II

(Tiedonannot)

EUROOPAN UNIONIN TOIMIELINTEN, ELINTEN, TOIMISTOJEN JA VIRASTOJEN TIEDONANNOT

EUROOPAN PARLAMENTTI

EUROOPAN PARLAMENTIN PUHEMIEHISTÖN PÄÄTÖS,

tehty 15 päivänä huhtikuuta 2013,

luottamuksellisten tietojen käsittelyä Euroopan parlamentissa koskevista säännöistä

(2014/C 96/01)

EUROOPAN PARLAMENTIN PUHEMIEHISTÖ, joka

ottaa huomioon työjärjestyksen 23 artiklan 12 kohdan,

SEKÄ KATSOO SEURAAVAA:

(1) Euroopan parlamentin ja Euroopan komission välisiä suhteita koskevan puitesopimuksen ([1]), joka allekirjoitettiin 20 päivänä lokakuuta 2010, jäljempänä 'puitesopimus', ja Euroopan parlamentin ja neuvoston välisen, neuvoston hallussa olevien, muita kysymyksiä kuin yhteisen ulko- ja turvallisuuspolitiikan alaa koskevien turvallisuusluokiteltujen tietojen toimittamisesta Euroopan parlamentille ja niiden käsittelemisestä Euroopan parlamentissa tehdyn toimielinten välisen sopimuksen ([2]), joka allekirjoitettiin 12 päivänä maaliskuuta 2014, jäljempänä 'toimielinten välinen sopimus', nojalla on tarpeen vahvistaa luottamuksellisten tietojen käsittelyä Euroopan parlamentissa koskevat erityiset säännöt.

(2) Lissabonin sopimuksessa Euroopan parlamentille annetaan uusia tehtäviä, ja Euroopan parlamentin toimintojen kehittämiseksi luottamuksellisuutta edellyttävillä aloilla on tarpeen vahvistaa perusperiaatteet, turvallisuutta koskevat vähimmäisvaatimukset sekä asianmukaiset menettelyt luottamuksellisten, myös turvallisuusluokiteltujen tietojen käsittelemiseksi Euroopan parlamentissa.

(3) Tässä päätöksessä vahvistetuissa säännöissä pyritään varmistamaan yhtäläiset suojavaatimukset ja yhteensopivuus muiden perussopimusten nojalla tai perusteella perustettujen toimielinten, elinten, virastojen ja laitosten taikka jäsenvaltioiden hyväksymien sääntöjen kanssa Euroopan unionin päätöksentekomenettelyn moitteettoman toiminnan varmistamiseksi.

(4) Tämän päätöksen säännösten soveltaminen ei rajoita niiden nykyisten tai tulevien sääntöjen soveltamista, jotka koskevat oikeutta tutustua asiakirjoihin ja jotka on hyväksytty Euroopan unionin toiminnasta tehdyn sopimuksen 15 artiklan mukaisesti.

([1]) EUVL L 304, 20.11.2010, s. 47.
([2]) EUVL C 95, 1.4.2014, s. 1.

(5) Tämän päätöksen säännösten soveltaminen ei rajoita niiden henkilötietojen suojaa koskevien nykyisten tai tulevien sääntöjen soveltamista, jotka on hyväksytty Euroopan unionista tehdyn sopimuksen 16 artiklan mukaisesti.

ON TEHNYT TÄMÄN PÄÄTÖKSEN:

1 artikla

Tavoite

Tällä päätöksellä ohjataan luottamuksellisen tiedon hallinnointia ja käsittelyä Euroopan parlamentissa, mikä kattaa myös tiedon tuottamisen, vastaanottamisen, edelleen toimittamisen ja säilyttämisen siten, että tiedon luottamuksellisuus suojataan asianmukaisesti. Sillä pannaan erityisesti täytäntöön toimielinten välinen sopimus sekä puitesopimus ja erityisesti sen liite II.

2 artikla

Määritelmät

Tässä päätöksessä tarkoitetaan

a) ’tiedolla’ kaikkea suullista ja kirjallista tietoa sen muodosta ja antajasta riippumatta;

b) ’luottamuksellisella tiedolla’ turvallisuusluokiteltua tietoa ja ”muuta luottamuksellista tietoa”, jota ei ole turvallisuusluokiteltu;

c) ’turvallisuusluokitellulla tiedolla’ ’EU:n turvallisuusluokiteltua tietoa’ ja ’vastaavaa turvallisuusluokiteltua tietoa’;

d) ’EU:n turvallisuusluokitellulla tiedolla’ mitä tahansa tietoa ja aineistoa, jonka turvallisuusluokitus on ”TRÈS SECRET UE/EU TOP SECRET”, ”SECRET UE/EU SECRET”, ”CONFIDENTIEL UE/EU CONFIDENTIAL” tai ”RESTREINT UE/EU RESTRICTED” ja jonka luvaton ilmitulo saattaisi vaihtelevassa määrin vahingoittaa unionin tai sen yhden tai useamman jäsenvaltion etuja riippumatta siitä, onko tällainen tieto peräisin perussopimusten nojalla tai perusteella perustetuilta toimielimiltä, elimiltä, virastoilta tai laitoksilta vai ei. Tältä osin

— ”TRÈS SECRET UE/EU TOP SECRET” -luokitusta sovelletaan tietoon ja aineistoon, jonka luvaton ilmitulo saattaisi vahingoittaa poikkeuksellisen vakavasti unionin tai sen yhden tai useamman jäsenvaltion olennaisia etuja,

— ”SECRET UE/EU SECRET” -luokitusta sovelletaan tietoon ja aineistoon, jonka luvaton ilmitulo saattaisi vahingoittaa vakavasti Euroopan unionin tai sen yhden tai useamman jäsenvaltion olennaisia etuja,

— ”CONFIDENTIEL UE/EU CONFIDENTIAL” -luokitusta sovelletaan tietoon ja aineistoon, jonka luvaton ilmitulo saattaisi vahingoittaa Euroopan unionin tai sen yhden tai useamman jäsenvaltion olennaisia etuja,

— ”RESTREINT UE/EU RESTRICTED” -luokitusta sovelletaan tietoon ja aineistoon, jonka luvaton ilmitulo saattaisi olla epäedullista Euroopan unionin tai sen yhden tai useamman jäsenvaltion etujen kannalta;

e) ’vastaavalla turvallisuusluokitellulla tiedolla’ jäsenvaltioiden, kolmansien maiden tai kansainvälisten järjestöjen toimittamaa tietoa, jolla on jotakin EU:n turvallisuusluokiteltujen tietojen turvallisuusluokitusmerkintää vastaava turvallisuusluokitusmerkintä ja jonka neuvosto tai komissio on välittänyt Euroopan parlamentille;

f) ’muulla luottamuksellisella tiedolla’ mitä tahansa muuta luottamuksellista tietoa, jota ei ole turvallisuusluokiteltu, myös tietosuojan tai salassapitovelvollisuuden piiriin kuuluvaa tietoa, jonka Euroopan parlamentti on tuottanut tai jonka muut perussopimusten nojalla tai perusteella perustetut toimielimet, elimet, virastot ja laitokset taikka jäsenvaltiot ovat toimittaneet Euroopan parlamentille;

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

h) ’aineistolla’ mitä tahansa asiakirjaa tai konetta tai laitetta, joka on valmistettu tai jota ollaan valmistamassa;

i) ’tiedonsaantitarpeella’ henkilön tarvetta saada tutustua luottamukselliseen tietoon virallisen toimen tai tehtävän hoitamiseksi;

j) ’valtuutuksella’ Euroopan parlamentin jäsenten tapauksessa puhemiehen päätöstä tai Euroopan parlamentin virkamiesten ja muiden poliittisten ryhmien palveluksessa olevien Euroopan parlamentin työntekijöiden tapauksessa pääsihteerin päätöstä myöntää yksittäiselle henkilölle oikeus tutustua turvallisuusluokiteltuun tietoon tiettyyn tasoon saakka kansallisten viranomaisten kansallisen lainsäädännön nojalla tekemän luotettavuusselvityksen antaman myönteisen tuloksen perusteella ja liitteessä I olevan 2 osan säännösten mukaisesti;

k) ’turvallisuusluokituksen alentamisella’ salassapitotason alentamisesta johtuvaa turvallisuusluokituksen muuttamista;

l) ’turvallisuusluokituksen poistamisella’ minkä tahansa turvallisuusluokituksen poistamista;

m) ’merkinnällä’ ”muuhun luottamukselliseen tietoon” liitettyä merkkiä, jonka avulla on tarkoitus tunnistaa sen käsittelyä koskevat tietyt ennalta määrätyt ohjeet tai tietyn asiakirjan kattama ala. Se voidaan myös liittää turvallisuusluokiteltuun tietoon sen käsittelyä koskevien lisävaatimusten asettamiseksi;

n) ’merkinnän poistamisella’ minkä tahansa merkinnän poistamista;

o) ’luovuttajalla’ asianmukaisesti valtuutettua luottamuksellisen tiedon antajaa;

p) ’turvallisuusohjeilla’ liitteessä II vahvistettuja täytäntöönpanotoimia;

q) ’käsittelyohjeilla’ Euroopan parlamentin yksiköille annettuja teknisiä ohjeita luottamuksellisten tietojen hallinnoinnista.

3 artikla

Perusperiaatteet ja vähimmäisvaatimukset

1. Kun Euroopan parlamentissa käsitellään luottamuksellisia tietoja, noudatetaan liitteessä I olevassa 1 osassa vahvistettuja perusperiaatteita ja vähimmäisvaatimuksia.

2. Euroopan parlamentti perustaa perusperiaatteiden ja vähimmäisvaatimusten mukaisesti tietoturvan hallintajärjestelmän. Tietoturvan hallintajärjestelmä käsittää turvallisuusohjeet, käsittelyohjeet sekä sovellettavat työjärjestyksen määräykset. Tietoturvan hallintajärjestelmän tarkoituksena on helpottaa Euroopan parlamentin ja sen hallinnon työskentelyä ja varmistaa samalla Euroopan parlamentin käsittelemien luottamuksellisten tietojen suoja tiedon luovuttajan asettamia ja turvallisuusohjeissa vahvistettuja sääntöjä täysimääräisesti noudattaen.

Luottamuksellisen tiedon käsittely Euroopan parlamentin automaattisten viestintä- ja tietojärjestelmien avulla toteutetaan tiedonturvaamisperiaatetta noudattaen turvallisuusohjeen 3 mukaisesti.

3. Euroopan parlamentin jäsen saa ilman luotettavuusselvitystä tutustua turvallisuusluokiteltuihin tietoihin, joiden turvallisuusluokitus on enintään RESTREINT UE/EU RESTRICTED.

4. Kun asianomaisten tietojen turvallisuusluokitus on CONFIDENTIEL UE/EU CONFIDENTIAL tai vastaava, kyseisiin tietoihin saavat tutustua Euroopan parlamentin jäsenet, jotka ovat saaneet puhemieheltä valtuutuksen 5 kohdan mukaisesti tai jotka ovat allekirjoittaneet juhlallisen vakuutuksen siitä, etteivät he paljasta tällaisten tietojen sisältöä kolmansille osapuolille, että he noudattavat velvoitetta suojata tiedot, joiden turvallisuusluokitus on CONFIDENTIEL UE/EU CONFIDENTIAL ja että he ovat tietoisia laiminlyönnin aiheuttamista seurauksista.

5. Kun asianomaisten tietojen turvallisuusluokitus on SECRET UE/EU SECRET tai TRÈS SECRET/EU TOP SECRET tai vastaava, kyseisiin tietoihin saavat tutustua Euroopan parlamentin jäsenet, joille puhemies on antanut valtuutuksen sen jälkeen, kun:

a) heistä on tehty luotettavuusselvitys tämän päätöksen liitteessä I olevan 2 osan mukaisesti, tai

b) on saatu toimivaltaisen kansallisen viranomaisen ilmoitus siitä, että asianomaisilla Euroopan parlamentin jäsenillä on asianmukainen valtuutus tehtäviensä vuoksi kansallisen lainsäädännön nojalla.

6. Ennen kuin Euroopan parlamentin jäsenet saavat tutustua turvallisuusluokiteltuihin tietoihin, heille on selvitettävä heidän velvollisuutensa suojata tällaiset tiedot liitteen I mukaisesti ja heidän on hyväksyttämä nämä velvollisuutensa. Heille on lisäksi selvitettävä, miten tämä suojaaminen varmistetaan.

7. Euroopan parlamentin virkamies tai muu poliittisen ryhmän palveluksessa oleva parlamentin työntekijä saa tutustua luottamuksellisiin tietoihin, jos hänen ”tiedonsaantitarpeensa” on vahvistettu, sekä turvallisuusluokiteltuihin tietoihin, joiden turvallisuusluokitus on korkeampi kuin RESTREINT UE/EU RESTRICTED, jos hänelle on tehty tasoltaan asianmukainen luotettavuusselvitys. Pääsy turvallisuusluokiteltuihin tietoihin myönnetään vain, jos henkilöille on selvitetty ja annettu kirjalliset ohjeet heidän tällaisten tietojen suojaamista koskevista velvollisuuksistaan sekä siitä, miten tämä suojaaminen varmistetaan, ja he ovat allekirjoittaneet vakuutuksen siitä, että he ovat saaneet kyseiset ohjeet ja sitoutuvat noudattamaan niitä voimassa olevien sääntöjen mukaisesti.

4 artikla

Luottamuksellisten tietojen tuottaminen ja hallinnollinen käsittely Euroopan parlamentissa

1. Euroopan parlamentin puhemies, asiasta vastaavien parlamentin valiokuntien puheenjohtajat ja pääsihteeri tai kuka tahansa pääsihteerin asianmukaisesti kirjallisesti valtuuttama henkilö voi luovuttaa luottamuksellista tietoa ja/tai turvallisuusluokitella tietoa turvallisuusohjeissa vahvistetulla tavalla.

2. Turvallisuusluokiteltua tietoa tuottaessaan luovuttajan on sovellettava asianmukaista turvallisuusluokitustasoa kansainvälisten standardien ja liitteessä I vahvistettujen määritelmien mukaisesti. Luovuttaja määrittää yleensä myös tiedon vastaanottajat, joilla on valtuutus tutustua turvallisuusluokitusta vastaavaan tietoon. Tämä tieto annetaan turvallisuusluokiteltujen tietojen yksikölle, kun asiakirja luovutetaan kyseiselle yksikölle.

3. Muuta luottamuksellista tietoa käsitellään liitteen I ja II sekä käsittelyohjeiden mukaisesti.

5 artikla

Luottamuksellisten tietojen vastaanottaminen Euroopan parlamenttiin

1. Euroopan parlamentin vastaanottama luottamuksellinen tieto annetaan tiedoksi seuraavasti:

a) tietoja koskevan pyynnön esittäneen parlamentin elimen/parlamentin elimessä toimivan jäsenen sihteeristölle tai suoraan turvallisuusluokiteltujen tietojen yksikölle, kun on kyse tiedosta, jonka turvallisuusluokitus on RESTREINT UE/EU RESTRICTED tai vastaava, ja muusta luottamuksellisesta tiedosta,

b) turvallisuusluokiteltujen tietojen yksikölle, kun on kyse tiedosta, jonka turvallisuusluokitus on CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET tai TRÈS SECRET UE/EU TOP SECRET tai vastaava.

2. Luottamuksellisen tiedon kirjaamisen, säilyttämisen ja jäljitettävyyden varmistaa tilanteen mukaan joko tiedon vastaanottaneen parlamentin elimen/parlamentin elimessä toimivan jäsenen sihteeristö tai turvallisuusluokiteltujen tietojen yksikkö.

3. Yhteisesti sovittavat järjestelyt, joiden avulla pyritään säilyttämään tietojen luottamuksellisuus, kun kyse on komission antamista luottamuksellisista tiedoista puitesopimuksen liitteessä II olevan 3.2 kohdan mukaisesti, tai kun kyse on neuvoston toimielinten välisen sopimuksen 5 artiklan 4 kohdan mukaisesti toimittamista turvallisuusluokitelluista tiedoista, luovutetaan yhdessä luottamuksellisen tiedon kanssa tapauksen mukaan parlamentin elimen/parlamentin elimessä toimivan jäsenen sihteeristöön tai turvallisuusluokiteltujen tietojen yksikköön.

4. Tämän artiklan 3 kohdassa tarkoitettuja järjestelyjä voidaan soveltaa soveltuvin osin myös muiden perussopimusten nojalla tai perusteella perustettujen toimielinten, elinten, virastojen tai laitosten taikka jäsenvaltioiden toimittamiin luottamuksellisiin tietoihin.

5. Puheenjohtajakokous perustaa valvonnasta vastaavan komitean, jotta voidaan varmistaa turvallisuusluokitusta TRÈS SECRET UE/EU TOP SECRET tai vastaavaa turvallisuusluokitusta vastaava suojan taso. Tiedot, joiden turvallisuusluokitus on TRÈS SECRET UE/EU TOP SECRET tai vastaava, annetaan Euroopan parlamentille noudattaen lisäjärjestelyjä, joista on sovittava Euroopan parlamentin ja sen unionin toimielimen kesken, jolta tiedot saadaan.

6 artikla

Turvallisuusluokiteltujen tietojen antaminen kolmansille osapuolille Euroopan parlamentista

Euroopan parlamentti voi tapauksen mukaan luovuttajan tai turvallisuusluokitellut tiedot Euroopan parlamentille antaneen unionin toimielimen etukäteen antamalla kirjallisella suostumuksella toimittaa tällaisia turvallisuusluokiteltuja tietoja kolmansille osapuolille edellyttäen, että ne varmistavat, että tällaisten tietojen käsittelyssä niiden yksiköissä ja tiloissa noudatetaan tässä päätöksessä vahvistettuja vastaavia sääntöjä.

7 artikla

Turvalliset tilat

1. Euroopan parlamentti ottaa käyttöön turvallisen alueen ja turvallisia lukusaleja luottamuksellisten tietojen hallinnointia varten.

2. Turvallisella alueella on välineet turvallisuusluokiteltujen tietojen rekisteröintiä, niihin tutustumista, niiden arkistointia, välittämistä ja käsittelyä varten. Alueella on lukusali ja kokoushuone turvallisuusluokiteltuun tietoon tutustumista varten, ja sitä hallinnoi turvallisuusluokiteltujen tietojen yksikkö.

3. Turvallisen alueen ulkopuolella voidaan ottaa käyttöön turvallisia lukusaleja sellaisiin tietoihin tutustumista varten, joiden turvallisuusluokitus on enintään RESTREINT UE/EU RESTRICTED tai vastaava, ja muuhun luottamukselliseen tietoon tutustumista varten. Turvallisia lukusaleja hallinnoivat tapauksen mukaan parlamentin elimen/parlamentin elimessä toimivan jäsenen sihteeristön toimivaltaiset yksiköt tai turvallisuusluokiteltujen tietojen yksikkö. Niissä ei saa olla kopiokonetta, puhelinta, telekopiolaitetta, skanneria tai muita asiakirjojen jäljentämiseen tai välittämiseen soveltuvia teknisiä välineitä.

8 artikla

Luottamuksellisten tietojen kirjaaminen, käsittely ja säilyttäminen

1. Sen mukaan, kuka tiedot on vastaanottanut, parlamentin elimen tai parlamentin elimissä toimivan henkilön sihteeristöjen toimivaltaisten yksiköiden tai turvallisuusluokiteltujen tietojen yksikön on kirjattava ja säilytettävä tiedot, joiden turvallisuusluokitus on RESTREINT UE/EU RESTRICTED tai vastaava, tai muut luottamukselliset tiedot.

2. Sellaisten tietojen käsittelyyn, joiden turvallisuusluokitus on RESTREINT EU/EU RESTRICTED tai vastaava, ja muiden luottamuksellisten tietojen käsittelyyn sovelletaan seuraavia sääntöjä:

a) asiakirjat toimitetaan henkilökohtaisesti sihteeristön päällikölle, joka kirjaa ne ja antaa vastaanottotodistuksen;

b) kun kyseisiä asiakirjoja ei käytetä, niitä säilytetään lukitussa paikassa sihteeristön vastuulla;

c) tietoja ei saa missään tapauksessa tallentaa muulle välineelle eikä välittää kenellekään. Tällaisia asiakirjoja voidaan kopioida käyttäen asianmukaisesti hyväksyttyjä välineitä, jotka on määritetty turvallisuusohjeissa;

d) tällaisiin tietoihin voivat tutustua vain luovuttajan tai tiedot Euroopan parlamentille antaneen unionin toimielimen nimeämät henkilöt 4 artiklan 2 kohdan tai 5 artiklan 3, 4 ja 5 kohdan mukaisesti;

e) parlamentin elimen/parlamentin elimessä toimivan jäsenen sihteeristö pitää kirjaa henkilöistä, jotka ovat tutustuneet tietoihin, ja kirjaa ylös tutustumispäivän ja -ajan. Parlamentin elimen tai parlamentin elimissä toimivan jäsenen sihteeristö välittää kirjatut tiedot turvallisuusluokiteltujen tietojen yksikölle samalla, kun tiedot siirretään turvallisuusluokiteltujen tietojen yksikköön.

3. Turvallisuusluokiteltujen tietojen yksikkö kirjaa, käsittelee ja säilyttää tietoja, joiden turvallisuusluokitus on CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET tai TRÈS SECRET UE/EU TOP SECRET tai vastaava, turvallisella alueella noudattaen turvallisuusohjeissa määritettyä erityistä luokituksen tasoa.

4. Jos 1–3 kohdassa annettuja sääntöjä rikotaan, tapauksen mukaan parlamentin elimen/parlamentin elimessä toimivan jäsenen sihteeristön vastaava virkamies tai turvallisuusluokiteltujen tietojen yksikön vastaava virkamies ilmoittaa asiasta pääsihteerille, joka antaa asian puhemiehen käsiteltäväksi, jos kyseessä on Euroopan parlamentin jäsen.

9 artikla

Turvallisten tilojen käyttöoikeus

1. Pääsy turvalliselle alueelle on ainoastaan seuraavilla henkilöillä:

a) henkilöt, joilla on 3 artiklan 4–7 kohdan mukaisesti valtuutus tutustua turvallisella alueella säilytettäviin tietoihin ja jotka ovat esittäneet pyynnön 10 artiklan 1 kohdan mukaisesti;

b) henkilöt, joilla on 4 artiklan 1 kohdan mukaisesti valtuutus tuottaa turvallisuusluokiteltua tietoa ja jotka ovat esittäneet pyynnön 10 artiklan 1 kohdan mukaisesti;

c) turvallisuusluokiteltujen tietojen yksikössä työskentelevät Euroopan parlamentin virkamiehet;

d) viestintä- ja tietojärjestelmien hallinnoinnista vastaavat Euroopan parlamentin virkamiehet;

e) tarvittaessa turvallisuudesta ja paloturvallisuudesta vastaavat Euroopan parlamentin virkamiehet;

f) siivoushenkilöstö, mutta vain turvallisuusluokiteltujen tietojen yksikössä työskentelevän virkamiehen läsnä ollessa ja tarkassa valvonnassa.

2. Turvallisuusluokiteltujen tietojen yksikkö voi evätä turvalliselle alueelle pääsyn kaikilta henkilöiltä, joilla ei ole valtuutusta päästä alueelle. Valitukset tällaisista päätöksistä, joilla evätään pääsy, osoitetaan Euroopan parlamentin jäsenten pääsyä koskevien pyyntöjen tapauksessa puhemiehelle ja muissa tapauksissa pääsihteerille.

