KANSALLINEN TURVALLISUUSVIRANOMAINEN

KANSAINVÄLISEN TURVALLISUUSLUOKITELLUN TIETOAINEISTON KÄSITTELYOHJE

Päivitetty

16.3.2016

Sisältö

1. JOHDANTO

Tämän ohjeen tarkoituksena on selostaa ja kuvata kansainvälisten tietoturvallisuusvelvoitteiden toteuttamiseen kuuluvan turvallisuusluokitellun tiedon käsittelyyn liittyviä velvollisuuksia. Suomi on sitoutunut valtiosopimuksissa toteuttamaan tietoturvallisuustoimia sellaisen sopimusosapuolen turvallisuusluokitellun tiedon suojaamiseksi, joka on sopimuksen mukaisesti luovutettu Suomeen. Näiden velvoitteiden yleiseksi toteuttamiseksi on säädetty laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004 muutoksineen).

Kansainvälisten turvallisuusluokiteltujen tietoaineistojen käsittelyyn sovelletaan viranomaisten toiminnan julkisuudesta annetun lain (621/1999; jäljempänä julkisuuslaki) yleisiä hyvää tiedonhallintatapaa koskevia velvoitteita sekä tietoturvallisuudesta valtionhallinnosta annettua asetusta (681/2010; jäljempänä tietoturvallisuusasetus), jollei kansainvälisestä tietoturvallisuusvelvoitteesta muuta johdu. Tietoturvallisuusasetuksen täytäntöönpanon yksityiskohtia selventää valtiovarainministeriön ohje (VAHTI 2/2010).

Tämä ohje ei korvaa sopimusmääräyksiä tai muita kansainvälisiä tietoturvallisuusvelvoitteita. Niiden, jotka tarvitsevat tarkkaa tietoa velvoitteista, tulee käyttää ensisijaisena lähteenä velvoitteita määrittteleviä säännöksiä ja sopimuksia.

Ulkoasiainministeriö (UM) toimii kansainvälisten tietoturvallisuusvelvoitteiden toteuttamisessa kansallisena turvallisuusviranomaisena (*National Security Authority*, NSA). Kansallisen turvallisuusviranomaisen lisäksi kansainvälisiä tietoturvallisuusvelvoitteita toteuttavina määrättyinä turvallisuusviranomaisina (*Designated Security Authority*, DSA) toimivat puolustusministeriö, pääesikunta ja suojelupoliisi. Lisäksi Viestintävirasto toimii kansallisena tietojärjestelmien ja tietoliikenteen tietoturvallisuudesta vastaavana viranomaisena (*National Communication Security Authority*, NCSA). Näillä kaikilla on omat vastuualueensa kansallisen turvallisuusviranomaisen tehtäväkentässä.

Tarvittaessa tapauskohtaista neuvoa ja ohjausta on syytä kääntyä kansallisen turvallisuusviranomaisorganisaation puoleen. Yleiset kysymykset osoitetaan UM:ssä toimivalle kansalliselle turvallisuusviranomaiselle (nsa@formin.fi) ja sähköiseen tiedonsiirtoon liittyvät erityiskysymykset Viestintäviraston NCSA-FI-yksikölle (ncsa@ficora.fi).

2. KANSAINVÄLINEN TURVALLISUUSLUOKITELTU TIETOAINEISTO

Kansainvälisellä turvallisuusluokitellulla tietoaineistolla tarkoitetaan kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa tarkoitettua *erityissuojattavaa tietoaineistoa*, jota Suomen on kansainvälisen sopimuksen tai EU:n turvallisuussääntöjen perusteella suojattava. Kansainvälisiä turvallisuusluokiteltuja tietoaineistoja ovat siten Suomeen toimitetut asiakirjat, aineistot, materiaalit ja näihin sisältyvät tiedot, joihin luovuttaja on tehnyt turvallisuusluokkamerkinnän kansainvälisen tietoturvallisuusvelvoitteen mukaisesti.

2.1. Tietoaineiston salassapitovelvollisuus

Kansainväliseen turvallisuusluokiteltuun aineistoon sovelletaan kansainvälisistä tietoturvallisuusvelvoitteista annetun lain erityissäännöstä ehdottomasta salassapitovelvollisuudesta eikä siihen kohdistu julkisuuslain mukaista salassapidon tapauskohtaista arviointia. Kansainväliset turvallisuusluokitellut tietoaineistot on siten pidettävä salassa, jollei niitä koskevista sopimuksista tai säännöistä muuta johdu.

Kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa on rangaistussäännökset salassapitovelvollisuuden rikkomisesta. Rangaistus salassapitovelvollisuuden rikkomisesta tuomitaan rikoslain (39/1889) mukaan joko virkasalaisuuden rikkomisena tai tuottamuksellisena virkasalaisuuden rikkomisena, salassapitorikoksena tai salassapitorikkomuksena.

EU:n toimielinten asiakirjojen julkisuutta koskevaan säädökseen, ns. avoimuusasetukseen (1049/2001) sisältyy yleisiä säännöksiä arkaluonteisten EU-asiakirjojen käsittelystä. Avoimuusasetuksessa on säädetty perusteet turvallisuusluokitukselle. Tarkemmista EU:n turvallisuusluokitellun tiedon suojaamiseksi toteutettavista menettelyistä ja järjestelyistä säädetään Euroopan unionin toimielinten turvallisuussäännöissä.

2.2. Turvallisuusluokitellun tiedon suojaamisesta ja vaihtamisesta sopiminen

Turvallisuusluokitellun tiedon suojaamisesta sopiminen Suomen ja vieraan valtion taikka Suomen ja kansainvälisen järjestön välillä edellyttää valtiosopimusta. Tietoturvallisuussopimuksissa velvoitetaan sopimuspuolet huolehtimaan, että toisen sopimuspuolen turvallisuusluokiteltua tietoa käsitellään asianmukaisesti.
Suomen ja vieraiden valtioiden välisten sopimusten valmistelusta vastaa ulkoasiainministeriössä toimiva NSA, ja valmisteluun osallistuvat kaikki ne hallinnonalat, joiden asiantuntemusta pidetään kulloinkin tarpeellisena.

2.3. Velvoitteet koskevat viranomaisia ja yrityksiä

Kansainvälisiä turvallisuusluokiteltuja tietoaineistoja koskevia sääntöjä sovelletaan viranomaisten lisäksi myös elinkeinonharjoittajiin ja heidän palveluksessa oleviin silloin, kun nämä osallistuvat turvallisuusluokiteltuun hankkeeseen. Valtionhallinnon toimivaltaiset turvallisuusviranomaiset vastaavat siitä, että suomalainen elinkeinoelämä kykenee käsittelemään kansainvälistä turvallisuusluokiteltua tietoa silloin, kun sen haltuun siirtyy vieraan maan tai kansainvälisen järjestön turvallisuusluokiteltua tietoa. Yleiset kansainväliset vaatimukset on pyritty huomioimaan Suomen kansallisessa turvallisuusauditointikriteeristössä (KATAKRI), jota käytetään työkaluna suomalaisten viranomaisten tarkastaessa kotimaisten yritysten ja muiden yhteisöjen turvallisuustason.

3. EUROOPAN UNIONIN TIETOAINEISTO JA SEN KÄSITTELY

Neuvoston turvallisuussäännöt (488/2013) on jäsenvaltioiden kannalta keskeisin EU:n turvallisuusluokiteltujen tietojen suojaamista koskeva säädös. Myös muilla EU:n toimielimillä on omia turvallisuussääntöjä, joissa ne ovat sitoutuneet noudattamaan vastaavia turvallisuusvaatimuksia. Neuvoston turvallisuussäännöistä annettu päätös on soveltamisalaltaan laaja. Päätöksessä säädetään mm. EU:n asiakirjojen turvallisuusluokittelusta, tietojen käsittelystä, fyysisestä turvallisuudesta, henkilöstön luotettavuusselvitysmenettelystä, tietojen turvaamisesta tietojärjestelmissä sekä tietojen luovuttamisesta kolmansille valtioille ja kansainvälisille järjestöille.

3.1. Yleisiä periaatteita

EU:n turvallisuusluokiteltuja tietoja on suojattava koko niiden elinkaaren ajan siten, että pystytään estämään ja havaitsemaan niiden vaarantuminen tai katoaminen. Tällaiset turvatoimet liittyvät erityisesti EU:n turvallisuusluokiteltujen tietojen tuottamiseen, rekisteröimiseen, kopioimiseen, kuljettamiseen, säilyttämiseen ja hävittämiseen. EU:n turvallisuusluokitelluille tiedoille annetaan suojaa niiden turvallisuusluokituksen mukaisesti. Mitä korkeampaan turvallisuusluokkaan aineisto kuuluu, sitä tiukempia turvatoimia edellytetään. Suurin osa turvallisuusluokitelluista tiedoista kuuluu alimpaan RESTREINT UE/EU RESTRICTED turvallisuusluokkaan. Turvallisuusluokkiin CONFIDENTIEL UE/EU CONFIDENTIAL ja SECRET UE/EU SECRET kuuluvia aineistoja laaditaan harvemmin ja näitä koskevat turvatoimet ovat huomattavasti kireämmät.

