallinn
Puhelin: +372 7170019, +372 7170117
Faksi: +372 7170213
Sähköposti: nsa@mod.gov.ee

KREIKKA

Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ) Διακλαδική Διεύθυνση Στρατιωτικών Πληροφοριών (ΔΔΣΠ)
Διακλαδική Διεύθυνση Στρατιωτικών Πληροφοριών (ΔΔΣΠ)
Διεύθυνση Ασφαλείας και Αντιπληροφοριών
ΣΤΓ 1020 -Χολαργός (Αθήνα)
Ελλάδα
Puhelin: +30 2106572045 (virka-aikana)
+ 30 2106572009 (virka-aikana)
Faksi: +30 2106536279, +30 2106577612

Hellenic National Defence General Staff (HNDGS)
Military Intelligence Sectoral Directorate
Security Counterintelligence Directorate
GR-STG 1020 Holargos – Athens
Puhelin: +30 2106572045
+ 30 2106572009
Faksi: +30 2106536279, +30 2106577612

ESPANJA

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
ES-28023 Madrid
Puhelin: +34 913725000
Faksi: +34 913725808
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
75700 Paris 07 SP
Puhelin: +33 171758177
Faksi: 33 171758200

KROATIA

Office of the National Security Council
Croatian NSA
Jurjevska 34
10000 Zagreb
Kroatia
Puhelin: +385 14681222
Faksi: +385 14686049
Kotisivu: www.uvns.hr

IRLANTI

National Security Authority
Department of Foreign Affairs
76–78 Harcourt Street
IE-Dublin 2
Puhelin: +353 14780822
Faksi: +353 14082959

ITALIA

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

KYPROS

ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ
ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Υπουργείο Άμυνας
Λεωφόρος Εμμανουήλ Ροΐδη 4
1432 Λευκωσία, Κύπρος
Puhelin: +357 22807569, +357 22807643,
+357 22807764
Faksi: +357 22302351

Ministry of Defence
Minister's Military Staff
National Security Authority (NSA)
4 Emanuel Roidi street
1432 Nicosia
Puhelin: +357 22807569, +357 22807643,
+357 22807764
Faksi: +357 22302351
Sähköposti: cynsa@mod.gov.cy

LATVIA

National Security Authority
Constitution Protection Bureau of the Republic of Latvia
P.O.Box 286
LV-1001 Riga
Puhelin: +371 67025418
Faksi: +371 67025454
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: +370 706 66701, +370 706 66702
Faksi: +370 706 66700
Sähköposti: nsa@vsd.lt

LUXEMBURG

Autorité nationale de Sécurité
Boîte postale 2379
1023 Luxembourg
Puhelin: +352 2478 2210 (keskus)
+ 352 2478 2253 (ohivalinta)
Faksi: +352 24782243

UNKARI

Nemzeti Biztonsági Felügyelet
(National Security Authority of Hungary)
H-1024 Budapest, Szilágyi Erzsébet fasor 11/B
Puhelin: +36 (1) 7952303
Faksi: +36 (1) 7950344

Postiosoite:
H-1357 Budapest, PO Box 2
Sähköposti: nbf@nbf.hu
Kotisivu: www.nbf.hu

MALTA

Ministry for Home Affairs and National Security
P.O. Box 146
MT-Valletta
Puhelin: +356 21249844
Faksi: +356 25695321

ALANKOMAAT

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20010
2500 EA Den Haag
Puhelin: +31 703204400
Faksi: +31 703200733

Ministerie van Defensie
Beveiligingsautoriteit
Postbus 20701
2500 EA Den Haag
Puhelin: +31 703187060
Faksi: +31 703187522

ITÄVALTA

Informationssicherheitskommission
Bundeskanzleramt
Ballhausplatz 2
1014 Wien
Puhelin: +43 1531152594
Faksi: +43 1531152615
Sähköposti: ISK@bka.gv.at

PUOLA

Agencja Bezpieczeństwa Wewnętrznego – ABW
(Internal Security Agency)
Rakowiecka St.
00–993 Warszawa
Puhelin: +48 22, 57 944
Faksi: +48 22, 57 944
Sähköposti: nsa@abw.gov.pl
Kotisivu: www.abw.gov.pl

PORTUGALI

Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Rua da Junqueira, 69
PT-1300-342 Lisboa
Puhelin: +351 213031710
Faksi: +351 213031711

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: +40 212245830
Faksi: +40 212240714
Sähköposti: nsa.romania@nsa.ro
kotisivu: www.orniss.ro

SLOVENIA

Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
1000 Ljubljana
Puhelin: +386 14781390
Faksi: +386 14781399
Sähköposti: gp.uvtp@gov.si

SLOVAKIA

Národný bezpečnostný úrad
(National Security Authority)
Budatínska 30 P.O.
P.O. Box 16
850 07 Bratislava
Puhelin: +421 268692314
Faksi: +421 263824005
Kotisivu: www.nbusr.sk

SUOMI

Kansallinen turvallisuusviranomainen
Ulkoasiainministeriö
PL 453
FI-00023 Hallitus
Puhelin: +358 916055890
Faksi: +358 916055140
Sähköposti: NSA@formin.fi

RUOTSI

Utrikesdepartementet
(Ministry for Foreign Affairs)
SSSB
SE-103 39 Stockholm
Puhelin: +46 84051000
Faksi: +46 87231176
Sähköposti: ud-nsa@foreign.ministry.se

YHDISTYNYT KUNINGASKUNTA

UK National Security Authority
Room 335, 3rd Floor
70 Whitehall
London
SW1A 2AS
Puhelin 1: +44 2072765649
Puhelin 2: +44 2072765497
Faksi: +44 2072765651
Sähköposti: UK-NSA@cabinet-office.x.gsi.gov.uk