3. Pääsihteeri voi antaa luvan siihen, että turvallisella alueella olevassa kokoushuoneessa järjestetään kokous rajatulle määrälle osanottajia.

4. Pääsy turvallisen lukusaliin on ainoastaan seuraavilla henkilöillä:

a) Euroopan parlamentin jäsenet, Euroopan parlamentin virkamiehet ja muut poliittisten ryhmien palveluksessa olevat Euroopan parlamentin työntekijät edellyttäen, että henkilöillä on asianmukainen lupa tutustua luottamukselliseen tietoon tai tuottaa sitä;

b) luottamuksellisten tietojen yksikön hallinnoinnista vastaavat Euroopan parlamentin virkamiehet, tiedot vastaanottaneen parlamentin elimen/parlamentin elimessä toimivan jäsenen sihteeristön virkamiehet sekä turvallisuusluokiteltujen tietojen yksikön virkamiehet;

c) tarvittaessa turvallisuudesta ja paloturvallisuudesta vastaavat Euroopan parlamentin virkamiehet;

d) siivoushenkilöstö, mutta tapauksen mukaan vain parlamentin elimen/parlamentin elimessä toimivan jäsenen sihteeristössä tai turvallisuusluokiteltujen tietojen yksikössä työskentelevän virkamiehen läsnä ollessa ja tämän tarkassa valvonnassa.

5. Parlamentin elimen/parlamentin elimessä toimivan jäsenen asiasta vastaava sihteeristö tai turvallisuusluokiteltujen tietojen yksikkö voivat evätä pääsyn turvalliseen lukusaliin henkilöltä, jolla ei ole sinne pääsyyn oikeuttavaa valtuutusta. Valitukset tällaisista päätöksistä, joilla evätään pääsy, osoitetaan Euroopan parlamentin jäsenten pääsyä koskevien pyyntöjen tapauksessa puhemiehelle ja muissa tapauksissa pääsihteerille.

10 artikla

Luottamuksellisiin tietoihin tutustuminen tai niiden tuottaminen turvallisissa tiloissa

1. Henkilön, joka haluaa tutustua luottamukselliseen tietoon tai tuottaa sitä turvallisella alueella, on ilmoitettava etukäteen nimensä turvallisuusluokiteltujen tietojen yksikölle. Turvallisuusluokiteltujen tietojen yksikkö tarkastaa kyseisen henkilön henkilöllisyyden ja varmentaa, että hänellä on oikeus tutustua luottamuksellisiin tietoihin tai tuottaa niitä 3 artiklan 3–7 kohdassa, 4 artiklan 1 kohdassa tai 5 artiklan 3, 4 ja 5 kohdassa tarkoitettujen järjestelyjen mukaisesti.

2. Henkilön, joka haluaa 3 artiklan 3 ja 7 kohdan mukaisesti tutustua turvallisessa lukusalissa luottamuksellisiin tietoihin, joiden turvallisuusluokitus on RESTREINT EU/EU RESTRICTED tai vastaava, tai muihin luottamuksellisiin tietoihin, on ilmoitettava etukäteen nimensä parlamentin elimen/parlamentin elimessä toimivan jäsenen sihteeristön asiasta vastaaville yksiköille tai turvallisuusluokiteltujen tietojen yksikölle.

3. Poikkeustilanteita lukuun ottamatta (esimerkiksi kun lyhyen ajan kuluessa on esitetty paljon tutustumispyyntöjä) ainoastaan yhdellä henkilöllä kerrallaan on valtuutus tutustua luottamukselliseen tietoon turvallisessa tilassa parlamentin elimen/parlamentin elimessä toimivan jäsenen sihteeristön tai turvallisuusluokiteltujen tietojen yksikön virkamiehen läsnä ollessa.

4. Tietoihin tutustumisen aikana yhteydenpito ulkomaailmaan (mukaan lukien puhelimen tai muiden teknisten laitteiden käyttö), muistiinpanojen tekeminen tarkasteltavasta luottamuksellisesta tiedosta ja sen valokopioiminen tai valokuvaaminen on kielletty.

5. Ennen kuin parlamentin elimen/parlamentin elimessä toimivan jäsenen sihteeristön tai turvallisuusluokiteltujen tietojen yksikön virkamies antaa henkilölle luvan poistua turvallisesta tilasta, hän varmistaa, että tarkastellut luottamukselliset tiedot ovat yhä paikallaan, vahingoittumattomat ja täydelliset.

6. Jos edellä esitettyjä sääntöjä rikotaan, tapauksen mukaan parlamentin elimen/parlamentin elimessä toimivan jäsenen sihteeristön tai turvallisuusluokiteltujen tietojen yksikön virkamies ilmoittaa asiasta pääsihteerille, joka antaa asian puhemiehen käsiteltäväksi, jos kyseessä on Euroopan parlamentin jäsen.

11 artikla

Vähimmäisvaatimukset, jotka koskevat luottamuksellisiin tietoihin tutustumista turvallisen alueen ulkopuolella suljetuin ovin pidettävässä kokouksessa

1. Euroopan parlamentin valiokuntien tai muiden Euroopan parlamentin poliittisten ja hallinnollisten elinten jäsenet voivat tutustua tietoihin, joiden turvallisuusluokitus on RESTREINT EU/EU RESTRICTED tai vastaava, ja muihin luottamuksellisiin tietoihin turvallisen alueen ulkopuolella suljetuin ovin pidettävässä kokouksessa.

2. Edellä 1 kohdassa tarkoitetuissa olosuhteissa kokouksesta vastaavan parlamentin elimen/parlamentin elimessä toimivan jäsenen sihteeristö varmistaa, että seuraavia ehtoja noudatetaan:

a) kokoushuoneeseen on pääsy vain henkilöillä, jotka toimivaltaisen valiokunnan tai elimen puheenjohtaja on nimennyt osallistumaan kokoukseen;

b) kaikki asiakirjat numeroidaan ja jaetaan kokouksen alussa ja kerätään takaisin sen päättyessä ja niistä ei tehdä muistiinpanoja eikä oteta valokopioita tai valokuvia;

c) kokouksen pöytäkirjaan ei tehdä mainintoja käsitellyistä tiedoista käydyn keskustelun sisällöstä. Vain asiaa koskeva päätös, jos sellainen tehdään, kirjataan pöytäkirjaan;

d) luottamuksellisiin tietoihin, jotka annetaan suullisesti vastaanottajille Euroopan parlamentissa, sovelletaan vastaavaa suojatasoa kuin kirjallisina annettaviin luottamuksellisiin tietoihin;

e) kokoushuoneisiin ei varastoida mitään muita asiakirjoja;

f) kokouksen alussa osanottajille ja tulkeille jaetaan vain tarvittava määrä asiakirjoja;

g) kokouksen puheenjohtaja ilmoittaa asiakirjojen luokituksen tai merkinnän selvästi kokouksen alussa;

h) osallistujat eivät vie asiakirjoja pois kokoushuoneesta;

i) kokouksen päätyttyä parlamentin elimen/parlamentin elimessä toimivan jäsenen sihteeristö kerää ja laskee kaikki asiakirjojen kopiot; sekä

j) mitään sähköisiä viestintävälineitä tai muita elektronisia laitteita ei tuoda kokoushuoneeseen, jossa asianomaisiin luottamuksellisiin tietoihin tutustutaan tai niitä käsitellään.

3. Jos suljetuin ovin pidettävässä kokouksessa käsitellään puitesopimuksen liitteessä II olevassa 3.2.2 kohdassa ja toimielinten välisen sopimuksen 6 artiklan 5 kohdassa tarkoitettujen poikkeusten mukaisesti tietoja, joiden turvallisuusluokitus on CONFIDENTIEL UE/EU CONFIDENTIAL tai vastaava, kokouksesta vastaavan parlamentin elimen/parlamentin elimessä toimivan jäsenen sihteeristön on sen lisäksi, että se varmistaa, että 2 kohdan säännöksiä noudatetaan, varmistettava myös se, että kokoukseen osallistuviksi nimetyt henkilöt täyttävät 3 artiklan 4 ja 7 kohdan vaatimukset.

4. Edellä 3 kohdassa tarkoitetussa tapauksessa turvallisuusluokiteltujen tietojen yksikkö antaa suljetuin ovin pidettävästä kokouksesta vastaavalle parlamentin elimen/parlamentin elimessä toimivan jäsenen sihteeristölle tarvittavan määrän kopioita kokouksessa käsiteltävistä asiakirjoista, jotka on palautettava turvallisuusluokiteltujen tietojen yksikölle kokouksen jälkeen.

12 artikla

Luottamuksellisten tietojen arkistointi

1. Turvalliselle alueelle järjestetään turvallinen arkistojen säilytyspaikka. Turvallisuusluokiteltujen tietojen yksikkö vastaa turvallisen arkiston hallinnoinnista tavanomaisten arkistointikriteerien mukaisesti.

2. Turvallisuusluokiteltujen tietojen yksikölle luovutetut pitkäaikaisesti säilytettävät luottamukselliset tiedot sekä tiedot, joiden turvallisuusluokitus on RESTREINT EU/EU RESTRICTED tai vastaava ja jotka on siirretty parlamentin elimen/parlamentin elimessä toimivan jäsenen sihteeristölle, siirretään turvallisella alueella sijaitsevaan turvalliseen arkistoon kuuden kuukauden kuluttua siitä, kun niihin viimeksi tutustuttiin, ja viimeistään vuoden kuluttua siitä, kun ne luovutettiin. Asianomaisen parlamentin elimen/parlamentin elimessä toimivan jäsenen sihteeristö arkistoi muut luottamukselliset tiedot asiakirjojen käsittelyä koskevia yleisiä sääntöjä noudattaen, ellei niitä ole siirretty turvallisuusluokiteltujen tietojen yksikköön.

3. Turvallisessa arkistossa säilytettäviin luottamuksellisiin tietoihin tutustuminen on mahdollista seuraavia ehtoja noudattaen:

a) luottamukselliseen tietoon saavat tutustua ainoastaan henkilöt, joiden nimi, toimi tai asema mainitaan tiedon luovuttamisen yhteydessä täytetyssä saateasiakirjassa;

b) luottamukselliseen tietoon tutustumista koskeva pyyntö on esitettävä turvallisuusluokiteltujen tietojen yksikölle, joka siirtää asiakirjan turvallisesta arkistosta turvalliseen lukusaliin; sekä

c) luottamukselliseen tietoon tutustumiseen sovelletaan 10 artiklan mukaisia luottamuksellisiin tietoihin tutustumista koskevia menettelyjä ja ehtoja.

13 artikla

Luottamuksellisten tietojen turvallisuusluokituksen alentaminen ja poistaminen ja merkinnän poistaminen

1. Luottamuksellisen tiedon turvallisuusluokituksen alentaminen tai poistaminen tai merkinnän poistaminen on mahdollista vain tiedon luovuttajan etukäteen antamalla suostumuksella, ja asiasta on tarvittaessa ensin keskusteltava muiden asianosaisten kanssa.

2. Turvallisuusluokituksen alentaminen tai poistaminen vahvistetaan kirjallisesti. Tiedon luovuttajan on ilmoitettava tiedon vastaanottajille muutoksesta, ja näiden on puolestaan ilmoitettava muutoksesta kaikille myöhemmille vastaanottajille, joille he ovat lähettäneet asiakirjan tai sen kopion. Luovuttajat ilmoittavat mahdollisuuksien mukaan turvallisuusluokitellussa asiakirjassa päivämäärän, ajanjakson tai tapahtuman, jonka jälkeen asiakirjan sisällön turvallisuusluokitus voidaan alentaa tai poistaa. Muussa tapauksessa he tarkistavat asiakirjan vähintään joka viides vuosi varmistaakseen, onko alkuperäinen turvallisuusluokitus tarpeen.

3. Turvallisissa arkistoissa säilytettäviä luottamuksellisia tietoja tarkastellaan hyvissä ajoin ja viimeistään 25 vuoden kuluttua niiden tuottamisesta sen määrittämiseksi, pitäisikö tietojen turvallisuusluokitus alentaa tai poistaa tai pitäisikö merkintä poistaa. Tällaisten tietojen tarkastelussa ja julkistamisessa noudatetaan Euroopan talousyhteisön ja Euroopan atomienergiayhteisön historiallisten arkistojen avaamisesta yleisölle 1 päivänä helmikuuta 1983 annetun neuvoston asetuksen (ETY, Euratom) N:o 354/83 ([1]) säännöksiä. Turvallisuusluokituksen poistaa luottamuksellisen tiedon luovuttaja tai asiasta tuolloin vastaava yksikkö liitteessä I olevan 1 osan 10 kohdan mukaisesti.

4. Turvallisuusluokituksen poistamisen jälkeen turvallisessa arkistossa säilytetyt aiemmin turvallisuusluokitellut tiedot siirretään Euroopan parlamentin historiallisiin arkistoihin, jossa niitä säilytetään pysyvästi ja käsitellään edelleen sovellettavien sääntöjen mukaisesti.

5. Merkinnän poiston jälkeen muihin aiemmin luottamuksellisiin tietoihin sovelletaan asiakirjojen käsittelyä koskevia Euroopan parlamentin sääntöjä.

14 artikla

Luottamuksellisten tietojen turvallisuusrikkomukset, katoaminen tai vaarantuminen

1. Yleensä luottamuksellisuuden suojan ja erityisesti tämän päätöksen rikkominen johtaa Euroopan parlamentin jäsenten tapauksessa Euroopan parlamentin työjärjestyksen seuraamuksia koskevien määräysten soveltamiseen.

2. Euroopan parlamentin henkilöstöön kuuluvan henkilön syyllistyessä rikkomiseen sovelletaan asetuksessa (ETY, Euratom, EHTY) N:o 259/68 ([2]) säädetyissä Euroopan unionin virkamiehiin sovellettavissa henkilöstösäännöissä ja Euroopan unionin muuhun henkilöstöön sovellettavissa palvelussuhteen ehdoissa, jäljempänä 'henkilöstösäännöt', vahvistettuja menettelyjä ja seuraamuksia.

([1]) EYVL L 43, 15.2.1983, s. 1.
([2]) EYVL L 56, 4.3.1968, s. 1.

3. Tapauksen mukaan puhemiehen ja/tai pääsihteerin on teetettävä tarvittavat tutkimukset, jos tapahtuu turvallisuusohjeessa 6 määritelty rikkomus.

4. Jos luottamukselliset tiedot on antanut Euroopan parlamentille unionin toimielin tai jäsenvaltio, tapauksen mukaan puhemiehen ja/tai pääsihteerin on ilmoitettava asianomaiselle unionin toimielimelle tai jäsenvaltiolle todistetusta tai epäillystä turvallisuusluokiteltujen tietojen katoamisesta tai vaarantumisesta sekä tutkinnan tuloksista ja toimista, joilla tapauksen uusiutuminen pyritään estämään.

15 artikla

Tämän päätöksen ja sen täytäntöönpanosääntöjen muuttaminen sekä vuosittainen raportointi tämän päätöksen soveltamisesta

1. Pääsihteeri ehdottaa tarvittavia muutoksia tähän päätökseen ja sen täytäntöönpanoa koskeviin liitteisiin ja välittää ehdotukset puhemiehistölle päätöksentekoa varten.

2. Pääsihteeri vastaa tämän päätöksen täytäntöönpanosta Euroopan parlamentin yksiköissä ja antaa tietoturvan hallintajärjestelmän alaisuuteen kuuluvia tapauksia koskevat käsittelyohjeet tässä päätöksessä säädettyjen periaatteiden mukaisesti.

3. Pääsihteeri antaa puhemiehistölle vuosittaisen raportin tämän päätöksen soveltamisesta.

16 artikla

Siirtymä- ja loppusäännökset

1. Turvallisuusluokiteltujen tietojen yksikössä tai jossakin muussa Euroopan parlamentin arkistossa olevat muut kuin turvallisuusluokitellut tiedot, jotka katsotaan luottamuksellisiksi ja jotka on päivätty ennen 1 huhtikuuta 2014, katsotaan tätä päätöstä sovellettaessa muiksi luottamuksellisiksi tiedoiksi. Niiden luovuttaja voi milloin tahansa harkita luottamuksellisuuden tasoa uudelleen.

2. Poiketen tämän päätöksen 5 artiklan 1 kohdasta ja 8 artiklan 1 kohdasta, 12 kuukauden ajan 1 päivänä huhtikuuta 2014 lukien tiedot, jotka neuvosto toimittaa toimielinten välisen sopimuksen mukaisesti ja joiden turvallisuusluokitus on RESTREINT UE/EU RESTRICTED tai vastaava, siirretään turvallisuusluokiteltujen tietojen yksikköön ja kirjataan ja säilytetään siellä. Tällaisiin tietoihin voidaan tutustua toimielinten välisen sopimuksen 4 artiklan 2 kohdan a ja c alakohdan ja 5 artiklan 4 kohdan mukaisesti.

3. Kumotaan puhemiehistön 6 päivänä kesäkuuta 2011 tekemä päätös luottamuksellisten tietojen käsittelystä Euroopan parlamentissa.

17 artikla

Voimaantulo

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

LIITE I

1 osa

TURVALLISUUTTA KOSKEVAT PERUSPERIAATTEET JA VÄHIMMÄISVAATIMUKSET LUOTTAMUKSELLISTEN TIETOJEN SUOJAAMISEKSI

1. **JOHDANTO**

Näillä säännöksillä vahvistetaan turvallisuutta koskevat perusperiaatteet ja vähimmäisvaatimukset luottamuksellisten tietojen suojaamiseksi, joita on noudatettava kaikissa Euroopan parlamentin toimipaikoissa ja joita kaikkien turvallisuusluokitellun tiedon ja muun luottamuksellisen tiedon vastaanottajien on noudatettava, jotta voidaan taata turvallisuus ja olla varmoja siitä, että kaikki asianomaiset henkilöt noudattavat yhtäläisiä suojavaatimuksia. Näitä säännöksiä täydentävät liitteessä II olevat turvallisuusohjeet ja muut säännökset parlamentin valiokuntien, muiden parlamentin elinten ja näissä elimissä toimivien jäsenten suorittamasta luottamuksellisten tietojen käsittelystä.

2. **PERUSPERIAATTEET**

Euroopan parlamentin turvallisuuspolitiikka on olennainen osa parlamentin yleistä sisäistä hallintopolitiikkaa ja pohjautuu näin ollen parlamentin yleisen politiikan periaatteisiin. Näihin periaatteisiin kuuluvat laillisuus, avoimuus, vastuullisuus, toissijaisuus ja suhteellisuus.

Laillisuuteen sisältyy tarve pitäytyä tiukasti oikeudellisessa kehyksessä turvallisuustoimia toteutettaessa ja tarvetta noudattaa sovellettavia oikeudellisia vaatimuksia. Lisäksi turvallisuusalalla vastuun on perustuttava asianmukaisiin oikeudellisiin säännöksiin. Henkilöstösääntöjen säännöksiä sovelletaan kokonaisuudessaan, ja erityisesti henkilöstösääntöjen 17 artiklaa, joka koskee velvollisuutta pidättäytyä tehtäviensä myötä saamiensa tietojen luvattomasta luovuttamisesta, sekä niiden VI osastoa, joka koskee kurinpitomenettelyä, on sovellettava täysimääräisesti. Euroopan parlamentin vastuulle tulevaa turvallisuusrikkomusta on käsiteltävä parlamentin työjärjestyksen mukaisesti ja johdonmukaisesti kurinpitotoimenpiteitä koskevan parlamentin toimintalinjan kanssa.

Avoimuuteen kuuluu se, että kaikkien turvallisuussääntöjen ja säännösten on oltava selkeitä, eri yksiköiden ja alojen on oltava tasapainossa (fyysinen turvallisuus verrattuna tietojen suojaaminen jne.) ja turvallisuustietoisuutta koskevien toimintalinjojen on oltava johdonmukaisia ja jäsennettyjä. Lisäksi turvallisuustoimien toteuttamisesta tarvitaan selkeitä kirjallisia ohjeita.

Vastuullisuus merkitsee, että turvallisuusalan vastuualueet on määriteltävä selkeästi. Lisäksi siihen sisältyy tarve valvoa säännöllisesti, onko vastuu kannettu asianmukaisella tavalla.

Toissijaisuudella tarkoitetaan sitä, että turvallisuudesta on huolehdittava alimmalla mahdollisella tasolla sekä mahdollisimman lähellä Euroopan parlamentin pääosastoja ja parlamentin yksiköitä. Suhteellisuudella tarkoitetaan sitä, että turvallisuustoimet on rajoitettava tiukasti ainoastaan niihin osa-alueisiin, joilla ne ovat ehdottoman välttämättömiä, ja että turvallisuustoimien on oltava oikeassa suhteessa suojattaviin etuihin ja niihin kohdistuviin todellisiin tai mahdollisiin uhkiin siten, että näitä etuja on mahdollista puolustaa vähiten häiritsevällä tavalla.

3. **TIETOJEN TURVAAMISEN PERUSTEET**

Tietojen turvaaminen perustuu seuraaviin seikkoihin:

a) asianmukaiset viestintä- ja tietojärjestelmät. Ne ovat (turvallisuusohjeessa 1 määritetyn) Euroopan parlamentin turvallisuusviranomaisen vastuulla;

b) Euroopan parlamentissa on (turvallisuusohjeessa 1 määritetty) tiedonturvaamisviranomainen, jonka vastuulla on työskennellä turvallisuusviranomaisen kanssa tietojen ja neuvojen antamiseksi viestintä- ja tietojärjestelmien turvallisuutta uhkaavista teknisistä seikoista ja keinoista suojautua näiltä uhilta;

c) Euroopan parlamentin asiasta vastaavat yksiköt ja muiden unionin toimielinten turvallisuusyksiköt tekevät tiivistä yhteistyötä.

4. **TIETOJEN TURVAAMISEN PERIAATTEET**

4.1. ***Tavoitteet***

Päätavoitteet ovat seuraavat:

a) turvallisuusluokitellun tiedon ja muun luottamuksellisen tiedon suojaaminen vakoilulta, vaarantamiselta ja luvattomalta ilmitulolta;

b) tieto- ja tietoliikennejärjestelmissä ja -verkoissa käsiteltävän turvallisuusluokitellun tiedon suojaaminen tietojen luottamuksellisuuteen, eheyteen ja käytettävyyteen liittyviltä uhilta;

c) Euroopan parlamentin toimitilojen, joissa turvallisuusluokiteltua tietoa säilytetään, suojaaminen sabotoinnilta ja tahalliselta vahingoittamiselta;

d) suojaamisen epäonnistuessa vahinkojen arviointi, niiden seurausten rajoittaminen, turvallisuustutkintojen tekeminen ja tarpeellisten korjaavien toimenpiteiden toteuttaminen.

4.2. ***Turvallisuusluokitus***

4.2.1. Luottamuksellisuuden säilyttäminen edellyttää huolellisuutta ja kokemusta valittaessa suojattavaksi tarkoitettua tietoa ja aineistoa ja arvioitaessa sitä, minkä tasoista suojaa ne edellyttävät. On olennaisen tärkeää, että suojauksen taso vastaa suojattavan yksittäisen tiedon tai aineiston arkaluonteisuutta turvallisuuden kannalta. Kitkattoman tiedonkulun varmistamiseksi sekä yli- että aliluokitusta on vältettävä.