3.2. EU:n julkinen tieto

Euroopan unionin tieto on julkista, jos siihen ei kohdistu avoimuusasetuksessa säädettyjä tiedonsaantirajoituksia. Komission ja neuvoston julkiset asiakirjat ilmenevät mm. näiden ylläpitämistä julkisista asiakirjarekisteristä.

3.3. LIMITE-asiakirjat

”LIMITE”-merkintä ei ole turvallisuusluokitusta osoittava merkintä, vaan jakelumerkintä. Merkinnällä osoitetaan, että asiakirja on tarkoitettu sisäiseen jakeluun neuvostolle, sen jäsenille, komissiolle ja tietyille muille EU:n toimielimille ja elimille.

Asiakirjan mahdollisen salassapidon kansallisesti tulee perustua julkisuuslakiin, esimerkiksi julkisuuslain 24 §:n 1 momentin 2 kohtaan.

LIMITE

Kyseessä on EU:n sisäinen asiakirjan jakelurajoite.

- **toimitiloille** ei aseteta vaatimuksia
- **tietojärjestelmille** ei aseteta vaatimuksia
- **tiedonsiirrolle** ei aseteta vaatimuksia
- tietoa saa siirtää **Internetin** välityksellä ilman salausta
- saa **kopioida** tavallisella kopiokoneella
- saa **lähettää** postitse
- saa **hävittää** paperirepijällä tai hävityspalvelua käyttäen.

3.4. EU:n turvallisuusluokiteltu tieto

Turvallisuusluokiteltu EU-tieto, josta käytetään kansainvälistä lyhennettä EUCI (*European Union Classified Information*), tarkoittaa mitä tahansa tietoa tai materiaalia, jolle on määritetty jokin EU:n turvallisuusluokka ja jonka aiheeton paljastuminen saattaisi aiheuttaa eritasoista vahinkoa EU:n tai jonkin sen jäsenmaan eduille.

EU-tiedon turvallisuusluokittelusta vastaa se EU-taho, jonka tiedosta on kyse. **Turvallisuusluokitellun EU-tiedon luokituksen muuttaminen tai poistaminen voi tapahtua vain sen luvalla, jolta tieto on peräisin.**

EU:ssa ja Suomessa käytettävien turvallisuusluokitusmerkintöjen vastaavuudet:

Euroopan unionin turvallisuusluokka	**EU-lyhenne**	**Suomen vastaava turvallisuusluokka (tietoturvallisuusasetus)**
TRES SECRET UE / EU TOP SECRET	TS-UE/ EU-TS	ERITTÄIN SALAINEN / YTTERST HEMLIG
SECRET UE / EU SECRET	S-UE/EU-S	SALAINEN / HEMLIG
CONFIDENTIEL UE / EU CONFIDENTIAL	C-UE/EU-C	LUOTTAMUKSELLINEN / KONFIDENTIELL
RESTREINT UE / EU RESTRICTED	R-UE/EU-R	KÄYTTÖ RAJOITETTU / BEGRÄNSAD TILLGÅNG

EU:n asiakirjat on luokiteltava aina vähintään siihen turvallisuusluokkaan, joka vastaa asiakirjan korkeinta luokittelua sisältävää tietoa. Asiakirjan eri osat voivat kuulua keskenään eri turvallisuusluokkiin,jolloin ne merkitään vastaavasti. Suurissa tietoaineistoissa on harkittava erikseen, nouseeko asiakokonaisuus luokitukseltaan yksittäistä tietoa korkeampaan turvallisuusluokkaan (ns. agregaatioefekti).

HENKILÖSTÖ

EU:n turvallisuusluokiteltua tietoa saa luovuttaa vain sellaiselle henkilöille, joilla on viranomaisen hyväksymä työtehtäviin liittyvä tarve kyseiseen tietoon. Henkilön tulee perehtyä EU:n turvallisuusluokitellun tiedon suojaamista koskeviin velvoitteisiin, ennen kuin hänelle voidaan luovuttaa kyseistä tietoa.