4.2.2. Tässä jaksossa esitetyt periaatteet voidaan toteuttaa turvallisuusluokitusjärjestelmällä. Suunniteltaessa ja järjestettäessä toimia vakoilun, sabotoinnin, terrorismin ja muiden uhkien torjumiseksi on noudatettava samanlaista turvallisuusluokitusjärjestelmää, jotta tärkeimpiä tiloja, joissa turvallisuusluokiteltuja tietoja säilytetään, ja näiden tilojen herkimpiä alueita suojeltaisiin tehokkaimmin.

4.2.3. Tiedon luovuttaja vastaa yksin tiedon turvallisuusluokituksesta.

4.2.4. Turvallisuusluokitus perustuu yksinomaan asianomaisten tietojen sisältöön.

4.2.5. Jos tietoja ryhmitellään yhteen, kokonaisuuteen on sovellettava vähintään yhtä korkeaa turvallisuusluokitusta kuin näihin tietoihin sovellettava korkein yksittäinen turvallisuusluokitus. Tietokokonaisuudelle voidaan kuitenkin antaa korkeampi turvallisuusluokitus kuin sen yksittäisille osille.

4.2.6. Turvallisuusluokitus annetaan vain tarvittaessa ja tarvittavan pitkäksi aikaa.

4.3. ***Turvallisuustoimien tavoitteet***

Turvallisuustoimet toteutetaan siten, että

a) ne koskevat kaikkia, joilla on pääsy turvallisuusluokiteltuihin tietoihin, turvallisuusluokiteltuja tietoja sisältäviin tietovälineisiin ja muihin luottamuksellisiin tietoihin sekä kaikkiin toimitiloihin, joissa on tällaisia tietoja, ja tärkeisiin säilytystiloihin;

b) ne suunnitellaan niin, että niiden avulla voidaan yksilöidä henkilöt, joiden aseman (pääsyn, suhteiden tai muiden seikkojen) vuoksi turvallisuusluokiteltujen tietojen ja niiden tärkeiden säilytystilojen turvallisuus voisi vaarantua, ja niissä on oltava säännökset kyseisten henkilöiden vapauttamisesta tehtävistään tai siirtämisestä muihin tehtäviin;

c) niillä estetään luvaton pääsy turvallisuusluokiteltuun tietoon ja tietojen säilytystiloihin;

d) niillä varmistetaan se, että turvallisuusluokiteltua tietoa levitetään ainoastaan tiedonsaantitarpeen periaatteen pohjalta, mikä on olennaista kaikkien turvallisuusnäkökohtien kannalta;

e) niillä varmistetaan kaikkien luottamuksellisten tietojen eheys (estämällä tietojen turmeleminen, luvaton muuttaminen ja luvaton poistaminen) ja käytettävyys (niiden henkilöiden osalta, joilla on tarve tutustua tietoihin ja joilla on tätä koskeva valtuutus) riippumatta siitä, ovatko tiedot turvallisuusluokiteltuja vai eivät; tämä koskee erityisesti sähkömagneettisesti säilytettäviä, käsiteltäviä tai lähetettäviä tietoja.

5. YHTEISET VÄHIMMÄISVAATIMUKSET

Euroopan parlamentti varmistaa, että kaikki sekä toimielimessä toimivat että sen valtuuttamat turvallisuusluokitellun tiedon vastaanottajat eli kaikki sen yksiköt ja toimeksisaajat noudattavat turvallisuutta koskevia yhteisiä vähimmäisvaatimuksia, jotta voidaan luottaa siihen, että tällaista tietoa käsitellään kaikkialla yhtä huolellisesti. Vähimmäisvaatimuksiin kuuluvat arviointiperusteet Euroopan parlamentin virkamiesten ja poliittisten ryhmien palveluksessa olevien muiden parlamentin työntekijöiden luotettavuuden selvittämiseksi ja menettelyt luottamuksellisten tietojen suojaamiseksi.

Euroopan parlamentti antaa kolmansille osapuolille oikeuden tutustua tällaiseen tietoon ainoastaan sillä edellytyksellä, että ne varmistavat, että tietoa käsiteltäessä noudatetaan vähintään näitä yhteisiä vähimmäisvaatimuksia täysin vastaavia säännöksiä.

Tällaisia yhteisiä vähimmäisvaatimuksia sovelletaan myös, kun Euroopan parlamentti antaa yrityksille ja muille yhteisöille hankinta- tai avustussopimuksen nojalla toimeksiantoja, joihin sisältyy luottamuksellisia tietoja.

6. TURVALLISUUS EUROOPAN PARLAMENTIN VIRKAMIESTEN JA POLIITTISTEN RYHMIEN PALVELUKSESSA OLEVIEN MUIDEN PARLAMENTIN TYÖNTEKIJÖIDEN OSALTA

6.1. *Euroopan parlamentin virkamiehille ja poliittisten ryhmien palveluksessa oleville muille parlamentin työntekijöille annettavat turvallisuusohjeet*

Euroopan parlamentin virkamiehille ja poliittisten ryhmien palveluksessa oleville muille parlamentin työntekijöille, jotka on otettu palvelukseen sellaiseen asemaan, jossa he voivat päästä tutustumaan turvallisuusluokiteltuihin tietoihin, on annettava heti heidän aloittaessaan tehtävässään ja säännöllisin väliajoin tarkat ohjeet turvallisuustoimien tarpeellisuudesta ja niihin liittyvistä menettelyistä. Tällaisen henkilöstön on vahvistettava kirjallisesti, että he ovat lukeneet nämä turvallisuussäännökset ja ymmärtävät ne täysin.

6.2. *Johdon velvollisuudet*

Johdon velvollisuus on tietää, ketkä kyseisen johdon alaisuudessa olevasta henkilöstöstä työskentelevät turvallisuusluokitellun tiedon parissa tai voivat päästä turvattuihin tieto- ja tietoliikennejärjestelmiin, ja johdon on pidettävä kirjaa ja raportoitava kaikista tapahtumista tai ilmeisistä puutteista, jotka voivat vaikuttaa turvallisuuteen.

6.3. *Parlamentin virkamiesten ja poliittisten ryhmien palveluksessa olevien parlamentin työntekijöiden luotettavuus*

On otettava käyttöön menettelyt sen varmistamiseksi, että parlamentin virkamiestä tai poliittisen ryhmän palveluksessa olevaa muuta parlamentin työntekijää koskevien kielteisten seikkojen tullessa ilmi ryhdytään toimiin sen määrittämiseksi, onko hän tekemisissä turvallisuusluokitellun tiedon kanssa tai onko hänellä pääsy turvattuihin tieto- ja tietoliikennejärjestelmiin, ja että Euroopan parlamentin asiasta vastaavalle yksikölle ilmoitetaan asiasta. Jos toimivaltainen kansallinen turvallisuusviranomainen toteaa henkilön olevan turvallisuusriski, häntä on estettävä suorittamasta tehtäviä, joissa hän voi vaarantaa turvallisuuden, tai hänet on siirrettävä suorittamaan muita tehtäviä.

7. FYYSINEN TURVALLISUUS

Fyysisellä turvallisuudella tarkoitetaan fyysisten ja teknisten suojatoimenpiteiden toteuttamista niin, että estetään luvaton pääsy turvallisuusluokiteltuihin tietoihin.

7.1. ***Suojan tarve***

Turvallisuusluokiteltujen tietojen suojaamiseksi sovellettavien fyysisten turvallisuustoimien taso on suhteutettava säilytettävän tiedon ja aineiston turvallisuusluokitukseen ja määrään sekä niihin mahdollisesti kohdistuviin uhkiin. Kaikkien turvallisuusluokiteltuja tietoja hallussaan pitävien on noudatettava yhdenmukaisia käytäntöjä tällaisten tietojen turvallisuusluokituksen määrittelyssä sekä yhtäläisiä suojavaatimuksia suojaa edellyttävän tiedon ja aineiston säilyttämisen, lähettämisen ja hävittämisen suhteen.

7.2. ***Tarkastukset***

Ennen kuin turvallisuusluokiteltua tietoa säilyttävissä tiloissa toimivat henkilöt poistuvat säilytystiloista, heidän on varmistettava, että tiedot ovat turvassa ja että kaikki turvalaitteet ovat toimintavalmiina (lukot, hälytykset jne.). Lisäksi tehdään erillisiä tarkastuksia työajan jälkeen.

7.3. ***Rakennusten turvallisuus***

Kiinteistöt, joissa on turvallisuusluokiteltua tietoa tai turvattuja tieto- ja tietoliikennejärjestelmiä, on suojeltava, jottei niihin pääse luvatta.

Tapa, jolla turvallisuusluokitellut tiedot suojataan, esimerkiksi varustamalla säilytystilojen ikkunat kalterein, lukitsemalla ovet, vartioimalla sisäänkäyntiä, asentamalla automaattisia kulun- tai pääsynvalvontajärjestelmiä sekä hälytys- tai murronpaljastusjärjestelmiä, tekemällä turvatarkastuksia ja -kierroksia taikka käyttämällä vartiokoiria, riippuu

a) suojattavan tiedon ja aineiston turvallisuusluokituksesta, määrästä ja sijainnista rakennuksessa;

b) ominaisuuksista, joita kyseisen tiedon ja aineiston turvalliselta säilytyspaikalta edellytetään; ja

c) rakennuksen fyysisistä ominaisuuksista ja sijainnista.

Myös tieto- ja tietoliikennejärjestelmien suojaustapa määräytyy sen mukaan, kuinka tärkeinä resursseja pidetään ja kuinka vakavaa vahinkoa turvallisuuden vaarantumisesta koituisi, sen rakennuksen fyysisistä ominaisuuksista ja sijainnista, joissa järjestelmä on, sekä järjestelmän sijainnista rakennuksessa.

7.4. ***Varautumissuunnitelma***

Turvallisuusluokiteltujen tietojen suojauksesta hätätilanteen aikana on laadittava ennakkoon yksityiskohtainen suunnitelma.

8. **TURVALLISUUSOSOITTIMET, MERKINNÄT, MERKINTÄTAPA JA TURVALLISUUSLUOKITUKSEN HALLINNOINTI**

8.1. ***Turvallisuusosoittimet***

Sallittuja ovat vain tämän päätöksen 2 artiklan d kohdassa tarkoitetut turvallisuusluokitukset.

Turvallisuusluokituksen kelpoisuuden rajaamiseksi (turvallisuusluokitellun tiedon osalta tämä merkitsee turvallisuusluokituksen automaattista alentamista tai poistamista) voidaan käyttää sovittua turvallisuusosoitinta.

Turvallisuusosoittimia voidaan käyttää ainoastaan yhdessä jonkin turvallisuusluokituksen kanssa.

Turvallisuusosoittimia säännellään lisäksi turvallisuusohjeella 2 ja ne määritellään käsittelyohjeissa.

8.2. ***Merkinnät***

Luottamuksellisten tietojen käsittelyä koskevat tietyt ennalta määrätyt ohjeet yksilöidään merkinnällä. Merkinnöillä voidaan osoittaa myös tietyn asiakirjan kattama ala, tiedonsaantitarpeeseen perustuva erityisjakelu tai (muun kuin turvallisuusluokitellun tiedon osalta) julkaisukiellon päättyminen.

Merkintä ei ole turvallisuusluokitus, eikä sitä voida käyttää turvallisuusluokituksen sijasta.

Merkintöjä säännellään lisäksi turvallisuusohjeella 2 ja ne määritellään käsittelyohjeissa.

8.3. ***Turvallisuusluokituksen ja turvallisuusosoittimen merkintätapa***

Turvallisuusluokitukset, turvallisuusosoittimet ja merkinnät määritetään turvallisuusohjeessa 2 olevan E kohdan sekä käsittelyohjeiden mukaisesti.

8.4. ***Turvallisuusluokituksen hallinnointi***

8.4.1 *Yleistä*

Tiedot turvallisuusluokitellaan vain, jos se on tarpeen. Turvallisuusluokitus on ilmoitettava selvästi ja oikein, ja se on säilytettävä vain niin kauan, kuin tiedot on tarpeen suojata.

Tiedon luovuttaja vastaa yksin tiedon turvallisuusluokituksesta ja mahdollisesta myöhemmästä turvallisuusluokituksen alentamisesta tai poistamisesta.

Euroopan parlamentin virkamiehet turvallisuusluokittelevat tiedot ja alentavat tai poistavat turvallisuusluokituksen pääsihteerin ohjeiden mukaan tai hänen valtuuttaminaan.

Turvallisuusluokiteltujen asiakirjojen käsittelyä koskevat yksityiskohtaiset menettelyt laaditaan niin, että voidaan varmistaa asiakirjojen suoja niiden sisältämien tietojen edellyttämällä tavalla.

Niiden henkilöiden lukumäärä, joilla on valtuutus luovuttaa TRÈS SECRET UE / EU TOP SECRET -turvallisuusluokituksen asiakirjoja, on pidettävä mahdollisimman pienenä ja heidän nimensä on kirjattava turvallisuusluokiteltujen tietojen yksikön laatimaan luetteloon.

8.4.2 *Turvallisuusluokituksen soveltaminen*

Asiakirjan turvallisuusluokitus on määriteltävä sen sisällön arkaluonteisuuden mukaan 2 artiklan d kohdassa olevan määritelmän mukaisesti. On tärkeää, että turvallisuusluokitusta myönnetään oikein ja rajoitetusti.

Liitteitä sisältävän kirjeen tai ilmoituksen turvallisuusluokituksen on oltava vähintään yhtä korkea kuin sen liitteille myönnetty korkein turvallisuusluokitus. Asiakirjan luovuttajan olisi ilmoitettava selvästi, mihin turvallisuusluokitukseen asiakirja on luokiteltava, jos se erotetaan liitteistään.

Turvallisuusluokiteltavaksi tarkoitetun asiakirjan luovuttajan on noudatettava edellä mainittuja sääntöjä ja vältettävä yli- ja aliluokittelua.

Tietyn asiakirjan yksittäiset sivut, kohdat, jaksot, liitteet, lisäykset, saatteet ja oheistukset saattavat edellyttää eri turvallisuusluokitusta, joten ne on turvallisuusluokiteltava sen mukaisesti. Koko asiakirja on turvallisuusluokiteltava korkeimman turvallisuusluokituksen saaneen osansa mukaan.

9. **TARKASTUKSET**

Euroopan parlamentin turvallisuus- ja riskianalyysiosasto tekee määräajoin sisäisiä tarkastuksia, ja se voi pyytää komission tai neuvoston turvallisuusviranomaisilta apua.

Unionin toimielinten turvallisuusviranomaiset ja toimivaltaiset yksiköt voivat suorittaa osana kumman tahansa osapuolen alulle panemaa sovittua prosessia vertaisarviointeja turvajärjestelyistä, joiden avulla pyritään suojaamaan toimielinten välisten asianomaisten sopimusten mukaisesti vaihdettavaa turvallisuusluokiteltua tietoa.

10. **TURVALLISUUSLUOKITUKSEN JA MERKINNÄN POISTAMISMENETTELYT**

10.1. Turvallisuusluokiteltujen tietojen yksikkö tarkastelee rekisterissään olevia luottamuksellisia tietoja ja ehdottaa luovuttajalle asiakirjan turvallisuusluokituksen tai merkinnän poistamista viimeistään 25 vuoden kuluttua asiakirjan tuottamispäivästä. Asiakirjat, joiden turvallisuusluokitusta tai merkintää ei poisteta ensimmäisessä tarkastelussa, tutkitaan uudestaan säännöllisin väliajoin vähintään joka viides vuosi. Merkinnän poistomenettely voi sellaisten asiakirjojen ohella, jotka todella sijaitsevat turvallisella alueella olevissa turvallisissa arkistoissa ja joilla on asianmukainen turvallisuusluokitus, kattaa myös muita luottamuksellisia tietoja, jotka ovat joko parlamentin elimen tai parlamentin historiallisista arkistoista vastaavan yksikön hallussa.

10.2 Asiakirjan turvallisuusluokituksen tai merkinnän poistamista koskevan päätöksen tekee pääsääntöisesti asiakirjan luovuttaja yksin tai poikkeuksellisesti luovuttaja yhdessä tällaista tietoa hallussaan pitävän parlamentin elimen / parlamentin elimessä toimivan jäsenen kanssa ennen kuin asiakirjan sisältämät tiedot siirretään parlamentin historiallisista arkistoista vastaavaan yksikköön. Turvallisuusluokitellun asiakirjan turvallisuusluokitus tai merkintä voidaan poistaa vain, kun luovuttaja on antanut siihen etukäteen kirjallisen luvan. Muiden luottamuksellisten tietojen tapauksessa parlamentin elimen / parlamentin elimessä toimivan jäsenen sihteeristö, jonka hallussa tiedot ovat, tekee yhdessä tietojen luovuttajan kanssa päätöksen siitä, voidaanko asiakirjan merkintä poistaa.

10.3. Turvallisuusluokiteltujen tietojen yksikkö ilmoittaa luovuttajan puolesta asiakirjan vastaanottajille turvallisuusluokituksen tai merkinnän muutoksesta, ja näiden on puolestaan ilmoitettava muutoksesta kaikille myöhemmille vastaanottajille, joille he ovat lähettäneet asiakirjan tai sen jäljennöksen.

10.4. Turvallisuusluokituksen poistaminen ei vaikuta asiakirjassa mahdollisesti oleviin turvallisuusosoittimiin tai merkintöihin.

10.5. Jos turvallisuusluokitus poistetaan, jokaisen sivun ylä- ja alareunaan merkitty alkuperäinen turvallisuusluokitus yliviivataan. Asiakirjan ensimmäiselle sivulle (kansilehdelle) merkitään leima ja lisätään turvallisuusluokiteltujen tietojen yksikön viite. Jos merkintä poistetaan, jokaisen sivun yläreunassa oleva alkuperäinen merkintä yliviivataan.

10.6. Asiakirjan, jonka turvallisuusluokitus tai merkintä on poistettu, teksti liitetään sähköiseen tietueeseen tai vastaavaan järjestelmään, jonne se on kirjattu.

10.7. Kun asiakirja kuuluu yksityisyyden suojaa ja yksilön koskemattomuutta tai luonnollisen henkilön tai oikeushenkilön kaupallisia etuja koskevien poikkeusten piiriin tai on arkaluonteinen, sovelletaan neuvoston asetuksen (ETY, Euratom) N:o 354/83 2 artiklan säännöksiä.

10.8. Edellä olevien 10.1–10.7. kohdan lisäksi sovelletaan seuraavia sääntöjä:

a) kun kyse on kolmannen osapuolen asiakirjasta, turvallisuusluokiteltujen tietojen yksikkö kuulee kyseistä kolmatta osapuolta ennen turvallisuusluokituksen tai merkinnän poistamista;

b) kun sovelletaan yksityiselämän ja yksilön koskemattomuuden suojaan liittyvää poikkeusta, turvallisuusluokituksen tai merkinnän poistamista koskevassa menettelyssä otetaan huomioon erityisesti asianomaisen henkilön suostumus tai tarvittaessa se, että asianomaista henkilöä ei voida tietojen perusteella tunnistaa;

c) kun sovelletaan tietyn luonnollisen henkilön tai oikeushenkilön taloudellisten etujen suojaan liittyvää poikkeusta, asianomaiselle henkilölle voidaan antaa asiasta tieto julkaisemalla tätä koskeva ilmoitus *Euroopan unionin virallisessa lehdessä* ja asettaa huomautusten esittämistä varten neljän viikon määräaika julkaisemisesta lukien.

2 osa

LUOTETTAVUUSSELVITYSMENETTELY

11. **EUROOPAN PARLAMENTIN JÄSENTEN LUOTETTAVUUSSELVITYSMENETTELY**

11.1. Saadakseen tutustua tietoihin, joiden turvallisuusluokitus on CONFIDENTIEL UE / EU CONFIDENTIAL tai vastaava, Euroopan parlamentin jäsenen on täytynyt saada tätä koskeva valtuutus joko tämän liitteen 11.3 ja 11.4 kohdassa tarkoitetun menettelyn mukaisesti tai sen perusteella, että hän on antanut tämän päätöksen 3 artiklan 4 kohdan mukaisesti juhlallisen vakuutuksen olla paljastamatta tietoja.

11.2 Saadakseen tutustua tietoihin, joiden turvallisuusluokitus on TRÈS SECRET UE / EU TOP SECRET- ja SECRET UE / EU SECRET tai vastaava, Euroopan parlamentin jäsenen on täytynyt saada tätä koskeva valtuutus 11.3 ja 11.14 kohdassa tarkoitetun menettelyn mukaisesti.

11.3. Valtuutus annetaan ainoastaan Euroopan parlamentin jäsenelle, josta jäsenvaltion toimivaltainen kansallinen viranomainen on tehnyt luotettavuusselvityksen 11.9–11.14 kohdassa tarkoitetun menettelyn mukaisesti. Puhemies vastaa valtuutusten antamisesta jäsenille.

11.4. Puhemies antaa kirjallisen valtuutuksen 11.8–11.13 kohdan mukaisesti suoritetun luotettavuusselvityksen perusteella saatuaan jäsenvaltion kansallisen toimivaltaisen viranomaisen lausunnon.

11.5. Euroopan parlamentin turvallisuus- ja riskianalyysiosasto pitää yllä ajantasaista luetteloa jäsenistä, joille on annettu valtuutus, myös 11.15 kohdassa tarkoitettu väliaikainen valtuutus.

11.6. Valtuutus on voimassa viisi vuotta, mutta enintään niin kauan kuin henkilö on valtuutuksen saamisen perusteena olevissa tehtävissä. Valtuutuksen voimassaoloa voidaan jatkaa 11.4 kohdan mukaista menettelyä noudattaen.

11.7. Puhemies peruuttaa valtuutuksen, jos katsoo peruuttamisen olevan perusteltua. Päätös valtuutuksen peruuttamisesta ilmoitetaan asianomaiselle Euroopan parlamentin jäsenelle, joka voi pyytää, että puhemies kuulee häntä ennen peruuttamisen voimaantuloa, sekä toimivaltaiselle kansalliselle viranomaiselle.

11.8. Luotettavuusselvitys tehdään puhemiehen pyynnöstä yhteistyössä kyseisen jäsenen kanssa. Luotettavuusselvityksen tekevä toimivaltainen kansallinen viranomainen on sen jäsenvaltion viranomainen, jonka kansalainen asianomainen tarvitseva jäsen on.

11.9. Luotettavuusselvitystä varten asianomaisen Euroopan parlamentin jäsenen on täytettävä henkilötietoilmoitus.

11.10. Puhemies yksilöi toimivaltaiselle kansalliselle viranomaiselle osoitetussa pyynnössään niiden turvallisuusluokiteltujen tietojen turvallisuusluokituksen, jotka kyseinen Euroopan parlamentin jäsen saisi tietoonsa, jotta toimivaltainen kansallinen viranomainen voi tehdä selvityksen.

11.11. Kansallisen viranomaisen suorittaman luotettavuusselvitysmenettelyn kaikkien vaiheiden ja sen tulosten on oltava kyseisessä jäsenvaltiossa voimassa olevan alaa koskevan lainsäädännön mukaiset, muutoksenhakukeinoja koskeva lainsäädäntö mukaan lukien.

11.12. Puhemies voi antaa valtuutuksen asianomaiselle Euroopan parlamentin jäsenelle, jos toimivaltainen kansallinen viranomainen antaa myönteisen lausunnon.

11.13. Jos toimivaltainen kansallinen viranomainen antaa kielteisen lausunnon, asianomaiselle Euroopan parlamentin jäsenelle ilmoitetaan tästä, ja hän voi pyytää, että puhemies kuulee häntä. Puhemies voi pyytää toimivaltaista kansallista viranomaista antamaan tarkempia tietoja, jos katsoo sen olevan tarpeen. Jos kielteinen lausunto vahvistetaan, valtuutusta ei anneta.

11.14. Euroopan parlamentin jäsenelle, joka on saanut valtuutuksen 11.3 kohdan mukaisesti, annetaan valtuutuksen antamisen yhteydessä ja tämän jälkeen määräajoin tarvittavat ohjeet turvallisuusluokiteltujen tietojen suojaamisesta ja siitä, miten tämä varmistetaan. Jäsen allekirjoittaa vakuutuksen siitä, että on saanut ohjeet.

11.15. Puhemies voi poikkeustilanteessa ennen 11.11 kohdassa tarkoitetun luotettavuusselvityksen saamista ilmoitettuaan asiasta kansalliselle toimivaltaiselle viranomaiselle ja edellyttäen, että tältä ei ole kuukauden kuluessa saatu huomautuksia, antaa jäsenelle väliaikaisen valtuutuksen enintään kuudeksi kuukaudeksi. Annettu väliaikainen valtuutus ei anna oikeutta tutustua tietoihin, joiden turvallisuusluokitus on TRÈS SECRET UE / EU TOP SECRET tai vastaava.

12. EUROOPAN PARLAMENTIN VIRKAMIESTEN JA POLIITTISTEN RYHMIEN PALVELUKSESSA OLEVIEN PARLAMENTIN MUIDEN TYÖNTEKIJÖIDEN LUOTETTAVUUSSELVITYSMENETTELY

12.1. Turvallisuusluokiteltuihin tietoihin voivat tutustua vain Euroopan parlamentin virkamiehet ja poliittisten ryhmien palveluksessa työskentelevät muut parlamentin työntekijät, joiden on tehtäviensä ja yksikön tarpeiden vuoksi saatava tutustua niihin tai käyttää niitä.

12.2. Saadakseen tutustua tietoihin, joiden turvallisuusluokitus on CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE / EU SECRET tai TRÈS SECRET UE / EU TOP SECRET tai vastaava, 12.1 kohdassa tarkoitetuilla henkilöillä on oltava 12.3 ja 12.4 kohdassa tarkoitetun menettelyn mukaisesti annettu valtuutus.

12.3. Valtuutus annetaan ainoastaan sellaisille 12.1 kohdassa tarkoitetuille henkilöille, joista jäsenvaltioiden toimivaltaiset kansalliset viranomaiset ovat tehneet luotettavuusselvityksen 12.9–12.14 kohdassa tarkoitetun menettelyn mukaisesti. Pääsihteeri vastaa valtuutuksen antamisesta parlamentin virkamiehille ja poliittisten ryhmien palveluksessa oleville parlamentin työntekijöille.

12.4. Pääsihteeri antaa kirjallisen valtuutuksen 12.8–12.13 alakohdan mukaisesti suoritetun luotettavuusselvityksen perusteella saatuaan jäsenvaltion kansallisen toimivaltaisen viranomaisen lausunnon.

12.5. Euroopan parlamentin turvallisuus- ja riskianalyysiosasto pitää yllä ajantasaista Euroopan parlamentin asianomaisten osastojen toimittamaa luetteloa kaikista luotettavuusselvitystä edellyttävistä tehtävistä ja kaikista henkilöistä, joille on annettu valtuutus, myös 12.15 kohdassa tarkoitettu väliaikainen valtuutus.

12.6. Valtuutus on voimassa viisi vuotta, mutta enintään niin kauan kuin henkilö on valtuutuksen saamisen perusteena olevissa tehtävissä. Valtuutuksen voimassaoloa voidaan jatkaa 12.4 kohdan mukaista menettelyä noudattaen.

12.7. Pääsihteeri voi peruuttaa valtuutuksen, jos katsoo peruuttamisen olevan perusteltua. Päätös valtuutuksen peruuttamisesta ilmoitetaan asianomaiselle Euroopan parlamentin virkamiehelle tai poliittisen ryhmän palveluksessa olevalle muulle parlamentin työntekijälle, joka voi pyytää, että pääsihteeri kuulee häntä ennen peruutuksen voimaantuloa, sekä toimivaltaiselle kansalliselle viranomaiselle.

12.8. Luotettavuusselvitys tehdään pääsihteerin pyynnöstä yhteistyössä asianomaisen Euroopan parlamentin virkamiehen tai poliittisen ryhmän palveluksessa olevan muun parlamentin työntekijän kanssa. Luotettavuusselvityksen tekevä toimivaltainen kansallinen viranomainen on sen jäsenvaltion viranomainen, jonka kansalainen asianomainen henkilö on. Kansallisten lakien ja asetusten salliessa toimivaltaiset kansalliset viranomaiset voivat tehdä tutkinnan muista kuin omista kansalaisistaan, jotka pyytävät saada tutustua tietoihin, joiden turvallisuusluokitus on CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE /E U SECRET tai TRÈS SECRET UE / EU TOP SECRET.

12.9. Luotettavuusselvitystä varten asianomaisen Euroopan parlamentin virkamiehen tai poliittisen ryhmän palveluksessa olevan muun parlamentin työntekijän on täytettävä henkilötietoilmoitus.

12.10. Pääsihteeri yksilöi toimivaltaiselle kansalliselle viranomaiselle osoitetussa pyynnössään niiden turvallisuusluokiteltujen tietojen turvallisuusluokituksen, jotka kyseinen Euroopan parlamentin virkamies tai poliittisen ryhmän palveluksessa oleva muu parlamentin työntekijä saisi tietoonsa, jotta toimivaltainen kansallinen viranomainen voi tehdä selvityksen ja antaa lausunnon kyseiselle henkilölle annettavan valtuutuksen asianmukaisesta tasosta.

12.11. Toimivaltaisen kansallisen viranomaisen suorittaman luotettavuusselvitysmenettelyn kaikkien vaiheiden ja sen tulosten on oltava kyseisessä jäsenvaltiossa voimassa olevan alaa koskevan lainsäädännön mukaiset, muutoksenhakukeinoja koskeva lainsäädäntö mukaan lukien.

12.12. Pääsihteeri voi antaa valtuutuksen asianomaiselle Euroopan parlamentin virkamiehelle tai muulle poliittisen ryhmän palveluksessa olevalle parlamentin työntekijälle, jos jäsenvaltion toimivaltainen kansallinen viranomainen antaa myönteisen lausunnon.

12.13. Jos toimivaltainen kansallinen viranomainen antaa kielteisen lausunnon, asianomaiselle Euroopan parlamentin virkamiehelle tai poliittisen ryhmän palveluksessa olevalle muulle parlamentin työntekijälle ilmoitetaan tästä, ja hän voi pyytää, että pääsihteeri kuulee häntä. Pääsihteeri voi pyytää toimivaltaista kansallista viranomaista antamaan tarkempia tietoja, jos katsoo sen olevan tarpeen. Jos kielteinen lausunto vahvistetaan, valtuutusta ei voida antaa.

12.14. Euroopan parlamentin virkamiehille ja poliittisten ryhmien palveluksessa oleville muille parlamentin työntekijöille, jotka ovat saaneet valtuutuksen 12.4 ja 12.5 kohdan mukaisesti, annetaan valtuutuksen antamisen yhteydessä ja tämän jälkeen määräajoin tarvittavat ohjeet turvallisuusluokiteltujen tietojen suojaamisesta ja siitä, miten tämä varmistetaan. Tällainen parlamentin virkamies tai poliittisen ryhmän palveluksessa oleva parlamentin työntekijä allekirjoittaa vakuutuksen siitä, että hän on saanut ohjeet ja sitoutuu noudattamaan niitä.

12.15. Pääsihteeri voi poikkeustilanteessa ennen 12.11 kohdassa tarkoitetun luotettavuusselvityksen saamista ilmoitettuaan asiasta kansalliselle toimivaltaiselle viranomaiselle ja edellyttäen, että tältä ei ole kuukauden kuluessa saatu huomautuksia, antaa Euroopan parlamentin virkamiehelle tai poliittisen ryhmän palveluksessa olevalle muulle parlamentin työntekijälle väliaikaisen valtuutuksen enintään kuudeksi kuukaudeksi. Annettu väliaikainen valtuutus ei anna oikeutta tutustua tietoihin, joiden turvallisuusluokitus on TRÈS SECRET UE / EU TOP SECRET tai vastaava.

LIITE II

JOHDANTO

Näillä säännöksillä säädetään turvallisuusohjeista, joilla ohjataan luottamuksellisten tietojen turvallinen käsittelyä ja hallinnointia Euroopan parlamentissa ja varmistetaan se. Turvallisuusohjeet muodostavat yhdessä käsittelyohjeiden kanssa tämän päätöksen 3 artiklan 2 kohdassa tarkoitetun Euroopan parlamentin tietoturvan hallintajärjestelmän:

TURVALLISUUSOHJE 1

Turvajärjestelyt Euroopan parlamentissa luottamuksellisten tietojen suojaamiseksi

TURVALLISUUSOHJE 2

Luottamuksellisten tietojen hallinnointi

TURVALLISUUSOHJE 3

Luottamuksellisten tietojen käsittely automaattisissa viestintä- ja tietojärjestelmissä

TURVALLISUUSOHJE 4

Fyysinen turvallisuus

TURVALLISUUSOHJE 5

Yhteisöturvallisuus

TURVALLISUUSOHJE 6

Tietoturvaloukkaukset ja luottamuksellisten tietojen katoaminen tai vaarantuminen

TURVALLISUUSOHJE 1

TURVAJÄRJESTELYT EUROOPAN PARLAMENTISSA LUOTTAMUKSELLISTEN TIETOJEN SUOJAAMISEKSI

1. Pääsihteeri vastaa tämän päätöksen kattavasta ja johdonmukaisesta täytäntöönpanosta.

Pääsihteeri toteuttaa kaikki tarvittavat toimet sen varmistamiseksi, että Euroopan parlamentin jäsenet, Euroopan parlamentin virkamiehet, muut poliittisten ryhmien palveluksessa olevat parlamentin työntekijät sekä sopimuspuolet soveltavat tätä päätöstä luottamuksellisten tietojen käsittelyssä ja varastoinnissa.

2. Turvallisuusviranomainen on pääsihteeri. Tässä ominaisuudessa pääsihteeri vastaa:

2.1. kaikkien sellaisten turvallisuuteen liittyvien seikkojen koordinoinnista, jotka koskevat parlamentin toimintaa suhteessa luottamuksellisten tietojen suojaan;

2.2. turvallisen alueen, turvallisten lukusalien ja turvallisten välineiden hyväksymisestä;

2.3. sellaisten päätösten täytäntöönpanosta tämän päätöksen 6 artiklan mukaisesti, joilla annetaan parlamentille lupa välittää turvallisuusluokiteltuja tietoja kolmansille osapuolille;

2.4. sellaisen luottamuksellisen tietojen vuodon tutkinnasta tai tutkinnan toimeksiantamisesta, joka on tapahtunut prima facie parlamentissa, yhdessä Euroopan parlamentin puhemiehen kanssa, jos tapaukseen liittyy Euroopan parlamentin jäsen;

2.5. tiiviin yhteyden säilyttämisestä unionin muiden elinten turvallisuusviranomaisten kanssa ja jäsenvaltioiden kansallisten turvallisuusviranomaisten kanssa, jotta voidaan varmistaa paras mahdollinen koordinointi turvallisuusluokiteltuun tietoon liittyvän turvallisuuspolitiikan yhteydessä;

2.6. parlamentin turvallisuuspolitiikan ja menettelyn jatkuvasta tarkastelusta ja siitä seuraavien asianmukaisten suositusten antamisesta;

2.7. raportoinnista kansalliselle turvallisuusviranomaiselle, joka on suorittanut luotettavuusselvityksen, liitteessä I olevan 2 osan 11.3 kohdan mukaisesti, jos kyseessä ovat tähän viranomaiseen mahdollisesti vaikuttavat kielteiset tiedot.

3. Kun kyse on Euroopan parlamentin jäsenistä, pääsihteeri hoitaa tehtäviään tiiviissä yhteydessä Euroopan parlamentin puhemiehen kanssa.

4. Pääsihteeriä avustavat hänen suorittaessaan 2 ja 3 kohdassa tarkoitettuja tehtäviään apulaispääsihteeri, turvallisuus- ja riskianalyysiosasto, tietohallinto-osasto ja turvallisuusluokiteltujen tietojen yksikkö.

4.1. Turvallisuus- ja riskianalyysiosasto vastaa henkilökohtaisista suojatoimista ja erityisesti liitteessä I olevan 2 osan mukaisesta luotettavuusselvityksestä. Lisäksi turvallisuus- ja riskianalyysiosasto:

a) toimii unionin muiden elinten turvaviranomaisten ja jäsenvaltioiden turvallisuusyksiköiden yhteyspisteenä asioissa, jotka liittyvät Euroopan parlamentin jäsenten, Euroopan parlamentin virkamiesten ja muiden poliittisten ryhmien palveluksessa olevien parlamentin työntekijöiden luotettavuusselvityksiin;

b) antaa tarvittavia yleisiä turvallisuusohjeita liittyen velvoitteisiin, jotka koskevat turvallisuusluokiteltujen tietojen suojaa ja sen laiminlyönnistä aiheutuvia seuraamuksia;

c) valvoo parlamentin tiloissa sijaitsevien turvallisen alueen ja turvallisten lukusalien toimintaa tarvittaessa yhteistyössä unionin muiden elinten turvaviranomaisten ja jäsenvaltioiden turvallisuusyksiköiden kanssa;

d) tarkastaa yhdessä unionin muiden elinten turvaviranomaisten ja jäsenvaltioiden turvallisuusyksiköiden kanssa turvallisuusluokiteltujen tietojen hallinnointiin ja varastointiin liittyviä menettelyjä sekä parlamentin tiloissa sijaitsevia turvallisia alueita ja turvallisia lukusaleja, joissa turvallisuusluokiteltuja tietoja käsitellään;

e) ehdottaa pääsihteerille tarvittavia käsittelyohjeita.

4.2. Tietohallinto-osasto vastaa luottamuksellisten tietojen käsittelystä turvallisissa tietojärjestelmissä Euroopan parlamentissa.

4.3. Turvallisuusluokiteltujen tietojen yksikkö:

a) määrittää luottamuksellisten tietojen tehokkaaseen suojaan liittyvät turvallisuustarpeet tiiviissä yhteistyössä turvallisuus- ja riskianalyysiosaston ja tietohallinto-osaston sekä unionin muiden elinten turvaviranomaisten kanssa;

b) määrittää kaikki luottamuksellisten tietojen hallinnointia ja varastointia parlamentissa koskevat näkökohdat käsittelyohjeiden pohjalta;

c) vastaa turvallisen alueen toiminnasta;

d) vastaa luottamuksellisten tietojen hallinnoinnista ja niihin tutustumisesta turvallisella alueella tai turvallisuusluokiteltujen tietojen yksikön lukusalissa tämän päätöksen 7 artiklan 2 ja 3 kohdan mukaisesti;

e) vastaa turvallisuusluokiteltujen tietojen yksikön rekisterin ylläpidosta;

f) raportoi turvallisuusviranomaiselle kaikista turvallisuusluokiteltujen tietojen yksikössä olevien ja turvallisella alueella tai turvallisuusluokiteltujen tietojen yksikön turvallisessa lukusalissa olevien luottamuksellisten tietojen todistetuista tai epäillyistä turvallisuusrikkomuksista, katoamisista ja vaarantumisista.

5. Lisäksi pääsihteeri nimittää turvallisuusviranomaisena seuraavat viranomaiset:

a) turvallisuusjärjestelyt hyväksyvä viranomainen;

b) operatiivinen tiedonturvaamisviranomainen;

c) salatun aineiston jakelusta vastaava viranomainen;

d) TEMPEST-viranomainen;

e) tiedonturvaamisviranomainen.

Näiden tehtävien hoitaminen ei edellytä yksittäisiä organisatorisia yksiköitä. Niillä on erilliset mandaatit. Kuitenkin nämä toiminnot ja niihin liittyvät tehtävät voidaan yhdistää samaan organisaatioyksikköön tai hajottaa eri organisaatioyksiköille edellyttäen, että vältetään eturistiriitoja ja tehtävien päällekkäisyyttä.

6. Turvallisuusjärjestelyt hyväksyvä viranomainen antaa neuvoja kaikista turvallisuusseikoista liittyen kaikkien tietotekniikkajärjestelmien ja -verkkojen hyväksymiseen parlamentissa niin, että se vastaa:

6.1. sen varmistamisesta, että viestintä- ja tietojärjestelmä on asiaankuuluvien turvallisuusperiaatteiden ja turvallisuutta koskevien suuntaviivojen mukainen, viestintä- ja tietojärjestelmän hyväksyntää turvallisuusluokiteltujen tietojen käsittelemiseksi tiettyyn turvallisuusluokitukseen asti järjestelmän käyttöympäristössä koskevan lausunnon antamisesta ja hyväksynnän ehtojen ja edellytysten sekä perusteiden, joiden täyttyessä järjestelmä on hyväksyttävä uudelleen, ilmoittamisesta;

6.2. asiaankuuluvien periaatteiden mukaisen turvallisuusjärjestelyjen hyväksyntäprosessin perustamisesta sekä alaisuudessaan olevien viestintä- ja tietojärjestelmien hyväksymisedellytysten ilmoittamisesta selkeästi;

6.3. sellaisen turvallisuushyväksyntästrategian laatimisesta, jossa määritetään hyväksyntäprosessin yksityiskohtaisuus niin, että se on suhteutettu edellytettävään turvaamistasoon;

6.4. turvallisuuteen liittyvien asiakirjojen tarkastelusta ja hyväksymisestä, riskinhallintaa ja jäännösriskiä koskevat lausunnot, turvallisuusjärjestelyjen täytäntöönpanon tarkistusasiakirjat ja turvamenettelyt mukaan luettuina, ja sen varmistamisesta, että ne ovat parlamentin turvallisuussääntöjen ja -periaatteiden mukaisia;

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

6.6. viestintä- ja tietojärjestelmään liittyvien arkaluonteisten tehtävien turvallisuusvaatimusten (esimerkiksi henkilöturvallisuusselvitysten tasojen) määrittämisestä;

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

6.8. sellaisen teknisten välineistön turvanormien hyväksymisestä, joka on tarkoitettu turvallisuusluokiteltujen tietojen turvalliseen käsittelyyn ja suojaamiseen;

6.9. sen varmistamisesta, että parlamentissa käytettävät salaustuotteet sisältyvät EU:n hyväksymien tuotteiden luetteloon;

6.10. järjestelmän toimittajan, turvallisuusalan toimijoiden ja käyttäjien edustajien kuulemisesta turvallisuusriskien hallinnasta, erityisesti jäännösriskistä, ja hyväksyntälausunnon ehdoista ja edellytyksistä.

7. Operatiivisen tiedonturvaamisviranomaisen on huolehdittava:

7.1. turvallisuusasiakirjojen laatimisesta turvallisuusperiaatteiden ja turvallisuutta koskevien suuntaviivojen mukaisesti, erityisesti jäännösriskiä koskevan lausunnon, turvamenettelyjen ja viestintä- ja tietojärjestelmän hyväksyntäprosessiin kuuluvan salaussuunnitelman laatimisesta;

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

7.3. turvamenettelyjen täytäntöönpanon ja soveltamisen valvomisesta, jolloin operatiivinen turvallisuusvastuu voidaan tarvittaessa siirtää järjestelmän omistajalle eli turvallisuusluokiteltujen tietojen yksikölle;

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

7.5. turvallisuusanalyysien tarkistusten ja testien suorittamisesta erityisesti turvallisuusjärjestelyt hyväksyvän viranomaisen vaatimien asiaankuuluvien riskiraporttien laatimiseksi;

7.6. viestintä- ja tietojärjestelmäkohtaisen tiedonturvaamiskoulutuksen antamisesta;

7.7. viestintä- ja tietojärjestelmäkohtaisten turvatoimien toteuttamisesta ja käytöstä.

8. Salatun aineiston jakelusta vastaavan viranomaisen on huolehdittava:

8.1. EU:n salausaineiston hallinnoinnista ja kirjanpidosta;

8.2. sen varmistamisesta tiiviissä yhteistyössä turvallisuusjärjestelyt hyväksyvän viranomaisen kanssa, että EU:n salausaineiston kirjanpidossa, suojatussa käsittelyssä, säilyttämisessä ja jakelussa käytetään asianmukaisia menettelyjä ja että sitä varten on asianmukaiset suunnitelmat; ja

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

9. TEMPEST-viranomainen vastaa siitä, että turvallisuusluokiteltujen tietojen yksikkö noudattaa TEMPEST-menettelyjä ja -käsittelyohjeita. Sen tehtävänä on hyväksyä TEMPEST-turvatoimia turvallisuusluokiteltujen tietojen suojaamiseen tarkoitetuille tiloille ja tuotteille määrättyyn turvallisuusluokitukseen saakka niiden käyttöympäristössä.

10. Tiedonturvaamisviranomainen vastaa kaikista näkökohdista, jotka liittyvät luottamuksellisten tietojen hallinnointiin ja käsittelyyn Euroopan parlamentissa, ja erityisesti:

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

10.2. salaustuotteisiin liittyvien teknisten tietojen tallessa pitämisestä ja hallinnoinnista;

10.3. sen varmistamisesta, että turvallisuusluokiteltujen tietojen suojaamiseksi valitut tiedonturvaamistoimenpiteet ovat niiden kelpoisuutta ja valintaa koskevien asiaankuuluvien periaatteiden mukaisia;

10.4. sen varmistamisesta, että salaustuotteiden valinnassa noudatetaan niiden kelpoisuutta ja valintaa koskevia periaatteita;

10.5. järjestelmän toimittajan, turvallisuusalan toimijoiden ja käyttäjien edustajien kuulemisesta tietojen turvaamiseen liittyen.

TURVALLISUUSOHJE 2

LUOTTAMUKSELLISTEN TIETOJEN HALLINNOINTI

A. **JOHDANTO**

1. Tässä turvallisuusohjeessa esitetään määräykset, jotka koskevat parlamentin harjoittamaa luottamuksellisen tiedon hallinnointia.

2. Luottamuksellisia tietoja tuotettaessa tietojen luovuttajan on arvioitava luottamuksellisuuden tasoa ja tehtävä päätös noudattaen tässä turvallisuusohjeessa määritettyjä periaatteita tällaisten tietojen turvallisuusluokittelusta ja merkinnästä.

B. **EU:n TURVALLISUUSLUOKITELLUT TIEDOT**

3. Päätös asiakirjan turvallisuusluokituksesta on tehtävä ennen asiakirjan laatimista. Siksi tietojen luokittelu EU:n turvallisuusluokitelluiksi tiedoiksi edellyttää tietojen luottamuksellisuuden tason etukäteisarviointia sekä tietojen luovuttajan päätöstä siitä, että tällaisten tietojen luvaton paljastaminen aiheuttaisi jonkinasteista haittaa Euroopan unionin tai sen yhden tai useamman jäsenvaltion tai yksilöiden eduille.

4. Kun päätös tietojen turvallisuusluokituksesta tehdään, suoritetaan toinen etukäteisarviointi turvallisuusluokituksen asianmukaisen tason määrittämiseksi. Asiakirjan turvallisuusluokitus riippuu sen sisällön arkaluontoisuuden asteesta.

5. Vastuu tietojen turvallisuusluokituksesta on kokonaan niiden luovuttajalla. Parlamentin virkamiehet turvallisuusluokittelevat tiedot pääsihteerin ohjeiden mukaan tai hänen valtuuttaminaan.