Mikäli henkilö käsittelee CONFIDENTIAL UE / EU CONFIDENTIAL tai sitä korkeamman tason EU:n turvallisuusluokiteltua tietoa, hänellä tulee tulla kansallisen turvallisuusviranomaisen myöntämä henkilöturvallisuustodistus (personnel security clearance, PSC). Työnantajan on määriteltävä PSC todistusta edellyttävät tehtävät ja pidettävä tästä ajan tasalla olevaa luetteloa. PSC-todistus perustuu Suojelupoliisin turvallisuusselvityslain (726/2014) nojalla tekemään turvallisuusselvitykseen. PSC-todistusta ja turvallisuusselvitystä ei kuitenkaan edellytetä niistä henkilöistä, joille luovutetaan tarpeeseen perustuen korkeintaan RESTREINT UE / EU RESTRICTED -luokan tietoa.

Linkki NSA:n sivuille, josta löytyy ohje PSC-todistuksen hakemisesta

TILAT

Fyysinen turvallisuus on mitoitettava siten, että EU:n turvallisuusluokiteltuun tietoon ei ole mahdollisuutta päästä käsiksi oikeudetta. Vaatimus koskee kaikkia niitä tiloja, joissa EU:n turvallisuusluokiteltua tietoa käsitellään tai säilytetään. Toimivaltaisen viranomaisen hyväksyntää edellytetään tilojen osalta riippuen turvallisuusluokan tasosta. EU:n turvallisuusluokitellun tiedon käsittely on turvallisuusluokasta riippuen mahdollista kolmella eritasoisella alueella:

- **hallinnolliset alueet**,
- pääsynvalvonnan piiriin kuuluvat varsinaiset **turva-alueet** ja
- **teknisin keinoin suojatut turva-alueet**, joissa salakuuntelu on estetty.

JÄRJESTELMÄT

Tietojärjestelmät, joilla EU:n turvallisuusluokiteltua tietoa siirretään tai käsitellään, tulee erikseen hyväksyttää toimivaltaisella turvallisuusviranomaisella (akkreditointi)(SAA). Tietojärjestelmissä, joissa käsitellään vähintään turvallisuusluokan CONFIDENTIEL UE / EU CONFIDENTIAL -tietoa, tulee lisäksi huomioida sähkömagneettisen hajasäteilyn vaarat jatoteuttaa keinot niiden minimoimiseksi (ns. TEMPEST-toimet).

Kun EU:n turvallisuusluokiteltua tietoa siirretään tietojärjestelmissä ja niiden kesken, tieto tulee salata kansallisen tietoturvatuotteiden hyväksyntäviranomaisen (CAA) hyväksymillä salaamismenetelmillä. Ennen kuin tietojärjestelmissä tai niiden välillä voidaan siirtää SECRET UE / EU SECRET -luokan tietoa, käytettävä salaamismenetelmä tai tietoturvatuote tulee hyväksyttää EU:n neuvoston tietoturvatuotteiden hyväksyntäviranomaisella. Tämä koskee myös niitä suomalaisia tietojärjestelmiä, joihin SECRET UE / EU SECRET -luokan järjestelmästä on yhteys.

3.4.1 RESTREINT UE / EU RESTRICTED

Kyseessä on turvallisuusluokka, jonka mukaan

- **henkilöllä** tulee olla viranomaisen hyväksymä, työtehtävään liittyvä tarve turvallisuusluokiteltuun tietoon (need-to-know) ja hänen tulee **perehtyä** turvallisuusluokan mukaisiin velvoitteisiin

- **toimitiloille** ei aseteta erityisvaatimuksia, mutta RESTREINT UE / EU RESTRICTED -luokan aineistoa käsiteltäessä tila on pidettävä lukittuna, kun sieltä poistutaan. Kyseinen aineisto tulee säilyttää lukitussa paikassa, eivätkä sivulliset saa päästä tutustumaan aineistoon

- **tietojärjestelmä** tulee erikseen hyväksyttää toimivaltaisella viranomaisella (NCSA-FI)
- **tietoa sähköisesti siirrettäessä** salausmenetelmän tulee olla toimivaltaisen viranomaisen (CAA) hyväksymä
- tietoa **ei saa siirtää Internetin** välityksellä, ellei tieto ole salattu tarkoitukseen erikseen hyväksytyllä salaamismenetelmällä

- saa **kopioida** tavallisella kopiokoneella
- saa **lähettää** postitse läpinäkymättömässä kirjekuoressa
- saa **kuljettaa**, huolehdittava suojauksesta
- saa **hävittää** paperirepijällä tai hävityspalvelua käyttäen, mikäli hävityspalvelu on viranomaisten hyväksymä.

3.4.2 CONFIDENTIEL UE / EU CONFIDENTIAL

Kyseessä on turvallisuusluokka, jonka mukaan

- **henkilöllä** tulee olla viranomaisen hyväksymä, työtehtävään liittyvä **tarve** turvallisuusluokiteltuun tietoon (need-to-know)
- henkilöllä tulee olla riittävän tasoinen henkilöturvallisuustodistus (**PSC**)
- henkilön tulee **perehtyä** turvallisuusluokan mukaisiin velvoitteisiin
- työnantajan on myönnettävä henkilölle kirjallisesti **oikeus** CONFIDENTIEL UE / EU CONFIDENTIAL -luokan tiedon käsittelyyn

- CONFIDENTIEL UE / EU CONFIDENTIAL -luokan tietoa voidaan käsitellä hallinnollisella alueella, mikäli pääsy tietoihin on suojattu sivullisilta. Tällöin on huolehdittava, ettei tilaan ole näköyhteyttä ulkopuolelta
- CONFIDENTIEL UE / EU CONFIDENTIAL -luokan tieto tulee säilyttää kansallisesti hyväksytyssä kassakaapissa aina huonetilasta poistuttaessa, ellei tila ole tarkoitukseen hyväksytty, hälytysjärjestelmällä varustettu holvi.

- **tietojärjestelmä** tulee erikseen hyväksyttää toimivaltaisella viranomaisella (NCSA-FI).
- kansallisten tietoverkkojen liittäminen EU:n luokiteltuun tietoverkkoon tulee hyväksyttää kansallisella toimivaltaisella viranomaisella (SAA)
- mikäli CONFIDENTIEL UE / EU CONFIDENTIAL -luokan tietoa käsitellään sähköisesti, sähkömagneettinen hajasäteily on estettävä riittävän tehokkaasti (ns. TEMPEST-toimet)
- tietoa **sähköisesti siirrettäessä** salausmenetelmän tulee olla EU:n turvallisuusviranomaisen tai kansallisen toimivaltaisen viranomaisen (CAA) hyväksymä
- tietoa ei saa siirtää **Internetin** välityksellä, ellei tieto ole salattu tarkoitukseen erikseen hyväksytyllä salaamismenetelmällä

- **rekisteröitävä** ennen lähettämistä, vastaanotettaessa ja hävitettäessä
- ei saa **kopioida** tavallisella kopiokoneella. Kopiokoneessa ei saa olla verkkoyhteyttä ja sen massamuistin tulee olla työyksikön turvallisuusvastaavan hallinnassa (ei huoltomiestä yksin koneelle).
- saa **lähettää** EU:n alueella kaupallista kuriiripalvelua koskevien vaatimusten mukaisesti kirjattuna kahdessa läpinäkymättömässä kirjekuoressa tai lukitussa ja/tai sinetöidyssä kuljetuspussissa. Uloimmassa kuoressa ei saa olla merkintää turvallisuusluokituksesta. Unionin alueelta kolmanteen valtioon ainoastaan kuriiritse.

- saa **kuljettaa** suljettuna kirjekuoreen, jossa vastaanottajana oma organisaatio. Kuljetusvälinettä (salkku tms.) ei saa jättää vartioimatta.
- saa **hävittää** DIN4-paperirepijällä (rekisterinpitäjä kirjaamossa).

3.4.3 SECRET UE / EU SECRET

Kyseessä on turvallisuusluokka, jonka mukaan

- **henkilöllä** tulee olla viranomaisen hyväksymä, työtehtävään liittyvä **tarve** turvallisuusluokiteltuun tietoon (need-to-know)
- henkilöllä tulee olla riittävän tasoinen henkilöturvallisuustodistus (**PSC**)
- henkilön tulee **perehtyä** turvallisuusluokan mukaisiin velvoitteisiin
- työnantajan on myönnettävä henkilölle kirjallisesti **oikeus** SECRET UE / EU SECRET -luokan tiedon käsittelyyn