6. Turvallisuusluokitusta käytetään asianmukaisesti ja säästeliäästi. Turvallisuusluokituksen saavan asiakirjan luovuttajan on estettävä liian korkean tai liian matalan turvallisuusluokituksen käyttö.

7. Tiedoille määritetty turvallisuusluokituksen taso määrää suojan tason, joka niille annetaan henkilöstön turvallisuuteen, fyysiseen turvallisuuteen, menettelyn turvallisuuteen ja tietojen turvaamiseen liittyen.

8. Turvallisuusluokitusta edellyttävät tiedot merkitään sellaisiksi ja niitä käsitellään sellaisina tietojen fyysisestä muodosta riippumatta. Tietojen turvallisuusluokitus ilmoitetaan selvästi tietojen vastaanottajille joko turvallisuusluokitusmerkinnän avulla (jos tiedot esitetään kirjallisesti paperilla tai viestintä- ja tietojärjestelmässä) tai ilmoituksen avulla (jos tiedot esitetään suullisesti esimerkiksi keskustelun tai suljetun kokouksen yhteydessä). Turvallisuusluokitellut tiedot merkitään fyysisesti niin, että niiden turvallisuusluokitus on helposti nähtävissä.

9. Sähköisessä muodossa olevaa EU:n turvallisuusluokiteltua tietoa voidaan tuottaa vain hyväksytyssä viestintä- ja tietojärjestelmässä. Itse turvallisuusluokitellut tiedot sekä tiedostonimi ja tallennusväline (jos se on ulkoinen, kuten CD-ROM-levy tai USB-tikku) varustetaan asianmukaisella turvallisuusluokitusmerkinnällä.

10. Tiedoille annetaan turvallisuusluokitus heti, kun niistä aletaan laatia asiakirjoja. Esimerkiksi henkilökohtaiset muistiinpanot, luonnokset tai sähköpostiviestit, jotka sisältävät turvallisuusluokituksen edellyttämiä tietoja, merkitään EU:n turvallisuusluokitelluiksi tiedoiksi alusta lähtien ja niitä tuotetaan ja käsitellään noudattaen tätä päätöstä ja sen fyysisiä ja teknisiä käsittelyohjeita. Tällaiset tiedot voivat sen jälkeen kehittyä viralliseksi asiakirjaksi, joka niin ikään saa asianmukaisen merkinnän ja käsittelyn. Luonnosvaiheessa virallista asiakirjaa on ehkä arvioitava uudelleen ja sille on annettava korkeampi tai matalampi luokitus sen muuttuessa.

11. Tietojen luovuttaja voi päättää standardinmukaisen luokituksen myöntämisestä sentyyppisille tiedoille, joita hän tuottaa säännöllisesti. Tietojen luovuttajan on kuitenkin varmistettava, että hän ei tällöin määritä tiedoille järjestelmällisesti liian korkeaa tai matalaa luokitusta.

12. EU:n turvallisuusluokitelluilla tiedoilla on aina oltava niiden turvallisuusluokitustasoa vastaava turvallisuusluokitusmerkintä.

B.1. ***Luokitteluasteet***

13. EU:n turvallisuusluokitellut tiedot jaetaan seuraaviin turvallisuusluokituksiin:

— TRÈS SECRET UE / EU TOP SECRET sellaisena kuin se on määritelty tämän päätöksen 2 artiklan d kohdassa, kun tietojen vaarantuminen todennäköisesti:

a) uhkaisi suoraan unionin tai yhden tai useamman sen jäsenvaltion tai kolmannen maan tai kansainvälisen järjestön sisäistä vakautta;

b) aiheuttaisi poikkeuksellisen vakavaa vahinkoa suhteille kolmansiin maihin tai kansainvälisiin järjestöihin;

c) aiheuttaisi suoraan laajamittaista ihmishenkien menetystä;

d) vahingoittaisi vakavasti jäsenvaltioiden tai muiden osallistujien käyttämän henkilöstön toiminnan tehokkuutta tai turvallisuutta tai erittäin arvokkaiden turvallisuus- tai tiedusteluoperaatioiden jatkuvaa tehokkuutta; tai

e) aiheuttaisi vakavaa pitkäaikaista haittaa unionin tai jäsenvaltioiden taloudelle;

— SECRET UE / EU SECRET sellaisena kuin se on määritelty tämän päätöksen 2 artiklan d kohdassa, kun tietojen vaarantuminen todennäköisesti:

a) lisäisi kansainvälistä jännitystä merkittävästi;

b) vahingoittaisi vakavasti suhteita kolmansiin maihin ja kansainvälisiin järjestöihin;

c) uhkaisi ihmishenkiä suoraan tai vaarantaisi vakavasti yleisen järjestyksen tai yksilön turvallisuuden tai vapauden;

d) vahingoittaisi tärkeitä kaupallisia tai poliittisia neuvotteluja tai aiheuttaisi merkittäviä toiminnallisia ongelmia unionille tai jäsenvaltioille;

e) vahingoittaisi vakavasti jäsenvaltioiden toiminnan turvallisuutta tai erittäin tärkeiden turvallisuus- tai tiedusteluoperaatioiden tehokkuutta;

f) aiheuttaisi huomattavaa aineellista vahinkoa unionin tai jäsenvaltion rahoitukseen, rahaan, talouteen tai kauppaan liittyville eduille;

g) heikentäisi merkittävästi tärkeiden järjestöjen tai toimijoiden taloudellista elinkelpoisuutta;

h) heikentäisi vakavasti unionin politiikan kehittämistä tai toimintaa tavalla, jolla on huomattavia taloudellisia tai kauppaan tai rahoitukseen liittyviä seurauksia;

— CONFIDENTIEL UE / EU CONFIDENTIAL sellaisena kuin se on määritelty tämän päätöksen 2 artiklan d kohdassa, kun tietojen vaarantuminen todennäköisesti:

a) vahingoittaisi merkittävällä tavalla diplomaattisuhteita ja esimerkiksi johtaisi virallisiin protesteihin tai muihin pakotteisiin;

b) vaarantaisi yksilön turvallisuuden tai vapauden;

c) vaarantaisi vakavasti kaupallisten tai poliittisten neuvottelujen tuloksen tai aiheuttaisi toiminnallisia ongelmia unionille tai jäsenvaltioille;

d) vahingoittaisi jäsenvaltioiden toiminnan turvallisuutta tai turvallisuus- tai tiedusteluoperaatioiden tehokkuutta;

e) heikentäisi merkittävästi tärkeiden järjestöjen tai toimijoiden taloudellista elinkelpoisuutta;

f) haittaisi rikosten tai terrorismin tutkimista tai helpottaisi niiden toteuttamista;

g) vahingoittaisi merkittävästi unionin tai jäsenvaltion rahoitukseen, rahaan, talouteen tai kauppaan liittyviä etuja;

h) heikentäisi vakavasti unionin politiikan kehittämistä tai toimintaa tavalla, jolla on huomattavia taloudellisia tai kauppaan tai rahoitukseen liittyviä seurauksia;

— RESTREINT UE / EU RESTRICTED sellaisena kuin se on määritelty tämän päätöksen 2 artiklan d kohdassa, kun tietojen vaarantuminen todennäköisesti:

a) haittaisi unionin yleistä etua;

b) vaikuttaisi kielteisesti diplomaattisuhteisiin;

c) aiheuttaisi huomattavaa haittaa yksilöille tai yrityksille;

d) haittaisi unionin tai jäsenvaltioiden kaupallisia tai poliittisia neuvotteluja;

e) vaikeuttaisi tehokkaan turvallisuuden ylläpitämistä unionissa tai jäsenvaltioissa;

f) haittaisi unionin politiikan tehokasta kehittämistä tai toteuttamista;

g) heikentäisi unionin ja sen toimien asianmukaista hallinnointia;

h) rikkoisi parlamentin antamia sitoumuksia kolmansien osapuolten toimittamien tietojen turvallisuusluokituksen ylläpitämisestä;

i) rikkoisi tietojen julkistamista koskevia sääntömääräisiä rajoituksia;

j) aiheuttaisi taloudellisia menetyksiä tai mahdollistaisi yksilöille tai yrityksille epäasianmukaisen voiton tai edun saamisen; tai

k) haittaisi rikosten tutkimista tai helpottaisi niiden tekemistä.

B.2. ***Koottujen tietojen, kansilehtien ja otteiden turvallisuusluokitus***

14. Liitteitä sisältävän kirjeen tai ilmoituksen turvallisuusluokituksen on oltava yhtä korkea kuin sen liitteille myönnetty korkein turvallisuusluokitus. Asiakirjan luovuttajan olisi ilmoitettava selvästi, mihin turvallisuusluokitukseen asiakirja on luokiteltava, jos se erotetaan liitteistään. Jos ilmoitus/kirje ei tarvitse turvallisuusluokitusta, sen lopussa on seuraavat sanat: ”Irrotettuna liitteistään tämä ilmoitus/kirje ei ole turvallisuusluokiteltu.”

15. Turvallisuusluokitukseltaan erilaisia osia sisältävien asiakirjojen tai tiedostojen rakenne määritetään mahdollisuuksien mukaan niin, että erilaiset osat ovat helposti havaittavissa ja tarvittaessa erotettavissa. Koko asiakirjan tai tiedoston turvallisuusluokituksen on oltava vähintään yhtä korkea kuin sen korkeimpaan turvallisuusluokitukseen määritellyn osan turvallisuusluokitus.

16. Tietyn asiakirjan yksittäiset sivut, kohdat, jaksot, liitteet, lisäykset, saatteet ja oheistukset saattavat edellyttää erilaisia turvallisuusluokituksia, joten ne on turvallisuusluokiteltava sen mukaisesti. EU:n turvallisuusluokiteltua tietoa sisältävissä asiakirjoissa voidaan käyttää vakiomuotoisia lyhenteitä, joilla ilmoitetaan alle yhden sivun mittaisten jaksojen tai tekstin osien turvallisuusluokitus.

17. Kun eri lähteistä peräisin olevia tietoja yhdistetään, lopputulos on tarkistettava sen kokonaisturvallisuusluokituksen määrittämiseksi, koska asiakirja voi edellyttää korkeampaa turvallisuusluokitusta kuin sen osat.

C. **MUUT LUOTTAMUKSELLISET TIEDOT**

18. Muut luottamukselliset tiedot merkitään tämän turvallisuusohjeen E kohdan ja käsittelyohjeiden mukaisesti.

D. **LUOTTAMUKSELLISTEN TIETOJEN TUOTTAMINEN**

19. Luottamuksellisia tietoja saavat tuottaa vain henkilöt, joilla on siihen asianmukainen oikeus tämän päätöksen mukaisesti tai jotka ovat saaneet luvan turvallisuusviranomaiselta.

20. Luottamuksellisia tietoja ei saa lisätä internetissä tai intranetissä olevaan asiakirjojen hallinnointijärjestelmään.

D.1. ***EU:n turvallisuusluokiteltujen tietojen tuottaminen***

21. Sellaisten EU:n turvallisuusluokiteltujen tietojen tuottaminen, joiden turvallisuusluokitus on CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE / EU SECRET tai TRÈS SECRET UE / EU TOP SECRET, edellyttää, että asianomaisella henkilöllä on siihen oikeus tämän päätöksen mukaisesti tai hänellä on tämän päätöksen 4 artiklan 1 kohdan mukainen valtuutus.

22. EU:n turvallisuusluokiteltuja tietoja, joiden turvallisuusluokitus CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE / EU SECRET tai TRÈS SECRET UE / EU TOP SECRET, voidaan tuottaa vain turvallisella alueella.

23. EU:n turvallisuusluokiteltujen tietojen luomiseen sovelletaan seuraavia sääntöjä:

a) sovellettava turvallisuusluokitus on merkittävä selvästi jokaiselle sivulle;

b) kukin sivu numeroidaan ja kullakin sivulla mainitaan sivujen kokonaismäärä;

c) asiakirjan ensimmäisellä sivulla on viitenumero ja viittaus sen käsittelemään tietoon, joka ei sinällään ole turvallisuusluokiteltua tietoa, ellei sitä ilmoiteta sellaiseksi;

d) asiakirjan ensimmäisellä sivulla on päiväys;

e) kaikkien sellaisten asiakirjojen, joiden turvallisuusluokitus on vähintään CONFIDENTIEL UE / EU CONFIDENTIAL, ensimmäisellä sivulla on luettelo kaikista liitteistä;

f) sellaisten asiakirjojen, joiden turvallisuusluokitus on CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE / EU SECRET tai TRÈS SECRET UE / EU TOP SECRET, jokaiselle sivulle on merkittävä kopion numero, jos asiakirjat on tarkoitus jakaa useampana kappaleena; kunkin kopion ensimmäisellä sivulla on myös ilmoitettava kopioiden ja sivujen kokonaismäärä; ja

g) jos asiakirjassa viitataan muihin muista unionin toimielimistä saatuihin turvallisuusluokiteltua tietoa sisältäviin asiakirjoihin tai jos asiakirja sisältää tällaisista asiakirjoista peräisin olevaa turvallisuusluokiteltua tietoa, asiakirjalla on oltava sama turvallisuusluokitustaso kuin näillä asiakirjoilla, eikä sitä saa jakaa ilman sen luovuttajan etukäteen antamaa kirjallista lupaa kellekään muille kuin turvallisuusluokiteltua tietoa sisältävän alkuperäisen asiakirjan tai asiakirjojen jakeluluettelossa mainituille henkilöille.

24. EU:n turvallisuusluokitellun asiakirjan hallinta säilyy sen laatineella luovuttajalla. Tarvitaan luovuttajan etukäteen antama kirjallinen lupa, ennen kuin:

a) EU:n turvallisuusluokitellun asiakirjan luokitusta alennetaan tai se poistetaan;

b) EU:n turvallisuusluokiteltua asiakirjaa käytetään muihin kuin luovuttajan määrittämiin tarkoituksiin;

c) se paljastetaan kolmannelle maalle tai kansainväliselle organisaatiolle;

d) se paljastetaan henkilölle, laitokselle, maalle tai kansainväliselle organisaatiolle, joka ei sellaisiin kohderyhmiin, joille luovuttaja on alun perin antanut luvan tutustua asianomaisiin tietoihin;

e) se paljastetaan kolmannessa maassa sijaitsevalle sopimuspuolelle tai mahdolliselle sopimuspuolelle;

f) se kopioidaan tai käännetään, jos tietojen turvallisuusluokitus on TRES SECRET UE / EU TOP SECRET;

g) se tuhotaan.

D.2. ***Muiden luottamuksellisten tietojen tuottaminen***

25. Turvallisuusviranomaisena toimiva pääsihteeri voi päättää, annetaanko tietylle toimelle, yksikölle ja/tai henkilölle lupa muiden luottamuksellisten tietojen tuottamiseen.

26. Muilla luottamuksellisilla tiedoilla on jokin käsittelyohjeissa määritetyistä merkinnöistä.

27. Muiden luottamuksellisten tietojen tuottamiseen sovelletaan seuraavia sääntöjä:

a) tietojen merkintä on asiakirjan ensimmäisen sivun yläosassa;

b) kukin sivu numeroidaan ja kullakin sivulla mainitaan sivujen kokonaismäärä;

c) asiakirjan ensimmäisellä sivulla on viitenumero ja viittaus sen sisältöön;

d) asiakirjan ensimmäisellä sivulla on päiväys ja

e) asiakirjan viimeisellä sivulla on luettelo kaikista sen liitteistä.

28. Muiden luottamuksellisten tietojen tuottamiseen sovelletaan käsittelyohjeiden mukaisia erityisiä sääntöjä ja menettelyjä.

E. **TURVALLISUUSOSOITTIMET JA -MERKINNÄT**

29. Asiakirjojen turvallisuusosoittimilla ja -merkinnöillä pyritään valvomaan tiedonkulkua ja rajoittamaan pääsyä luottamuksellisiin tietoihin tiedonsaantitarpeen periaatteen mukaan.

30. Kun turvallisuusosoittimia ja/tai -merkintöjä käytetään, on pyrittävä välttämään sekaannusta seuraavissa EU:n turvallisuusluokiteltuja tietoja koskevissa turvallisuusluokituksissa: RESTREINT UE / EU RESTRICTED, CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE / EU SECRET, TRES SECRET UE / EU TOP SECRET.

31. Käsittelyohjeissa säädetään erityissäännöistä, jotka koskevat turvallisuusosoittimia ja -merkintöjä sekä Euroopan parlamentin hyväksymistä turvallisuusmerkinnöistä.

E.1. ***Turvallisuusosoittimet***

32. Turvallisuusosoittimia voidaan käyttää ainoastaan yhdessä turvallisuusluokituksen kanssa, eikä niitä voida soveltaa erillisesti asiakirjoihin. Turvallisuusosoitinta voidaan soveltaa EU:n turvallisuusluokiteltuihin tietoihin seuraavissa tapauksissa:

a) turvallisuusluokituksen kelpoisuuden rajaamiseksi (turvallisuusluokitellun tiedon osalta tämä merkitsee luokituksen automaattista alentamista tai poistamista);

b) asianomaisten EU:n turvallisuusluokiteltujen tietojen levityksen rajoittamiseksi;

c) erityisten käsittelyjärjestelyjen määrittelemiseksi turvallisuusluokittelun mukaisen käsittelyn lisäksi.

33. EU:n turvallisuusluokiteltujen tietojen käsittelyyn ja säilytykseen sovellettavat ylimääräiset valvontatoimet aiheuttavat lisärasitteita kaikille asianosaisille. Tähän liittyvän työn minimoimiseksi katsotaan tällaista asiakirjaa laadittaessa hyväksi käytännöksi määritellä aikaraja tai muu tapahtuma, jonka jälkeen luokitus automaattisesti raukeaa ja asiakirjan sisältämien tietojen turvallisuusluokitus alentuu tai poistuu.

34. Jos asiakirja koskee tiettyä tehtäväkenttää ja sen levitystä on rajoitettava ja/tai siihen sovelletaan erityisiä käsittelyjärjestelyjä, asiaa koskeva lausunto on lisättävä sen turvallisuusluokitukseen kohdeyleisön määrittämiseksi.

E.2. ***Merkinnät***

35. Merkinnät eivät ole osa turvallisuusluokitusta. Niillä pyritään vain tarjoamaan konkreettisia ohjeita asiakirjan käsittelyä varten eikä niitä pidä käyttää kuvailemaan kyseisen asiakirjan sisältöä.

36. Merkintöjä voidaan soveltaa erikseen asiakirjoihin tai käyttää yhdessä turvallisuusluokituksen kanssa.

37. Pääsääntöisesti merkintöjä sovelletaan tietoihin, jotka kuuluvat Euroopan unionin toiminnasta tehdyn sopimuksen 339 artiklassa ja henkilöstösääntöjen 17 artiklassa tarkoitetun salassapitovelvollisuuden piiriin tai joita parlamentin on suojeltava oikeudellisista syistä, mutta joita ei tarvitse tai ei voi luokitella.

E.3. ***Merkintöjen käyttö viestintä- ja tietojärjestelmissä***

38. Sääntöjä merkintöjen käytöstä sovelletaan myös hyväksytyn viestintä- ja tietojärjestelmän piirissä.

39. Turvallisuusjärjestelyt hyväksyvä viranomainen laatii erityiset säännöt hyväksytyn viestintä- ja tietojärjestelmän piirissä sovellettavista merkinnöistä.

F. **TIETOJEN VASTAANOTTO**

40. Parlamentissa ainoastaan turvallisuusluokiteltujen tietojen yksiköllä on oikeus vastaanottaa kolmansilta osapuolilta tietoja, joiden turvallisuusluokitus on CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE / EU SECRET tai TRÈS SECRET UE / EU TOP SECRET tai vastaava.

41. Turvallisuusluokiteltujen tietojen yksikkö tai asiasta vastaava parlamentin elin / asiasta vastaavassa parlamentin elimessä toimiva jäsen voivat vastaanottaa kolmansilta osapuolilta tietoja, joiden turvallisuusluokitus on RESTREINT UE / EU RESTRICTED tai vastaava, tai muuta luottamuksellista tietoa, ja soveltaa tässä turvallisuusohjeessa määriteltyjä periaatteita.

G. **KIRJAAMINEN**

42. Kirjaaminen tarkoittaa sellaisten menettelyjen soveltamista, joiden avulla tallennetaan luottamuksellisten tietojen elinkaari, mukaan lukien niiden jakelu, niihin tutustuminen ja niiden hävittäminen.

43. Tässä turvallisuusohjeessa ”päiväkirja” tarkoittaa rekisteriä, johon tallennetaan erityisesti ne päivämäärät ja ajankohdat, jolloin luottamukselliset tiedot

a) saapuvat parlamentin elimen / parlamentin elimessä toimivan jäsenen sihteeristöön tai turvallisuusluokiteltujen tietojen yksikköön tai lähtevät sieltä;

b) ovat valtuutetun henkilön käyttäminä tai tälle lähetettyinä; ja

c) on tuhottu.

44. Turvallisuusluokiteltujen tietojen luovuttaja on vastuussa näitä tietoja sisältävän asiakirjan laatimista koskevan ensimmäisen vakuutuksen merkitsemisestä. Kyseinen vakuutus ilmoitetaan turvallisuusluokiteltujen tietojen yksikköön asiakirjaa laadittaessa.

45. Turvallisuusluokiteltujen tietojen yksikkö voi kirjata tiedot, joiden turvallisuusluokitus on CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE / EU SECRET tai TRÈS SECRET UE / EU TOP SECRET tai vastaava, vain turvallisuuteen liittyvissä tapauksissa. Kolmansilta osapuolilta vastaanotettujen tietojen, joiden turvallisuusluokitus on RESTREINT UE / EU RESTRICTED tai vastaava tai jotka ovat muuta luottamuksellista tietoa, kirjaamisen suorittaa hallinnollisista syistä asiakirjan virallisesti vastaanottanut yksikkö, eli turvallisuusluokiteltujen tietojen yksikkö tai parlamentin elimen / parlamentin elimessä toimivan jäsenen sihteeristö. Parlamentissa tuotetun muun luottamuksellisen tiedon kirjaamisen suorittaa hallinnollisista syistä tiedon luovuttaja.

46. Tiedot, joiden turvallisuusluokitus on CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE / EU SECRET tai TRÈS SECRET UE / EU TOP SECRET tai vastaava, kirjataan erityisesti silloin, kun

a) ne tuotetaan;

b) kun ne saapuvat turvaluokiteltujen tietojen yksikköön tai lähtevät sieltä; ja

c) kun ne saapuvat viestintä- ja tietojärjestelmään tai lähtevät sieltä.

47. Tiedot, joiden turvallisuusluokitus on RESTREINT UE / EU RESTRICTED tai vastaava, kirjataan erityisesti silloin, kun

a) ne tuotetaan;

b) ne saapuvat parlamentin elimen / parlamentin elimessä toimivan jäsenen sihteeristöön tai turvallisuusluokiteltujen tietojen yksikköön tai lähtevät sieltä; ja

c) kun ne saapuvat viestintä- ja tietojärjestelmään tai lähtevät sieltä.

48. Luottamuksellisten tietojen kirjaaminen voidaan tehdä paperimuodossa tai sähköisessä muodossa oleviin päiväkirjoihin tai viestintä- ja tietojärjestelmään.

49. Tiedoista, joiden turvallisuusluokitus on RESTREINT EU / EU RESTRICTED tai vastaava, ja muista luottamuksellista tiedoista on kirjattava ainakin seuraavat seikat:

a) päivämäärä ja kellonaika, jolloin tiedot saapuvat parlamentin elimen / parlamentin elimessä toimivan jäsenen sihteeristöön tai turvallisuusluokiteltujen tietojen yksikköön tai lähtevät sieltä;

b) asiakirjan otsikko, turvallisuusluokitus tai merkintä, turvallisuusluokituksen/merkinnän päättymisajankohta ja asiakirjalle annettu viitenumero.

50. Tiedoista, joiden turvallisuusluokitus on CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE / EU SECRET tai TRÈS SECRET UE / EU TOP SECRET tai vastaava, on rekisteröitävä ainakin seuraavat seikat:

a) päivämäärä ja kellonaika, jolloin tiedot saapuvat turvallisuusluokiteltujen tietojen yksikköön tai lähtevät sieltä;

b) asiakirjan otsikko, turvallisuusluokitus tai merkintä, turvallisuusluokituksen/merkinnän päättymisajankohta ja asiakirjalle annettu viitenumero.

c) luovuttajaa koskevat tiedot;

d) tiedot siitä, kenellä on oikeus käsitellä asiakirjaa ja milloin kyseinen henkilö käsitteli sitä;

e) asiakirjan mahdollisia kopioita tai käännöksiä koskevat tiedot;

f) päivämäärä ja kellonaika, jolloin turvallisuusluokiteltu tieto tai sen kopio tai käännös lähtee turvallisuusluokiteltujen tietojen yksiköstä tai palaa sinne takaisin, ja tiedot siitä, mihin se on lähetetty ja kuka sen on palauttanut;

g) päivämäärä ja kellonaika, jolloin asiakirja on tuhottu ja kuka sen on tuhonnut, tuhoamista koskevien parlamentin turvallisuussääntöjen mukaisesti ja

h) asiakirjan turvallisuusluokan poistaminen tai alentaminen.

51. Päiväkirjat voidaan turvallisuusluokitella tai merkitä tarpeen mukaan. Tietoja, joiden turvallisuusluokitus on TRES SECRET UE / EU TOP SECRET tai vastaava, koskevat päiväkirjat kirjataan samalle tasolle.

52. Turvallisuusluokitellut tiedot voidaan kirjata:

a) yhteen päiväkirjaan tai

b) erillisiin päiväkirjoihin seuraavien tietojen mukaan: niiden turvallisuusluokitus, niiden asema tulevina tai lähtevinä tietoina ja niiden lähtö- tai määräpaikka.

53. Viestintä- ja tietojärjestelmässä tapahtuvassa sähköisessä tietojenkäsittelyssä kirjaamismenettelyt voidaan toteuttaa viestintä- ja tietojärjestelmän omilla keinoilla edellyttäen, että ne ovat edellä esitettyjen vaatimusten mukaisia. Jos EU:n turvallisuusluokitellut tiedot poistetaan viestintä- ja tietojärjestelmästä, sovelletaan edellä kuvattua kirjaamismenettelyä.

54. Turvallisuusluokiteltujen tietojen yksikkö pitää kirjaa kaikista parlamentin kolmansille valtioille luovuttamista turvallisuusluokitelluista tiedoista sekä kaikista kolmansilta valtioilta vastaanotetuista turvallisuusluokitelluista tiedoista.

55. Kun sellaisten tietojen, joiden turvallisuusluokitus on CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE / EU SECRET tai TRÈS SECRET UE / EU TOP SECRET tai vastaava, kirjaaminen on suoritettu, turvallisuusluokiteltujen tietojen yksikkö tarkistaa, onko vastaanottajalla tarvittava turvallisuusluokitus. Jos turvallisuusluokitus on voimassa, turvallisuusluokiteltujen tietojen yksikkö ilmoittaa asiasta vastaanottajalle. Turvallisuusluokiteltuihin tietoihin voi tutustua vasta kun asiakirja on kirjattu.

H. **JAKELU**

56. Tietojen luovuttaja perustaa alustavan jakelulistan laatimilleen EU:n turvallisuusluokitelluille tiedoille.

57. Tietojen luovuttaja vastaa turvallisuusluokituksen RESTREINT UE / EU RESTRICTED ja muiden parlamentin tuottamien luottamuksellisten tietojen jakelusta parlamentissa käsittelysääntöjen ja tiedonsaantitarpeen periaatteen mukaisesti. Turvallisuusluokiteltujen tietojen yksikkö on vastuussa sellaisten tietojen hallinnoinnista, jotka on tuotettu parlamentissa turvallisella alueella ja joiden turvallisuusluokitus on CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE / EU SECRET tai TRÈS SECRET UE / EU TOP SECRET, ja se laatii niiden jakelulistan (ja tarvittaessa niiden jakelua koskevat lisäohjeet).

58. Ainoastaan turvallisuusluokiteltujen tietojen yksikkö voi jakaa kolmansille osapuolille parlamentin tuottamia EU:n turvallisuusluokiteltuja tietoja tiedonsaantitarpeen periaatteen mukaisesti.

59. Turvallisuusluokiteltujen tietojen yksikön tai pyynnön esittäneen parlamentin elimen tai parlamentin elimessä toimivan jäsenen sihteeristön vastaanottamat luottamukselliset tiedot on jaettava tietojen luovuttajalta saatujen ohjeiden mukaisesti.

I. **TIETOJEN KÄSITTELY, SÄILYTTÄMINEN JA NIIHIN TUTUSTUMINEN**

60. Luottamuksellisten tietojen käsittely, säilyttäminen ja niihin tutustuminen suoritetaan turvallisuusohjeen 4:n ja käsittelyohjeiden mukaisesti.

J. **TURVALLISUUSLUOKITELTUJEN TIETOJEN KOPIOINTI, KÄÄNTÄMINEN JA TULKKAUS**

61. Asiakirjoja, joiden sisältämien tietojen turvallisuusluokitus on TRÈS SECRET UE / EU TOP SECRET tai vastaava, ei saa kopioida tai kääntää ilman luovuttajan etukäteen antamaa kirjallista hyväksyntää. Asiakirjoja, joiden sisältämien tietojen turvallisuusluokitus on SECRET UE / EU SECRET tai CONFIDENTIEL UE / EU CONFIDENTIAL tai vastaava, voidaan jäljentää tai kääntää haltijan pyynnöstä edellyttäen, ettei luovuttaja ole kieltänyt sitä.

62. Asiakirjoja, joiden sisältämien tietojen turvallisuusluokitus on TRES SECRET UE / EU TOP SECRET, SECRET UE / EU SECRET tai CONFIDENTIEL UE / EU CONFIDENTIAL tai vastaava, kaikki kopiot on kirjattava.

63. Kopioihin ja käännöksiin sovelletaan alkuperäisen asiakirjan sisältämiä luokiteltuja tietoja koskevia turvallisuustoimia.

64. Neuvostolta vastaanotetut tiedot olisi saatava kaikilla virallisilla kielillä.

65. Tietojen luovuttaja tai kopion haltija voi pyytää turvallisuusluokiteltuja tietoja sisältävien asiakirjojen kopioita ja/tai käännöksiä. Asiakirjojen, joiden sisältämien tietojen turvallisuusluokitus on CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE / EU SECRET tai TRES SECRET UE / EU TOP SECRET tai vastaava, kopioita voidaan tuottaa ainoastaan turvallisella alueella ja sellaisilla kopiokoneilla, jotka ovat osa hyväksyttyä viestintä- ja tietojärjestelmää. Asiakirjojen, joiden sisältämien tietojen turvallisuusluokitus on RESTREINT UE / EU RESTRICTED tai vastaava, kopioita voidaan tehdä parlamentin tiloissa hyväksytyllä kopiokoneella.

66. Kaikki luottamuksellisia tietoja sisältävien asiakirjojen tai niiden osien kopiot ja käännökset on merkittävä, numeroitava ja kirjattava asianmukaisesti.

67. Kopioita ei saa tehdä enempää kuin on välttämättä tarpeen. Kaikki kopiot on tuhottava käsittelyohjeiden mukaisesti tutustumisjakson päätyttyä.

68. Ainoastaan ne tulkit ja kääntäjät, jotka ovat parlamentin virkamiehiä, saavat tutustua turvallisuusluokiteltuun aineistoon.

69. Asiakirjoihin, joiden sisältämien tietojen turvallisuusluokitus on CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE / EU SECRET tai TRES SECRET UE / EU TOP SECRET tai vastaava, tutustuvilla tulkeilla ja kääntäjillä on oltava asianmukainen luotettavuusselvitys.

70. Asiakirjojen, joiden sisältämien tietojen turvallisuusluokitus on CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE / EU SECRET tai TRES SECRET UE / EU TOP SECRET tai vastaava, parissa työskentelevien tulkkien ja kääntäjien on työskenneltävä turvallisessa tilassa.

K. LUOTTAMUKSELLISTEN TIETOJEN TURVALLISUUSLUOKITUKSEN ALENTAMINEN JA POISTAMINEN JA MERKINNÄN POISTAMINEN

K.1. *Yleisperiaatteet*

71. Luottamuksellisten tietojen turvallisuusluokitus on alennettava, poistettava tai merkintä on poistettava, kun suojaus ei enää ole tarpeen tai sitä ei enää tarvita alkuperäisellä tasolla.

72. Päätökset parlamentissa laadittuihin asiakirjoihin sisältyvien tietojen turvallisuusluokituksen alentamisesta, poistamisesta tai niiden merkinnän poistamisesta voidaan tehdä myös ad hoc -periaatteella esimerkiksi vastauksena suurelta yleisöltä tai toiselta unionin toimielimeltä saatuun pyyntöön tai turvallisuusluokiteltujen tietojen yksikön tai parlamentin elimen tai parlamentin elimessä toimivan jäsenen aloitteeseen.

73. EU:n turvallisuusluokiteltuja tietoja tuottaessaan luovuttajan on mahdollisuuksien mukaan ilmoitettava, voidaanko EU:n turvallisuusluokiteltujen tietojen turvallisuusluokitusta alentaa tai turvallisuusluokitus poistaa tiettynä päivänä tai tietyn tapahtuman jälkeen. Ellei tällaisen ilmoituksen antaminen ole käytännössä mahdollista, tietojen luovuttaja, turvallisuusluokiteltujen tietojen yksikkö tai parlamentin elin tai parlamentin elimessä toimiva jäsen tarkastelee uudelleen EU:n turvallisuusluokiteltujen tietojen turvallisuusluokitusta vähintään viiden vuoden välein. Kaikissa tapauksissa EU:n turvallisuusluokiteltujen tietojen turvallisuusluokitus voidaan alentaa tai poistaa ainoastaan tiedon luovuttajan kirjallisella etukäteissuostumuksella.

74. Jos parlamentissa laadittuihin asiakirjoihin sisältyvien EU:n turvallisuusluokiteltujen tietojen luovuttajaa ei pystytä nimeämään tai jäljittämään, turvallisuusviranomainen arvioi uudelleen kyseessä olevien EU:n turvallisuusluokiteltujen tietojen turvallisuusluokituksen tasoa tietoja hallussaan pitävän parlamentin elimen tai parlamentin elimessä toimivan jäsenen ehdotuksesta ja kuulee turvallisuusluokiteltujen tietojen yksikköä tarvittaessa.

75. Tietoja hallussaan pitävällä turvallisuusluokiteltujen tietojen yksiköllä tai parlamentin elimellä tai parlamentin elimessä toimivalla jäsenellä on velvollisuus kertoa vastaanottajalle tai vastaanottajille tietojen turvallisuusluokituksen alentamisesta tai poistamisesta, ja kyseisellä vastaanottajalla tai vastaanottajilla on puolestaan velvollisuus ilmoittaa niille mahdollisille vastaanottajille, joille he ovat lähettäneet tai kopioineet asiakirjan.

76. Asiakirjaan sisältyvien tietojen turvallisuusluokituksen poistaminen, alentaminen tai merkinnän poistaminen on kirjattava.

K.2. *Turvallisuusluokituksen poistaminen*

77. EU:n turvallisuusluokitus voidaan poistaa kokonaan tai osittain. Se voidaan poistaa osittain silloin, kun suojausta ei enää pidetä tarpeellisena asiakirjan tietyn osan kannalta, mutta se on yhä perusteltua asiakirjan muiden osien kannalta.

78. Kun parlamentissa laadittuun asiakirjaan sisältyvien EU:n turvallisuusluokiteltujen tietojen uudelleenarviointi on johtanut päätökseen niiden turvallisuusluokituksen poistamisesta, on harkittava voidaanko asiakirjan julkistaa vai laitetaanko siihen jakelumerkintä (eli sitä ei julkisteta).

79. Kun EU:n turvallisuusluokiteltujen tietojen turvallisuusluokitus poistetaan, poistaminen kirjataan päiväkirjaan seuraavien tietojen kera: turvallisuusluokituksen poistamisen päivämäärä, poistamista pyytäneiden ja poistamisen hyväksyneiden henkilöiden nimet, sen asiakirjan viitenumero ja lopullinen määräpaikka, jonka turvallisuusluokitus on poistettu.

80. Asiakirjasta, jonka turvallisuusluokitus on poistettu, ja kaikista siitä otetuista kopioista on yliviivattava vanhat luokitusmerkinnät. Asiakirjat ja kaikki sen kopiot on varastoitava asianmukaisesti.

81. Jos turvallisuusluokitellun asiakirjan luokitus poistetaan osittain, asiakirjasta on tuotettava turvallisuusluokittelematon ote, jota on säilytettävä asianmukaisesti. Toimivaltaisen yksikön on kirjattava

a) osittaisen turvallisuusluokituksen poistamisen päivämäärä;

b) poistamista pyytäneiden ja poistamisen hyväksyneiden henkilöiden nimet; ja

c) sen asiakirjan viitenumero, jonka turvallisuusluokitus on poistettu.

K.3. ***Turvallisuusluokituksen alentaminen***

82. Turvallisuusluokituksen alentamisen jälkeen kyseinen asiakirja kirjataan päiväkirjoihin sekä vanhaa että uutta turvallisuusluokitusta vastaavasti. Turvallisuusluokituksen alentamispäivämäärä ja alentamiseen luvan antaneen henkilön nimi on kirjattava.

83. Turvallisuusluokitukseltaan alennettuun asiakirjaan ja kaikkiin siitä otettuihin kopioihin on merkittävä uusi turvallisuusluokitus, ja niitä on säilytettävä asianmukaisesti

L. **LUOTTAMUKSELLISTEN TIETOJEN TUHOAMINEN**

84. Luottamukselliset tiedot (joko painetussa tai sähköisessä muodossa), joita ei enää tarvita, tuhotaan tai poistetaan käsittelyohjeiden ja arkistointia koskevien sääntöjen mukaisesti.

85. Tiedot, joiden turvallisuusluokitus on TRÈS SECRET UE / EU TOP SECRET tai vastaava tai SECRET UE / EU SECRET tai vastaava, tuhotaan turvallisuusluokiteltujen tietojen yksikössä. Tuhoaminen tapahtuu sellaisen henkilön todistamana, jonka turvallisuusluokitus vastaa vähintään tuhottavien tietojen turvallisuusluokituksen tasoa.

86. Tiedot, joiden turvallisuusluokitus on TRÈS SECRET UE / EU TOP SECRET tai vastaava, tuhotaan vain tietojen luovuttajan etukäteen antaman kirjallisen hyväksynnän perusteella.

87. Tiedot, joiden turvallisuusluokitus on CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE / EU SECRET tai TRES SECRET UE / EU TOP SECRET tai vastaava, tuhotaan ja hävitetään vain turvallisuusluokiteltujen tietojen yksikössä tietojen luovuttajan tai toimivaltaisen viranomaisen määräyksestä. Päiväkirjat ja muut rekisterit on päivitettävä vastaavasti. Turvallisuusluokiteltujen tietojen yksikkö tai parlamentin elimen tai yksikön viranhaltija tuhoaa ja hävittää tiedot, joiden turvallisuusluokitus on RESTREINT UE / EU RESTRICTED tai vastaava.

88. Tuhoamisen suorittaneen virkamiehen ja tuhoamisen todistajan on allekirjoitettava tuhoamistodistus, joka tallennetaan turvallisuusluokiteltujen tietojen yksikköön. Yksikkö säilyttää tiedot, joiden turvallisuusluokitus on TRES SECRET UE / EU TOP SECRET tai vastaava, vähintään kymmenen vuoden ajan sekä tiedot, joiden turvallisuusluokitus on SECRET UE / EU SECRET tai vastaava ja CONFIDENTIEL UE / EU CONFIDENTIAL tai vastaava, vähintään viiden vuoden ajan yhdessä jakelulomakkeiden ja tuhoamistodistusten kanssa.

89. Turvallisuusluokiteltuja tietoja sisältävä asiakirja tuhotaan menetelmillä, jotka ovat asiaa koskevien unionin normien tai vastaavien normien mukaisia, jotta estettäisiin tietojen kokoaminen uudelleen kokonaan tai osittain.

90. Turvallisuusluokiteltua tietoa varten käytetyn atk-tallennusvälineen tuhoaminen suoritetaan asiaa koskevien käsittelyohjeiden mukaisesti.

91. Turvallisuusluokiteltujen tietojen tuhoamisesta on kirjattava asiaankuuluvaan päiväkirjaan seuraavat tiedot:

a) tuhoamisen päivämäärä ja aika;

b) tuhoamisesta vastaavan virkamiehen nimi;

c) tuhotun asiakirjan tai sen kopioiden tunniste;

d) EU:n turvallisuusluokiteltujen tietojen alkuperäinen fyysinen tallennusmuoto;

e) tuhoamistapa ja

f) tuhoamispaikka.

M. **ARKISTOINTI**

92. Turvallisuusluokitellut tiedot, mukaan luettuna mahdolliset ilmoitus/kirje, liitteet, siirtokuitti ja muut asiakirja-aineiston osat siirretään turvallisella alueella olevaan turvalliseen arkistoon kuusi kuukautta viimeisen tutustumisen jälkeen ja viimeistään yhden vuoden kuluttua siirrosta. Turvallisuusluokiteltujen tietojen arkistoinnista säädetään yksityiskohtaisemmin käsittelyohjeissa.

93. Muiden luottamuksellisten tietojen suhteen sovelletaan asiakirjojen käsittelyä koskevia yleisiä sääntöjä sen kuitenkaan rajoittamatta muita erityismääräyksiä luottamuksellisten tietojen käsittelystä.

TURVALLISUUSOHJE 3

LUOTTAMUKSELLISTEN TIETOJEN KÄSITTELY AUTOMAATTISISSA VIESTINTÄ- JA TIETOJÄRJESTELMISSÄ

A. **TIETOJÄRJESTELMISSÄ KÄSITELTYJEN TURVALLISUUSLUOKITELTUJEN TIETOJEN TURVAAMINEN**

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

2. Viestintä- ja tietojärjestelmällä tarkoitetaan turvallisuusluokiteltujen tietojen käsittelyssä järjestelmää, joka mahdollistaa tietojen käsittelyn sähköisessä muodossa. Viestintä- ja tietojärjestelmä käsittää kaikki toimintansa kannalta tarpeelliset resurssit, myös infrastruktuurin, organisaation, henkilöstön ja tietoresurssit.

3. Viestintä- ja tietojärjestelmissä on käsiteltävä turvallisuusluokiteltuja tietoja tietojen turvaamisen periaatteen mukaisesti.

4. Viestintä- ja tietojärjestelmien on läpikäytävä hyväksymisprosessi. Hyväksymisellä pyritään varmistamaan, että kaikki asiaankuuluvat turvatoimet on pantu täytäntöön ja että on saavutettu riittävä turvallisuusluokiteltujen tietojen ja viestintä- ja tietojärjestelmän suojaustaso tämän turvallisuusilmoituksen mukaisesti. Hyväksymislausunnossa on määriteltävä niiden tietojen korkein sallittu turvallisuusluokitus, joita viestintä- ja tietojärjestelmässä voidaan käsitellä, ja sitä koskevat ehdot ja edellytykset.

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

a) aitous: tae siitä, että tiedot ovat aitoja ja peräisin vilpittömistä lähteistä;

b) käytettävyys: ominaisuus, että tiedot ovat pyynnöstä valtuutetun yksikön saatavilla ja käytettävissä;

c) luottamuksellisuus: ominaisuus, että tietoja ei saa paljastaa sivullisille henkilöille, yksiköille eikä prosesseille;

d) eheys: ominaisuus, että tietojen ja resurssien oikeellisuus ja täydellisyys turvataan;

e) kiistämättömyys: kyky todistaa tietyn toimen tai tapahtuman olemassaolo niin, ettei tapahtumaa tai toimea voida myöhemmin kiistää.

B. **TIEDONTURVAAMISPERIAATTEET**

6. Jäljempänä esitetyt säännökset muodostavat kaikkien turvallisuusluokiteltuja tietoja käsittelevien viestintä- ja tietojärjestelmien turvallisuuden lähtökohdan. Säännösten täytäntöönpanoa koskevat yksityiskohtaiset vaatimukset määritellään tietojen turvaamista koskevissa turvallisuusperiaatteissa ja turvallisuutta koskevissa suuntaviivoissa.

B.1. ***Turvallisuusriskien hallinta***

7. Turvallisuusriskien hallinnan on oltava erottamaton osa viestintä- ja tietojärjestelmän määrittelyä, kehittämistä, käyttöä ja ylläpitoa. Riskinhallinta (arviointi, käsittely, hyväksyminen ja viestintä) on toteutettava iteroivana prosessina, järjestelmän omistajien edustajien, hankkeesta vastaavien viranomaisten, toiminnasta vastaavien viranomaisten ja turvallisuusohjeessa 1 tarkoitettujen, turvallisuusjärjestelyt hyväksyvien viranomaisten on osallistuttava toteuttamiseen, ja siinä on käytettävä vakiintunutta, avointa ja täysin ymmärrettävää riskinarviointiprosessia. Viestintä- ja tietojärjestelmän laajuus ja resurssit on määriteltävä selkeästi riskinhallintaprosessin aluksi.

8. Turvallisuusohjeessa 1 tarkoitettujen toimivaltaisten viranomaisten on tarkasteltava viestintä- ja tietojärjestelmiin mahdollisesti kohdistuvia uhkia ja pidettävä yllä ajantasaisia ja tarkkoja uhka-arvioita, jotka perustuvat ajankohtaiseen toimintaympäristöön. Niiden on jatkuvasti päivitettävä haavoittuvuusasioita koskevia tietojaan ja tarkistettava säännöllisin väliajoin haavoittuvuusarviota mukautuakseen muuttuvaan tietotekniikkaympäristöön.

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

10. Viestintä- ja tietojärjestelmän hyväksyntään on liitettävä vastaavan viranomaisen virallinen lausunto jäännösriskistä ja sen hyväksymisestä. Asiaankuuluvan turvallisuusjärjestelyt hyväksyvän viranomaisen viestintä- ja tietojärjestelmän hyväksymistä varten määrittämät erityiset vaatimukset, laajuus ja yksityiskohtaisuus on suhteutettava arvioituun riskiin ottaen huomioon kaikki asiaankuuluvat tekijät, myös viestintä- ja tietojärjestelmässä käsiteltyjen turvallisuusluokiteltujen tietojen turvallisuusluokitus.

B.2. ***Turvallisuus viestintä- ja tietojärjestelmän koko elinkaaren ajan***

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

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

13. Viestintä- ja tietojärjestelmän turvallisuus, myös sen tekniset ja muut kuin tekniset turvatoimet, on testattava hyväksymisprosessin aikana sen varmistamiseksi, että asianmukainen turvaamistaso saavutetaan, ja sen tarkistamiseksi, että viestintä- ja tietojärjestelmä, myös sen tekniset ja muut kuin tekniset turvatoimet, on moitteettomasti toteutettu, integroitu ja konfiguroitu.