- SECRET UE / EU SECRET -luokan tietoa voidaan käsitellä hallinnollisella alueella, mikäli pääsy tietoihin on suojattu sivullisilta. Tällöin on huolehdittava, ettei tilaan ole näköyhteyttä ulkopuolelta.
- SECRET UE / EU SECRET -luokan tieto tulee säilyttää kansallisesti hyväksytyssä kassakaapissa aina huonetilasta poistuttaessa, ellei tila ole tarkoitukseen hyväksytty, hälytysjärjestelmällä varustettu holvi.
-

- **tietojärjestelmä** tulee hyväksyttää erikseen toimivaltaisella viranomaisella (NCSA-FI).
- kansallisten tietoverkkojen liitännät EU:n luokiteltuun tietoverkkoon tulee hyväksyttää kansallisella toimivaltaisella viranomaisella (SAA)
- mikäli SECRET UE / EU SECRET -luokan tietoa käsitellään sähköisesti, sähkömagneettinen hajasäteily on estettävä riittävän tehokkaasti (ns. TEMPEST-toimet)

- SECRET UE / EU SECRET -luokan **tietoa siirtävissä** tietojärjestelmissä tai kyseisten tietojärjestelmien välillä käytettävä salaamismenetelmä tai tietoturvatuote tulee hyväksyttää EU:n neuvoston tietoturvatuotteiden hyväksyntäviranomaisella. Tämä koskee myös niitä suomalaisia tietojärjestelmiä, joihin SECRET UE / EU SECRET -luokan järjestelmästä on yhteys. tietoa ei saa siirtää **Internetin** välityksellä, ellei tieto ole salattu tarkoitukseen EU:n turvallisuusviranomaisten nimenomaisesti hyväksymällä salaamismenetelmällä

- **rekisteröitävä** ennen lähettämistä, vastaanotettaessa ja hävitettäessä
- ei saa **kopioida** tavallisella kopiokoneella. Kopiokoneessa ei saa olla verkkoyhteyttä ja sen massamuistin tulee olla työyksikön turvallisuusvastaavan hallinnassa (ei huoltomiestä yksin koneelle).
- saa **lähettää** ainoastaan kuriiritse

- saa **kuljettaa** kuriirimenettelyn vaatimukset (kuriiritodistus jne.) huomioiden suljettuna kirjekuoreen, jossa vastaanottajana oma organisaatio. Avataan virallisesti vastaanottopäässä. Kuljetusvälinettä (salkku tms.) ei saa jättää vartioimatta.
- saa **hävittää** DIN4-paperirepijällä (rekisterinpitäjä kirjaamossa).

3.4.4 TRES SECRET UE / EU TOP SECRET

TRES SECRET UE / EU TOP SECRET -asiakirjojen laatiminen ja käsittely EU:ssa ja sen jäsenmaissa on hyvin harvinaista. Niiden käsittelyssä edellytetään SECRET UE / EU SECRET -luokan vaatimuksia, mutta käsittelijän henkilövalintaan liittyy lisäksi erikseen ratkaistavia erityistoimenpiteitä (käsittelyoikeudet ja turvallisuusselvitystasomäärittelyt). Lisäksi kyseisen luokan asiakirjojen rekisteröinti ja hävittäminen poikkeavat alemmista turvallisuusluokista (mm. rekisteröinti erillisrekisteriin), eikä tämän turvallisuusluokan tietojärjestelmästä saa olla yhteyksiä suojaamattomiin verkkoihin.

4. NATON TIETOAINEISTO JA SEN KÄSITTELY

Naton ja Suomen tekemän tietoturvallisuussopimuksen (SopS 7 ja 8/2013) mukaisesti sopimuspuolet suojelevat toistensa turvallisuusluokiteltua tietoa. Nato:lla on erillinen, sisäisesti hyväksytty säännöstö turvallisuusluokitellun tiedon käsittelemisestä. Suomen ja Naton välisessä tietoturvallisuussopimuksessa Suomi on sitoutunut kunnioittamaan Naton turvallisuussäännöstössä esitettyjä vaatimuksia riittävillä kansallisilla toimenpiteillä.

Suomen viranomaisten asiakirjoihin sovelletaan julkisuusperiaatetta. Naton asiakirjoihin sovelletaan salassapitoperiaatetta. Voimassa oleva Naton turvallisuussäännöstö pohjautuu dokumentaatiokokonaisuuteen, josta käytetään nimitystä *Nato Security Policy* (NSP). Turvallisuussäännöstön käytännön ylläpitotyön toteuttaa Naton turvallisuusyksikkö NOS (*Nato Office of Security*).

Mikäli Natolle luovutettu tieto on turvallisuusluokiteltua, tiedon luovuttaneen maan määräysvalta asiakirjaan säilyy, eikä tietoa voida Natossa luokitella uudestaan ilman sen luovuttaneen maan kirjallista lupaa.

Nato edellyttää jäsenmailtaan ja sopimuskumppanimailtaan keskitettyä turvallisuusluokitellun tiedon hallintaa. Tämä tarkoittaa keskusrekisterin (enintään kaksi maata kohti) ja alarekistereiden perustamista. Suomen Nato-keskusrekisteri sijaitsee ulkoasiainministeriössä.

4.1. Naton julkinen tieto

Julkista on sellainen Naton tieto, jota ei ole turvallisuusluokiteltu ja jonka asiasta vastuussa oleva Naton toimielin tai virasto julkaisee.

4.2. Naton luokittelematon tieto

Naton sisäiseen käyttöön tarkoitettu tieto, jota ei ole turvallisuusluokiteltu, merkitään turvallisuusluokan sijasta jakelurajoitemerkinnällä NATO UNCLASSIFIED (NU). Kyseistä tietoa voidaan luovuttaa harkinnanvaraisesti Naton jäsenmaiden viranomaisten ulkopuolelle ilman turvallisuusluokitellun tiedon käsittelylle asetettuja edellytyksiä.

NATO UNCLASSIFIED

Kyseessä on jakelurajoite.

- **henkilöllä** tulee olla viranomaisen hyväksymä, työtehtävään liittyvä tarve tietoon ja hänen tulee ymmärtää asiakirjan jakelurajoitteisuuden merkitys
- **toimitiloille** ei aseteta vaatimuksia
- **tietojärjestelmille** ei aseteta vaatimuksia
- **tiedonsiirrolle** ei aseteta vaatimuksia
- voidaan siirtää **Internetin** välityksellä salaamattomana
- saa **kopioida** tavallisella kopiokoneella
- saa **lähettää** postitse
- saa **hävittää** paperirepijällä tai hävityspalvelua käyttäen.

4.3. Naton turvallisuusluokiteltu tieto

Naton turvallisuusluokiteltu tieto tarkoittaa mitä tahansa tietoa tai materiaalia, jolle on määritetty jokin Naton turvallisuusluokka ja jonka aiheeton paljastuminen saattaisi aiheuttaa eritasoista vahinkoa Naton tai jonkin sen jäsenmaan eduille.

MERKINNÄT Naton ja Suomen turvallisuusluokitusmerkintöjen vastaavuudet:

Naton turvallisuusluokka	**Lyhenne**	**Suomen vastaava turvallisuusluokka (tietoturvallisuusasetus)**
COSMIC TOP SECRET	CTS	ERITTÄIN SALAINEN / YTTERST HEMLIG
NATO SECRET	NS	SALAINEN / HEMLIG
NATO CONFIDENTIAL	NC	LUOTTAMUKSELLINEN / KONFIDENTIELL
NATO RESTRICTED	NR	KÄYTTÖ RAJOITETTU / BEGRÄNSAD TILLGÅNG

Turvallisuusluokkamerkintä liitetään Naton asiakirjoihin jokaiselle sivulle sekä sivun ylä- että alalaitaan. Merkintä tehdään lisäksi viimeisen sivun kääntöpuolelle. Naton asiakirjat on luokiteltava aina vähintään siihen turvallisuusluokkaan, joka vastaa asiakirjan korkeinta luokittelua sisältävää tietoa. Suurissa tietoaineistoissa on harkittava erikseen, nouseeko

asiakokonaisuus luokitukseltaan yksittäistä tietoa korkeampaan turvallisuusluokkaan (ns. agregaatioefekti).