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

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

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

B.3. ***Parhaat toimintatavat***

17. Tiedonturvaamisviranomaisen on kehitettävä parhaita toimintatapoja viestintä- ja tietojärjestelmissä käsiteltävien turvallisuusluokiteltujen tietojen suojelemiseksi. Parhaita toimintatapoja koskevissa suuntaviivoissa on vahvistettava viestintä- ja tietojärjestelmiä koskevat tekniset, fyysiset, organisatoriset ja menettelyyn liittyvät turvatoimet, joiden tehokkuus tiettyjen uhkien ja haavoittuvuuden torjumisessa on todistettu.

18. Viestintä- ja tietojärjestelmissä käsiteltävien EU:n turvallisuusluokiteltujen tietojen suojaamisessa on hyödynnettävä tietojen turvaamisessa mukana olevien tahojen kokemuksia.

19. Parhaiden toimintatapojen levittämisen ja niiden myöhemmän täytäntöönpanon on edesautettava yhtäläisen turvaamistason aikaansaamista parlamentin sihteeristön käyttämissä viestintä- ja tietojärjestelmissä, joissa käsitellään turvallisuusluokiteltuja tietoja.

B.4. ***Monitasoinen turvallisuus***

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

a) pelote: turvatoimet, joilla pyritään saamaan mahdolliset viholliset luopumaan suunnittelemasta hyökkäystä viestintä- ja tietojärjestelmää vastaan;

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

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

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

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

Tällaisten turvatoimien pakollisuusaste on määriteltävä riskinarvioinnin perusteella.

21. Toimivaltaisten viranomaisten on turvallisuusohjeen 1:n mukaisesti varmistettava, että ne voivat käsitellä poikkeuksellisia tapahtumia, jotka saattavat ulottua organisaatioiden ulkopuolelle, jotta voidaan koordinoida vastatoimia ja jakaa tapahtumia ja niihin liittyviä riskejä koskevat tiedot kolmansien osapuolten kanssa (tietotekniset hätävalmiudet).

B.5. ***Vähimmäistoimintojen ja pienimmän mahdollisen etuoikeuden periaate***

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

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

B.6. ***Tietoisuus tietojen turvaamisesta***

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

a) että turvallisuuden vaarantuminen voi merkittävästi vahingoittaa viestintä- ja tietojärjestelmiä, joissa käsitellään turvaluokiteltuja tietoja;

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

c) että heillä on henkilökohtainen vastuu ja tilivelvollisuus viestintä- ja tietojärjestelmien turvallisuudesta sen mukaan, mikä on heidän tehtävänsä järjestelmissä ja prosesseissa.

25. Sen varmistamiseksi, että turvallisuuteen liittyvät tehtävät ymmärretään, koko henkilöstölle, myös johtohenkilöstölle, Euroopan parlamentin jäsenille ja viestintä- ja tietojärjestelmien käyttäjille, on annettava pakollinen tiedonturvaamista ja tietoisuuden lisäämistä koskeva koulutus.

B.7. ***Tietoturvallisuustuotteiden arviointi ja hyväksyntä***

26. Viestintä- ja tietojärjestelmät, joissa käsitellään tietoja, joiden turvallisuusluokitus on CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE / EU SECRET tai TRÈS SECRET UE / EU TOP SECRET tai vastaava, on suojattava niin, etteivät tahattomat sähkömagneettiset vuodot vaaranna tietoja (TEMPEST-turvatoimet).

27. Jos EU:n turvallisuusluokiteltujen tietojen suojaamiseen käytetään salaustuotteita, turvallisuusjärjestelyistä vastaavan viranomaisen on hyväksyttävä tällaiset tuotteet on EU:n hyväksymiksi salaustuotteiksi.

28. Lähetettäessä turvallisuusluokiteltuja tietoja sähköisesti on käytettävä EU:n hyväksymiä salaustuotteita. Tästä vaatimuksesta poiketen poikkeuksellisissa olosuhteissa voidaan soveltaa erityisiä menettelyjä tai erityisiä teknisiä määrityksiä 41–44 kohdan mukaisesti.

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

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

31. Turvallisuusjärjestelyistä vastaava viranomainen hyväksyy ohjeet muiden tietoturvallisuustuotteiden kuin salaustuotteiden luokittelun ja hyväksynnän turvallisuudesta.

B.8. ***Tietojen lähettäminen turvallisella alueella***

32. Jos turvallisuusluokiteltujen tietojen lähettäminen tapahtuu turvallisella alueella, salaamatonta jakelua tai alemman tason salausta voidaan käyttää riskinhallintaprosessin tulosten perusteella ja turvallisuusjärjestelyt hyväksyvän viranomaisen luvalla.

B.9. ***Viestintä- ja tietojärjestelmien suojattu yhteenliittäminen***

33. Yhteenliittämisellä tarkoitetaan kahden tai useamman tietotekniikkajärjestelmän välitöntä liittämistä toisiinsa tietojen ja muiden tietoresurssien jakamiseksi yksi- tai monisuuntaisesti.

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

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

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

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

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

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

37. Jos suojaamatonta tai julkista verkkoa käytetään ainoastaan tietovälineenä ja tiedot on salattu 27 kohdan mukaisesti hyväksytyllä EU:n salaustuotteella, tällaista liitäntää ei pidetä yhteenliitäntänä.

38. Tietojen, joiden turvallisuusluokitus on TRES SECRET UE / EU TOP SECRET tai vastaava taikka SECRET UE / EU SECRET tai vastaava, käsittelyyn hyväksytyn viestintä- ja tietojärjestelmän välitön tai porrastettu yhteenliitäntä suojaamattoman tai julkisen verkon kanssa on kiellettyä.

B.10. ***Atk-tallennusvälineet***

39. Atk-tallennusvälineet on tuhottava asianomaisen toimivaltaisen viranomaisen hyväksymällä menettelyllä.

40. Atk-tallennusvälineiden uudelleenkäytössä, luokituksen laskemisessa ja poistamisessa on noudatettava käsittelyohjeita.

B.11. ***Kiireelliset olosuhteet***

41. Jäljempänä kuvattuja erityismenettelyjä voidaan soveltaa hätätapauksessa, esimerkiksi kriisitilanteen uhatessa tai toteutuessa, konfliktissa, sotatilanteissa taikka poikkeuksellisissa toimintaolosuhteissa.

42. Turvallisuusluokiteltujen tietojen lähettämisessä voidaan käyttää alempaa turvallisuusluokitusta varten hyväksyttyjä salaustuotteita tai ne voidaan lähettää ilman salausta toimivaltaisen viranomaisen suostumuksella, jos mahdollinen viivästyminen aiheuttaisi selvästi suuremman vahingon kuin turvallisuusluokitellun aineiston mahdollisen paljastumisen aiheuttama vahinko ja jos

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

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

43. Edellä 41 kohdassa esitetyissä olosuhteissa lähetetyissä turvallisuusluokitelluissa tiedoissa ei saa olla mitään merkintöjä eikä mainintoja, jotka erottavat ne turvallisuusluokittelemattomista tiedoista tai tiedoista, jotka voidaan suojata käytettävissä olevalla salauslaitteella. Tietojen vastaanottajille on ilmoitettava turvallisuusluokituksesta viipymättä muulla tavoin.

44. Jos 41 tai 42 kohtaa sovelletaan, toimivaltaiselle viranomaiselle on annettava asiasta raportti.

TURVALLISUUSOHJE 4

FYYSINEN TURVALLISUUS

A. **JOHDANTO**

Tässä turvallisuusohjeessa määritellään turvallisuusperiaatteet turvallisen ympäristön luomiseksi luottamuksellisten tietojen asianmukaiselle käsittelylle Euroopan parlamentissa. Näiden periaatteiden, tekninen turvallisuus mukaan luettuna, lisäksi sovelletaan käsittelyohjeita.

B. **TURVALLISUUSRISKIEN HALLINTA**

1. Turvallisuusluokiteltuihin tietoihin kohdistuvia riskejä on hallittava prosessina. Prosessissa on pyrittävä määrittelemään tunnetut turvallisuusriskit ja turvatoimet niiden vähentämiseksi hyväksyttävälle tasolle tässä päätöksessä säädettyjen perusperiaatteiden ja vähimmäisvaatimusten mukaisesti, sekä soveltamaan kyseisiä turvatoimia turvallisuusohjeessa 4 määritellyn monitasoisen turvallisuuden käsitteen pohjalta. Turvatoimien tehokkuutta on arvioitava jatkuvasti.

2. Turvatoimet turvallisuusluokiteltujen tietojen suojaamiseksi koko niiden elinkaaren ajan on suhteutettava erityisesti niiden turvallisuusluokitukseen, kyseessä olevien tietojen tai aineistojen muotoon ja määrään, turvallisuusluokiteltujen tietojen sijoitustilojen sijaintiin ja rakentamiseen sekä paikallisesti arvioituun vihamielisen ja/tai rikollisen toiminnan uhkaan, vakoilu, sabotaasi ja terrorismi mukaan luettuina.

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

4. Toiminnan jatkuvuussuunnitelmiin on sisällytettävä ennalta ehkäiseviä ja tilanteen korjaamiseen tarvittavia toimenpiteitä, jotta minimoitaisiin merkittävien toimintahäiriöiden tai poikkeuksellisten tapahtumien vaikutukset turvallisuusluokiteltujen tietojen käsittelyyn ja säilyttämiseen.

C. **YLEISET PERIAATTEET**

5. Tiedoille määritetty turvallisuusluokituksen taso määrää suojelun tason, joka niille annetaan fyysiseen turvallisuuteen liittyen.

6. Turvallisuusluokitusta edellyttävät tiedot merkitään sellaisiksi ja niitä käsitellään sellaisina tietojen fyysisestä muodosta riippumatta. Tietojen turvallisuusluokitus ilmoitetaan selvästi tietojen vastaanottajille joko turvallisuusluokitusmerkinnän avulla (jos tiedot esitetään kirjallisesti paperilla tai viestintä- ja tietojärjestelmässä) tai ilmoituksen avulla (jos tiedot esitetään suullisesti esimerkiksi keskustelun tai esityksen yhteydessä). Turvallisuusluokitellut tiedot merkitään fyysisesti niin, että niiden turvallisuusluokitus on helposti nähtävissä.

7. Luottamuksellisia tietoja ei saa missään tapauksessa lukea sellaisissa junien, lentokoneiden, kahviloiden tai baarien kaltaisissa julkisissa paikoissa, joissa henkilöt, joilla ei ole tiedonsaantitarvetta, saattaisivat nähdä niitä. Niitä ei saa jättää hotellien kassakaappeihin tai huoneisiin eikä niitä saa jättää vartioimatta julkisille paikoille.

D. **VASTUUT**

8. Turvallisuusluokiteltujen tietojen yksikkö vastaa sen turvallisiin tiloihin siirrettyjen luottamuksellisten tietojen konkreettisesta hallinnasta. Turvallisuusluokiteltujen tietojen yksikkö vastaa myös turvallisten tilojensa hallinnasta.

9. Tietojen, joiden turvallisuusluokitus on RESTREINT UE / EU RESTRICTED tai vastaava, sekä muiden luottamuksellisten tietojen konkreettinen hallinta on asianomaisen parlamentin elimen tai parlamentin elimessä toimivan jäsenen vastuulla.

10. Turvallisuus- ja riskianalyysiosasto vastaa henkilökohtaisista suojatoimista ja luottamuksellisten tietojen turvallisen käsittelyn edellyttämästä luotettavuusselvityksestä Euroopan parlamentissa.

11. Tietohallinto-osasto varmistaa neuvonnallaan, että laaditut tai käytetyt viestintä- ja tietojärjestelmät ovat turvallisuusohjeen 3:n ja asiaankuuluvien käsittelyohjeiden mukaisia.

E. **TURVALLISET TILAT**

12. Turvallisia tiloja voidaan asentaa teknisten turvanormien ja 7 artiklassa määritellyille luottamuksellisille tiedoille tarkoitettujen turvallisuustasojen mukaisesti.

13. Turvallisuusjärjestelyistä vastaava viranomainen päättää turvallisten tilojen asentamisesta ja turvallisuusviranomainen hyväksyy päätöksen.

F. **LUOTTAMUKSELLISIIN TIETOIHIN TUTUSTUMINEN**

14. Kun tietoja, joiden turvallisuusluokitus on RESTREINT EU / EU RESTRICTED tai vastaava, tai muita luottamuksellisia tietoja siirretään turvallisuusluokiteltujen tietojen yksikön sisällä ja niihin on tutustuttava turvallisuusalueen ulkopuolella, turvallisuusluokiteltujen tietojen yksikkö lähettää kopion asianmukaiselle valtuutetulle yksikölle, joka varmistaa, että kyseessä oleviin tietoihin tutustuminen ja niiden käsittely tapahtuu tämän päätöksen 8 artiklan 2 kohdan ja 10 artiklan sekä asianmukaisten käsittelyohjeiden mukaisesti.

15. Kun tietoja, joiden turvallisuusluokitus on RESTREINT EU / EU RESTRICTED tai vastaava, tai muita luottamuksellisia tietoja siirretään muun parlamentin elimen kuin turvallisuusluokiteltujen tietojen yksikön sisällä, kyseisen elimen tai parlamentin elimessä toimivan jäsenen sihteeristön on varmistettava, että kyseessä oleviin tietoihin tutustutaan ja niitä käsitellään tämän päätöksen 7 artiklan 3 kohdan, 8 artiklan 1, 2 ja 4 kohdan, 9 artiklan 3, 4 ja 5 kohdan, 10 artiklan 2–6 kohdan ja 11 artiklan sekä asianmukaisten käsittelyohjeiden mukaisesti.

16. Kun tietoihin, joiden turvallisuusluokitus on vähintään CONFIDENTIEL UE / EU CONFIDENTIAL tai vastaava, on tutustuttava turvallisuusalueella, turvallisuusluokiteltujen tietojen yksikön on varmistettava, että kyseessä oleviin tietoihin tutustuminen ja niiden käsittely tapahtuvat tämän päätöksen 9 ja 10 artiklan ja asianmukaisten käsittelyohjeiden mukaisesti.

G. **TEKNINEN TURVALLISUUS**

17. Tekniset turvatoimet kuuluvat turvallisuusjärjestelyistä vastaavalle viranomaiselle, joka määrittelee sovellettavat erityiset tekniset turvatoimet asiaa koskevissa käsittelyohjeissa.

18. Sellaisiin tietoihin, joiden turvallisuusluokitus on RESTREINT EU / EU RESTRICTED tai vastaava, tai muihin luottamuksellisiin tietoihin tutustumiseen tarkoitettujen turvallisten lukusalien on oltava käsittelyohjeissa ilmoitettujen erityisten teknisten määräysten mukaisia.

19. Turvallinen alue käsittää seuraavat tilat:

a) turvallinen lukusali, jonka asentamisessa on noudatettava käsittelyohjeisiin sisältyviä teknisen turvallisuuden määräyksiä. Tähän tilaan pääsy edellyttää rekisteröitymistä. Turvallisessa lukusalissa noudatetaan tiukkoja normeja luvan saaneiden henkilöiden tunnistamisen, videorekisteröinnin ja ulkopuolelle jätettävien henkilökohtaisten tavaroiden (puhelimet, kynät y.m.) turvallisen säilytyksen suhteen;

b) viestintähuone turvallisuusluokiteltujen ja myös salattujen tietojen lähettämiseksi ja vastaanottamiseksi turvallisuusohjeen 3 ja asianomaisten käsittelyohjeiden mukaisesti;

c) turvallinen arkisto, jossa käytetään hyväksyttyjä ja sertifioituja erillisiä säilytyspaikkoja tiedoille, joiden turvallisuusluokitus on RESTREINT UE / EU RESTRICTED, CONFIDENTIEL UE / EU CONFIDENTIAL ja/tai SECRET EU / EU SECRET tai vastaava. Tiedot, joiden turvallisuusluokitus on TRES SECRET UE / EU TOP SECRET tai vastaava, säilytetään erillisessä huoneessa erillisessä sertifioidussa säilytyspaikassa. Ainoa muu esine tässä huoneessa on apupöytä turvaluokiteltujen tietojen yksikön arkiston käsittelemiseksi;

d) kirjaamishuone, jossa on tarpeelliset välineet paperilla tai sähköisesti tapahtuvan kirjaamisen suorittamiseen ja jossa siten on tarvittava turvarakenne asianmukaisen viestintä- ja tietojärjestelmän asentamiseksi. Kirjaamishuone on ainoa paikka, jossa voi olla hyväksyttyjä kopiointilaitteita (paperikopioiden tai sähköisten kopioiden tekemistä varten). Käsittelyohjeissa eritellään, mitkä kopiointilaitteet ovat hyväksyttyjä. Kirjaamishuoneessa säilytetään ja käsitellään myös fyysisessä muodossa olevien turvallisuusluokiteltujen tietojen merkintöihin, kopiointiin ja lähettämiseen tarvittavia hyväksyttyjä välineitä. Turvallisuusluokiteltujen tietojen yksikön on määriteltävä ja turvallisuusjärjestelyistä vastaavan viranomaisen hyväksyttävä kaikki hyväksytty aineisto operatiiviselta tiedonturvaamisviranomaiselta saatujen ohjeiden mukaan. Huoneessa on oltava myös hyväksytty tuhoamislaite, joka on käsittelyohjeissa tarkoitetun korkeimman turvallisuusluokituksen mukainen. Tietojen, joiden turvallisuusluokitus on vähintään CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE / EU SECRET tai TRÈS SECRET UE / EU TOP SECRET tai vastaava, kääntäminen on suoritettava rekisteröintihuoneessa asianmukaisessa ja hyväksytyssä järjestelmässä. Rekisteröintihuoneessa on oltava työasemat enintään kahdelle kääntäjälle kerrallaan samaa asiakirjaa varten. Paikalla on oltava yksi turvallisuusluokiteltujen tietojen yksikön edustaja;

e) lukusali turvallisuusluokiteltuun tietoon tutustumista varten asianmukaisesti valtuutetuille henkilöille. Lukusalissa on oltava tilat kahdelle henkilölle, mukaan luettuna turvallisuusluokiteltujen tietojen yksikön edustaja, jonka on oltava koko ajan läsnä aina kun tietoihin tutustutaan. Lukusalin turvallisuustason on oltava riittävä siten, että siellä voidaan tutustua tietoihin, joiden luokitus on CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE / EU SECRET tai TRÈS SECRET UE / EU TOP SECRET tai vastaava. Lukusali voi olla varustettu TEMPEST-turvatoimilla, jotta asiakirjoihin voidaan tarvittaessa tutustua sähköisesti kyseessä olevien tietojen luokituksen mukaisella tavalla.

f) kokoussali, jossa on oltava tilat 25 henkilölle, jotta voidaan keskustella tiedoista, joiden turvallisuusluokitus on CONFIDENTIEL UE / EU CONFIDENTIAL ja SECRET EU / EU SECRET tai vastaava. Kokoussalissa on oltava tarvittavat, teknisesti turvalliset ja hyväksytyt välineet enintään kahdelle kielelle ja kahdesta kielestä tapahtuvaa tulkkausta varten. Kun kokoussalia ei käytetä kokouksiin, se voi toimia myös lukusalina tietoihin tutustumista varten. Poikkeustapauksissa turvallisuusluokiteltujen tietojen yksikkö voi sallia useamman kuin yhden valtuutetun henkilön tutustumisen tietoihin, jos kaikkien henkilöiden valtuutuksen ja tiedonsaantitarpeen taso on sama. Enintään neljä henkilöä voi kerrallaan tutustua turvallisuusluokiteltuihin tietoihin. Turvallisuusluokiteltujen tietojen yksikön virkamiesten läsnäoloa on tällöin tehostettava.

g) teknisen turvallisuuden huoneet kaikkien teknisten laitteiden, jotka liittyvät koko turvallisuusalueen turvallisuuteen, ja turvallisten verkkopalvelinten sijoittamiseksi.

20. Turvallisuusalueen on oltava sovellettavien kansainvälisten turvanormien mukainen ja turvallisuus- ja riskianalyysiosaston hyväksymä. Turvallisuusalueen on täytettävä seuraavat tekniset vähimmäisvaatimukset:

a) hälytys- ja valvontajärjestelmät;

b) turvalaitteet ja hätäjärjestelmät (kaksisuuntainen varoitusjärjestelmä);

c) kameravalvonta;

d) murronpaljastusjärjestelmä;

e) kulunvalvontajärjestelmä (myös biometrinen turvajärjestelmä);

f) säilytyspaikat;

g) säilytyslokerot;

h) sähkömagneettisuudelta suojeleva järjestelmä.

21. Turvallisuusjärjestelyistä vastaava viranomainen voi yhdessä turvallisuusluokiteltujen tietojen yksikön kanssa ja turvallisuusviranomaisen suostumuksella tarvittaessa lisätä muita teknisiä turvatoimia.

22. Infrastruktuurilaitteistot voidaan yhdistää turvallisuusalueen sijaintirakennuksen yleisiin hallintajärjestelmiin. Kulunvalvontaan sekä viestintä- ja tietojärjestelmiin kuuluvien turvalaitteiden on kuitenkin oltava riippumattomia Euroopan parlamentin muista vastaavista järjestelmistä.

H. **TURVALLISEN ALUEEN TARKASTUS**

23. Turvallisuusjärjestelyt hyväksyvä viranomainen tarkastaa turvallisen alueen säännöllisesti turvallisuusluokiteltujen tietojen yksikön pyynnöstä.

24. Turvallisuusjärjestelyt hyväksyvä viranomainen laatii ja päivittää käsittelyohjeiden mukaisesti tarvittavien turvallisuustarkastusten kohdeluettelon asioista, joihin tarkastus on kohdistettava.

I. **LUOTTAMUKSELLISTEN TIETOJEN KULJETTAMINEN**

25. Turvallisuusluokitellut tiedot kuljetetaan käsittelyohjeiden mukaisesti katseilta piilossa ilman osoitusta sisällön luottamuksellisesta luonteesta.

26. Ainoastaan sellaiset lähetit tai henkilöstön edustajat, joilla on riittävä turvallisuusvaltuutus, voivat kuljettaa tietoja, joiden turvallisuusluokitus on CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE / EU SECRET tai TRÈS SECRET UE / EU TOP SECRET tai vastaava.

27. Ulkoisten posti- tai kuriiripalvelujen käyttäminen rakennuksen ulkopuolella on mahdollista ainoastaan käsittelyohjeissa olevien ehtojen mukaisesti.

28. Tietoja, joiden turvallisuusluokitus on CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE / EU SECRET tai TRÈS SECRET UE / EU TOP SECRET tai vastaava, ei saa koskaan lähettää sähköpostilla tai faksilla, vaikka sähköpostijärjestelmä olisikin ”turvallinen” ja faksi ”salattu”. Tietoja, joiden turvallisuusluokitus on RESTREINT UE / EU RESTRICTED tai vastaava, tai muita luottamuksellisia tietoja voidaan lähettää sähköpostilla hyväksyttyä salausjärjestelmää käyttäen.

J. **LUOTTAMUKSELLISTEN TIETOJEN SÄILYTYS**

29. Luottamukselliselle tiedolle määritellystä turvaluokituksen tai merkinnän tasosta riippuu sille myönnettävä suojelun taso säilytyksessä. Sitä säilytetään tähän tarkoitukseen käsittelyohjeissa varatuilla keinoilla.

30. Tietoja, joiden turvallisuusluokitus on RESTREINT UE / EU RESTRICTED tai vastaava, ja muita luottamuksellisia tietoja

a) on säilytettävä tavanomaisessa lukitussa teräskaapissa työhuoneessa tai työskentelyalueella silloin, kun niitä ei käytetä;

b) ei saa jättää vartioimatta, ellei niitä ole asianmukaisesti lukittu ja varastoitu;

c) ei saa jättää pöydälle tai muualle siten, että valtuuttamaton henkilö, kuten vierailija, siivooja, huoltohenkilökunta tms. voisi lukea tai ottaa sen;

d) ei saa näyttää valtuuttamattomalle henkilölle tai keskustella niistä hänen kanssaan.

31. Tietoja, joiden turvallisuusluokitus on RESTREINT UE / EU RESTRICTED tai vastaava, ja muita luottamuksellisia tietoja on varastoitava ainoastaan parlamentin elinten tai parlamentin elimissä toimivien jäsenten sihteeristöissä tai turvallisuusluokiteltujen tietojen yksikössä käsittelyohjeiden mukaisesti.

32. Tietoja, joiden turvallisuusluokitus on vähintään CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE / EU SECRET tai TRÈS SECRET UE / EU TOP SECRET tai vastaava

a) säilytetään turvallisella alueella turvallisessa säilytyspaikassa tai kassaholvissa. Poikkeustapauksissa, kuten jos turvallisuusluokiteltujen tietojen yksikkö on suljettu, niitä voidaan säilyttää hyväksytyssä turvakaapissa turvallisuusyksikön tiloissa;

b) ei saa (lyhyeksikään aikaa) jättää vartioimatta turvallisuusalueella missään vaiheessa ilman, että ne on lukittu hyväksyttyyn turvakaappiin;

c) ei saa jättää pöydälle tai muualle siten, että valtuuttamaton henkilö voisi lukea tai ottaa sen, vaikka turvallisuusluokiteltujen tietojen yksikön vastaava virkamies olisikin huoneessa.

Kun turvallisuusluokiteltuja tietoja sisältävää dokumenttia laaditaan turvallisuusalueella sähköisessä muodossa, tietokone on lukittava ja näyttöruutu pimennettävä, jos tietojen luovuttaja tai turvallisuusluokiteltujen tietojen yksikön vastaava virkamies poistuu huoneesta (lyhyeksikin aikaa). Muutaman minuutin kuluttua päälle kytkeytyvä automaattinen turvalukko ei ole riittävä turvatoimi.

TURVALLISUUSOHJE 5

YHTEISÖTURVALLISUUS

A. **JOHDANTO**

1. Tämä turvallisuusohje koskee vain turvallisuusluokiteltuja tietoja.

2. Siinä vahvistetaan tämän päätöksen liitteessä I olevan 1 osan mukaisten vähimmäisvaatimusten täytäntöönpanoa koskevat määräykset.

3. Yhteisöturvallisuudella tarkoitetaan toimenpiteiden toteuttamista sen varmistamiseksi, että hankeosapuolet tai alihankkijat varmistavat turvallisuusluokiteltujen tietojen suojaamisen sopimusta edeltävissä neuvotteluissa ja turvallisuusluokiteltujen sopimusten koko elinkaaren ajan. Kyseisiin sopimuksiin ei saa kuulua pääsyä tietoihin, joiden turvallisuusluokitus on TRES SECRET UE / EU TOP SECRET.

4. Euroopan parlamentin on hankeviranomaisena varmistettava, että tässä päätöksessä säädettyjä ja sopimuksessa tarkoitettuja yhteisöturvallisuutta koskevia vähimmäisvaatimuksia noudatetaan tehtäessä turvallisuusluokiteltuja sopimuksia yritysten tai muiden yhteisöjen kanssa.

B. **TURVALLISUUSLUOKITELLUN SOPIMUKSEN TURVALLISUUTTA KOSKEVAT OSAT**

B.1. ***Turvallisuusluokitusopas***

5. Ennen tarjouskilpailun käynnistämistä tai turvallisuusluokitellun sopimuksen tekemistä hankeviranomaisena toimivan Euroopan parlamentin on määriteltävä tarjouksen tekijöille ja hankeosapuolille toimitettavien tietojen turvallisuusluokitus sekä hankeosapuolen tuottamien tietojen turvallisuusluokitus. Euroopan parlamentin on sitä varten laadittava turvallisuusluokitusopas, jota noudatetaan sopimuksen toimeenpanossa.

6. Turvallisuusluokitellun sopimuksen eri osien turvallisuusluokituksen tason määrittämiseksi sovelletaan seuraavia periaatteita:

a) turvallisuusluokitusopasta laatiessaan Euroopan parlamentin on otettava huomioon kaikki asiaankuuluvat turvallisuusnäkökohdat, mukaan lukien turvallisuusluokitus, jonka tietojen alkuperäinen luovuttaja on antanut luovutetuille tiedoille ja hyväksynyt myös sopimuksen osalta;

b) koko sopimuksen turvallisuusluokitus ei voi olla alempi kuin sen minkä tahansa osan korkein turvallisuusluokitus.

B.2. ***Turvallisuutta koskeva lisälauseke***

7. Sopimuskohtaiset turvallisuusvaatimukset on ilmoitettava turvallisuutta koskevassa lisälausekkeessa. Turvallisuutta koskevan lisälausekkeen on tarvittaessa sisällettävä turvallisuusluokitusopas, ja sen on oltava erottamaton osa turvallisuusluokiteltua sopimusta tai alihankintasopimusta.

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

B.3. ***Ohjelman tai hankkeen turvallisuusohjeet***

9. EU:n turvallisuusluokiteltuihin tietoihin pääsyä tai tietojen käsittelyä tai säilyttämistä edellyttävien ohjelmien tai hankkeiden soveltamisalasta riippuen kyseisten ohjelmien tai hankkeiden hallinnointia varten nimetty hankeviranomainen voi laatia niitä koskevat erityiset turvallisuusohjeet.

C. **YHTEISÖTURVALLISUUSSELVITYS**

10. Yhteisöturvallisuusselvityksen myöntää jäsenvaltion kansallinen turvallisuusviranomainen tai muu toimivaltainen turvallisuusviranomainen osoittaakseen kansallisten lakien ja asetusten mukaisesti, että yritys tai muu yhteisö pystyy suojaamaan toimitiloissaan asianmukaisesti EU:n turvallisuusluokiteltuja tietoja, joiden turvallisuusluokitus on CONFIDENTIEL UE / EU CONFIDENTIAL tai SECRET UE / EU SECRET tai vastaava. Selvitys siitä, että yhteisöturvallisuusselvitys on myönnetty, on esitettävä hankeviranomaisena toimivalle Euroopan parlamentille ennen kuin hankeosapuolelle tai alihankkijalle taikka mahdolliselle hankeosapuolelle tai alihankkijalle voidaan luovuttaa EU:n turvallisuusluokiteltuja tietoja tai myöntää pääsy niihin.

11. Yhteisöturvallisuusselvityksellä

a) arvioidaan yrityksen tai muun yhteisön eheyttä;

b) arvioidaan turvallisuusriskejä, joita saattaa aiheutua omistussuhteista, valvonnasta ja/tai mahdollisuuksista epäasianmukaiseen vaikutusvaltaan;

c) todennetaan, että yritys tai muu yhteisö on ottanut toimitilassa käyttöön turvallisuusjärjestelmän, joka kattaa kaikki tässä päätöksessä säädettyjen vaatimusten mukaiset turvatoimet, jotta se voi suojata asianmukaisesti tietoja tai aineistoja, joiden turvallisuusluokitus on CONFIDENTIEL UE / EU CONFIDENTIAL tai SECRET UE / EU SECRET;

d) todennetaan, että johtohenkilöstön, omistajien ja työntekijöiden, joiden tehtävät edellyttävät pääsyä tietoihin, joiden turvallisuusluokitus on CONFIDENTIEL UE / EU CONFIDENTIAL tai SECRET UE / EU SECRET, henkilöturvallisuus on selvitetty tässä päätöksessä säädettyjen vaatimusten mukaisesti; sekä

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

12. Hankeviranomaisena toimivan Euroopan parlamentin on tarvittaessa ilmoitettava asianmukaiselle kansalliselle turvallisuusviranomaiselle tai muulle toimivaltaiselle turvallisuusviranomaiselle, että yhteisöturvallisuusselvitys vaaditaan sopimuksen tekemistä edeltävässä vaiheessa tai sopimuksen toimeenpanoa varten. Kansallista turvallisuusviranomaista tai muuta toimivaltaista turvallisuusviranomaista tarvitaan sopimusta edeltävien neuvottelujen aikana, kun osana tarjousmenettelyjä on annettava tietoja, joiden turvallisuusluokitus on CONFIDENTIEL UE / EU CONFIDENTIAL tai SECRET UE / EU SECRET.

13. Hankeviranomainen ei saa myöntää turvallisuusluokiteltua sopimusta valitulle tarjoajalle ennen kuin se on saanut sen jäsenvaltion kansalliselta turvallisuusviranomaiselta tai muulta toimivaltaiselta turvallisuusviranomaiselta, johon asianomainen hankeosapuoli tai alihankkija on rekisteröity, vahvistuksen siitä, että mahdollisesti vaadittava asianmukainen yhteisöturvallisuusselvitys on myönnetty.

14. Yhteisöturvallisuusselvityksen antaneen toimivaltaisen turvallisuusviranomaisen on ilmoitettava hankeviranomaisena toimivalle Euroopan parlamentille yhteisöturvallisuusselvitykseen vaikuttavista muutoksista. Jos kyse on alihankkijasta, toimivaltaiselle turvallisuusviranomaiselle on vastaavasti ilmoitettava.

15. Jos asiaankuuluva kansallinen tai muu toimivaltainen turvallisuusviranomainen peruuttaa yhteisöturvallisuusselvityksen, hankeviranomaisena toimivalla Euroopan parlamentilla on riittävät perusteet päättää turvallisuusluokiteltu sopimus tai sulkea tarjoaja kilpailun ulkopuolelle.

D. **TURVALLISUUSLUOKITELLUT SOPIMUKSET JA ALIHANKINTASOPIMUKSET**

16. Jos turvallisuusluokiteltuja tietoja luovutetaan mahdollisille tarjoajille sopimusta edeltävässä vaiheessa, tarjouspyynnössä on oltava määräys, jolla tarjoajia, jotka eivät esitä tarjousta tai joiden tarjousta ei valita, velvoitetaan palauttamaan kaikki turvallisuusluokitellut asiakirjat tietyn ajan kuluessa.

17. Kun turvallisuusluokiteltu sopimus tai alihankintasopimus on tehty, hankeviranomaisena toimivan Euroopan parlamentin on annettava hankeosapuolen tai alihankkijan kansalliselle ja/tai muulle toimivaltaiselle turvallisuusviranomaiselle tiedoksi turvallisuusluokitellun sopimuksen turvallisuusmääräykset.

18. Kun tällainen sopimus päättyy, hankeviranomaisena toimivan Euroopan parlamentin (ja/tai alihankintasopimuksen tapauksessa toimivaltaisen turvallisuusviranomaisen) on ilmoitettava asiasta viipymättä hankeosapuolen tai alihankkijan rekisteröintijäsenvaltion kansalliselle tai muulle toimivaltaiselle turvallisuusviranomaiselle.

19. Yleensä hankeosapuolen tai alihankkijan edellytetään palauttavan hankeviranomaiselle turvallisuusluokitellun sopimuksen tai alihankintasopimuksen päättyessä kaikki hallussaan olevat turvallisuusluokitellut tiedot.

20. Turvallisuutta koskevaan lisälausekkeeseen on sisällytettävä erityiset säännökset turvallisuusluokiteltujen tietojen hallussapidosta sopimuksen täytäntöönpanon aikana tai sopimuksen päättyessä.

21. Jos hankeosapuoli tai alihankkija saa luvan säilyttää turvallisuusluokiteltuja tietoja sopimuksen päätyttyä, tässä päätöksessä säädettyjä vähimmäisvaatimuksia on yhä sovellettava, ja hankeosapuolen tai alihankkijan on suojattava EU:n turvallisuusluokiteltujen tietojen luottamuksellisuus.

22. Tarjouksessa ja sopimuksessa on määriteltävä, millä edellytyksin hankeosapuoli voi tehdä alihankintasopimuksia.

23. Hankeosapuolen on saatava hankeviranomaisena toimivan Euroopan parlamentin lupa ennen kuin se antaa turvallisuusluokitellun sopimuksen mitään osia alihankkijoiden toteutettavaksi. Alihankintasopimusta ei voida myöntää yrityksille tai muille yhteisöille, jotka on rekisteröity sellaiseen kolmanteen valtioon, joka ei ole tehnyt tietoturvasopimusta unionin kanssa.

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

25. Jos hankeosapuoli tai alihankkija tuottaa tai käsittelee turvallisuusluokiteltuja tietoja, hankeviranomainen harjoittaa tietojen luovuttajan oikeuksia.

E. **TURVALLISUUSLUOKITELTUIHIN SOPIMUKSIIN LIITTYVÄT VIERAILUT**

26. Jos Euroopan parlamentti, hankeosapuolet tai alihankkijat haluavat turvallisuusluokitellun sopimuksen toimeenpanemiseksi tutustua toistensa toimitiloissa tietoihin, joiden turvallisuusluokitus on CONFIDENTIEL UE / EU CONFIDENTIAL tai SECRET UE / EU SECRET, vierailut järjestetään yhdessä kansallisten turvallisuusviranomaisten tai muiden toimivaltaisten turvallisuusviranomaisten kanssa. Kansalliset turvallisuusviranomaiset tai muut toimivaltaiset turvallisuusviranomaiset voivat kuitenkin sopia myös menettelystä, jolla vierailuista voidaan sopia suoraan.

27. Kaikilla vierailijoilla on oltava asianmukainen turvallisuusselvitys ja tiedonsaantitarve, jotta heille voidaan myöntää pääsy Euroopan parlamentin tekemään sopimukseen liittyviin turvallisuusluokiteltuihin tietoihin.

28. Vierailijat voivat tutustua vain käynnin tarkoitukseen liittyviin turvallisuusluokiteltuihin tietoihin.

F. **TURVALLISUUSLUOKITELTUJEN TIETOJEN LÄHETTÄMINEN JA KULJETTAMINEN**

29. Turvallisuusluokiteltujen tietojen lähettämiseen sähköisesti sovelletaan turvallisuusohjeen 3 asiaankuuluvia säännöksiä.

30. Turvallisuusluokiteltujen tietojen kuljettamiseen sovelletaan turvallisuusohjeen 4 asiaankuuluvia säännöksiä ja käsittelyohjeita.

31. Turvallisuusluokiteltujen tietojen rahtikuljetuksia koskevia turvallisuusjärjestelyjä määritettäessä sovelletaan seuraavia periaatteita:

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

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

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

d) ennen kuin aineistoa, jonka turvallisuusluokitus on CONFIDENTIEL UE / EU CONFIDENTIAL tai SECRET UE / EU SECRET tai vastaava, siirretään rajojen yli, lähettäjän on laadittava kuljetussuunnitelma, jonka pääsihteeri hyväksyy;

e) kuljetusten on mahdollisuuksien mukaan tapahduttava yhtäjaksoisesti lähtöpaikasta määränpäähän ja ne on suoritettava niin nopeasti kuin olosuhteet sallivat;

f) reitin on kuljettava aina kun mahdollista jäsenvaltioiden alueen kautta.

G. **TURVALLISUUSLUOKITELTUJEN TIETOJEN LÄHETTÄMINEN KOLMANSISSA VALTIOISSA SIJAITSEVILLE HANKEOSAPUOLILLE**

32. Turvallisuusluokiteltuja tietoja lähetetään kolmansissa valtioissa sijaitseville hankeosapuolille ja alihankkijoille hankeviranomaisena toimivan Euroopan parlamentin ja sen kolmannen valtion, johon hankeosapuoli on rekisteröity, välillä sovittujen turvatoimien mukaisesti.

H. **TIETOJEN, JOIDEN TURVALLISUUSLUOKITUS ON RESTREINT EU / EU RESTRICTED, KÄSITTELY JA SÄILYTYS**

33. Euroopan parlamentti voi hankeviranomaisena yhdessä jäsenvaltion kansallisen tai turvallisuusviranomaisen kanssa tehdä vierailuja hankeosapuolten tai alihankkijoiden toimitiloihin sopimusmääräysten pohjalta sen varmistamiseksi, että sopimuksessa edellytetyt tarpeelliset turvatoimet on toteutettu EU:n turvallisuusluokiteltujen tietojen, joiden turvallisuusluokitus on RESTREINT UE / EU RESTRICTED, suojaamiseksi.

34. Euroopan parlamentti hankeviranomaisena ilmoittaa kansallisille turvallisuusviranomaisille tai muille toimivaltaisille turvallisuusviranomaisille kansallisten lakien ja asetusten puitteissa toimeksiannoista ja alihankintasopimuksista, jotka sisältävät tietoja, joiden turvallisuusluokitus on RESTREINT UE / EU RESTRICTED.

35. Hankeosapuolilta tai alihankkijoilta ei vaadita yhteisöturvallisuusselvitystä eikä henkilöturvallisuusselvitystä sellaisia Euroopan parlamentin tekemiä sopimuksia varten, joihin sisältyy tietoja, joiden turvallisuusluokitus on RESTREINT UE / EU RESTRICTED.

36. Hankeviranomaisena toimivan Euroopan parlamentin on tutkittava tarjouspyyntöihin saadut vastaukset, jos sopimuksen tekeminen edellyttää sellaisten tietojen saamista, joiden turvallisuusluokitus on RESTREINT UE / EU RESTRICTED, rajoittamatta kuitenkaan vaatimuksia, joita kansallisissa laeissa ja asetuksissa saattaa olla yhteisöturvallisuusselvityksistä tai henkilöturvallisuusselvityksistä.

37. Tarjouksessa ja sopimuksessa on määriteltävä, millä edellytyksin hankeosapuoli voi tehdä alihankintasopimuksia.

38. Jos sopimukseen kuuluu sellaisten tietojen, joiden turvallisuusluokitus on RESTREINT UE / EU RESTRICTED, käsittelyä hankeosapuolen käyttämässä viestintä- ja tietojärjestelmässä, hankeviranomaisena toimivan Euroopan parlamentin on varmistettava, että sopimuksessa määrätään viestintä- ja tietojärjestelmän hyväksymistä koskevista tarvittavista teknisistä ja hallinnollisista vaatimuksista, jotka ovat oikeassa suhteessa arvioituun riskiin ja joissa on otettu huomioon kaikki asiaankuuluvat tekijät. Kyseisten viestintä- ja tietojärjestelmien hyväksynnän laajuudesta on sovittava hankeviranomaisen ja toimivaltaisen kansallisen turvallisuusviranomaisen tai nimetyn turvallisuusviranomaisen kanssa.

TURVALLISUUSOHJE 6

LUOTTAMUKSELLISTEN TIETOJEN TURVALLISUUSRIKKOMUKSET, KATOAMINEN TAI VAARANTUMINEN

1. Kyseessä on turvallisuusrikkomus, jos tätä päätöstä rikotaan tai laiminlyödään, mistä saattaa aiheutua vahinkoa tai vaaraa turvallisuusluokitellulle tiedolle.

2. Luottamuksellisten tietojen turvallisuus vaarantuu, jos ne ovat joutuneet kokonaisuudessaan tai osittain henkilöille, joita ei ole valtuutettu käsittelemään niitä, eli joiden luotettavuutta ei ole selvitetty asianmukaisella tavalla tai joilla ei ole tiedonsaantitarvetta, tai jos on todennäköistä, että tiedot ovat joutuneet kyseisille henkilöille.

3. Luottamuksellisen tiedon turvallisuus voi vaarantua huolimattomuuden, välinpitämättömyyden tai harkitsemattomuuden seurauksena, unioniin kohdistuvan tiedustelutoiminnan vuoksi tai muuta haitallista toimintaa harjoittavien järjestöjen vuoksi.

4. Jos pääsihteeri havaitsee tai hänelle kerrotaan luottamuksellisten tietojen todistetuista tai epäillyistä turvallisuusrikkomuksista, hänen on:

a) selvitettävä tosiasiat;

b) arvioitava tapahtunut vahinko ja minimoitava sen vaikutukset;

c) ryhdyttävä toimiin tapahtuneen toistamisen estämiseksi;

d) ilmoitettava asiasta sen kolmannen osapuolen tai jäsenvaltion toimivaltaiselle viranomaiselle, joka luovutti tai lähetti kyseiset luottamukselliset tiedot.

Jos asia koskee Euroopan parlamentin jäsentä, pääsihteeri toimii yhdessä Euroopan parlamentin puhemiehen kanssa.

Jos tiedot on saatu toiselta unionin toimielimeltä, pääsihteeri toimii turvallisuusluokiteltuihin tietoihin sovellettavien asianmukaisten turvatoimien ja komission kanssa tehdyn puitesopimuksen tai neuvoston kanssa tehdyn toimielinten välisen sopimuksen nojalla toteutettujen järjestelyjen mukaisesti.

5. Kaikille työnsä puolesta turvallisuusluokiteltuja tietoja käsitteleville henkilöille kerrotaan seikkaperäisesti turvallisuusmenettelyistä, huolimattomien keskustelujen vaaroista ja suhteista tiedotusvälineisiin, ja tarvittaessa heidän on allekirjoitettava vakuutus, jossa he lupaavat olla paljastamatta luottamuksellisia tietoja kolmansille osapuolille, suostuvat noudattamaan turvallisuusluokiteltujen tietojen suojelun velvoitetta ja ilmoittavat ymmärtävänsä seuraukset, jos näin ei tapahdu. Jos turvallisuusluokiteltuihin tietoihin tutustuu tai niitä käyttää henkilö, jolle ei ole kerrottu turvallisuusmenettelyistä ja joka ei ole allekirjoittanut lausuntoa, kyseessä on turvallisuusmääräysten rikkominen.

6. Jos Euroopan parlamentin jäsen, parlamentin virkamies tai poliittisten ryhmien tai hankeosapuolten palveluksessa oleva muu parlamentin työntekijä havaitsee turvallisuusmääräysten rikkomisen tai luottamuksellisten tietojen häviämisen tai vaarantumisen, hänen on ilmoitettava asiasta välittömästi pääsihteerille.

7. Henkilöön, joka on aiheuttanut luottamuksellisten tietojen vaarantumisen, voidaan kohdistaa kurinpidollisia toimenpiteitä sovellettavien sääntöjen ja määräysten mukaisesti. Kurinpitoseuraamus ei rajoita oikeutta ryhtyä oikeustoimiin asiassa sovellettavan lainsäädännön mukaisesti.

8. Parlamentin virkamiesten ja poliittisten ryhmien palveluksessa olevien muiden parlamentin työntekijöiden syyllistyessä rikkomiseen sovelletaan henkilöstösääntöjen VI osastossa säädettyjä menettelyjä ja seuraamuksia, tämän kuitenkaan rajoittamatta oikeutta ryhtyä muihin oikeustoimiin.

9. Euroopan parlamentin jäsenten syyllistyessä rikkomiseen sovelletaan parlamentin työjärjestyksen 9 artiklan 2 kohdan, 152 artiklan, 153 artiklan ja 154 artiklan menettelyjä, tämän kuitenkaan rajoittamatta oikeutta ryhtyä muihin oikeustoimiin.