Nato-tiedon turvallisuusluokittelusta vastaa asiakirjan laatinut taho. **Turvallisuusluokitellun Nato-tiedon luokituksen laskeminen tai julistaminen julkiseksi tiedoksi voi tapahtua vain asiakirjan laatineen etukäteen antamalla kirjallisella luvalla.**

Naton turvallisuusluokitellun tiedon jakelua voidaan hallita ja rajoittaa turvallisuusluokkamerkinnän yhteyteen sijoitettavien jakelumerkintöjen avulla. Tämä tulee kysymykseen erityisesti silloin, kun asiakirja tai materiaali jaetaan ns. kolmannelle osapuolelle. Seuraavassa on kolme esimerkkiä turvallisuusluokittelu- ja jakelumerkintöjen käytöstä:

1. Kohdeorganisaatio tai operaatio ja turvallisuusluokitus, esimerkiksi

ISAF CONFIDENTIAL

2. Jos pääsy ko. tietoaineistoon on rajoitettu vain tietyille rauhankumppanuusmaille, on merkintä esim.

NATO / PfP RESTRICTED

FINLAND AND SWEDEN ONLY

3. Jos pääsy ko. tietoaineistoon on sallittu esim. kaikille tiettyyn kriisinhallintaoperaatioon osallistuville valtioille, on merkintä esim.

NATO / CONFIDENTIAL

RELEASABLE to KFOR

HENKILÖSTÖ

Naton turvallisuusluokiteltua tietoa saa luovuttaa vain sellaisille henkilöille, joilla on kansallisen viranomaisen hyväksymä tarve kyseiseen tietoon. Henkilön tulee perehtyä Naton turvallisuusluokitellun tiedon suojaamista koskeviin velvoitteisiin, ennen kuin hänelle voidaan luovuttaa kyseistä tietoa.

Mikäli henkilö käsittelee NATO CONFIDENTIAL tai sitä korkeamman tason Naton turvallisuusluokiteltua tietoa, hänellä tulee tulla kansallisen turvallisuusviranomaisen myöntämä henkilöturvallisuustodistus (personnel security clearance, PSC). Työnantajan on määriteltävä PSC todistusta edellyttävät tehtävät ja pidettävä tästä ajan tasalla olevaa luetteloa. PSC-todistus perustuu Suojelupoliisin turvallisuusselvityslain

(177/2002) nojalla tehtyyn turvallisuusselvitykseen. PSC-todistusta ja turvallisuusselvitystä ei kuitenkaan edellytetä niistä henkilöistä, joille luovutetaan tarpeeseen perustuen korkeintaan NATO RESTRICTED -luokan tietoa.

Linkki NSA:n sivuille, josta löytyy ohje PSC-todistuksen hakemisesta

TILAT

Fyysinen turvallisuus on mitoitettava siten, että Naton turvallisuusluokiteltuun tietoon ei ole mahdollisuutta päästä käsiksi oikeudetta. Vaatimus koskee kaikkia niitä tiloja, joissa Naton turvallisuusluokiteltua tietoa käsitellään tai säilytetään. Mikäli käsiteltävän tiedon luokka on vähintään NATO SECRET, tulee säilytystilan turvallisuustaso hyväksyttää vastuuviranomaisella.

JÄRJESTELMÄT

Kaikki sellaiset **tietojärjestelmät**, joissa siirretään Naton turvallisuusluokiteltua tietoa, tulee erikseen hyväksyttää toimivaltaisella turvallisuusviranomaisella (akkreditointi). Tietojärjestelmien, joissa siirretään vähintään NATO SECRET -luokan tietoa, tulee olla Naton sotilaskomitean hyväksymiä. Tämä koskee myös niitä suomalaisia tietojärjestelmiä, joihin NATO SECRET -järjestelmästä on yhteys ja joissa Naton turvallisuusluokiteltua tietoa siirretään. Tietojärjestelmissä, joissa käsitellään vähintään turvallisuusluokan NATO CONFIDENTIAL -tietoa, tulee lisäksi huomioida sähkömagneettisen hajasäteilyn vaarat ja etsiä keinot niiden minimoimiseksi (ns. TEMPEST-toimet).

Kun Naton turvallisuusluokiteltua tietoa siirretään Naton tietojärjestelmän ja kotimaisen tietojärjestelmän välillä, tieto tulee salata Naton sotilaskomitean hyväksymällä menetelmällä. Kun Naton turvallisuusluokiteltua tietoa siirretään kansallisissa järjestelmissä, siinä käytettävät salaamisjärjestelyt tulee hyväksyttää Naton sotilaskomitealla aina, kun siirrettävän tiedon turvallisuusluokka on NATO SECRET. Alemman turvallisuusluokan Nato-tiedon siirtämiseen käytettävät salausjärjestelyt voidaan hyväksyttää Suomen toimivaltaisella viranomaisella (NCSA-FI), mikäli Nato sen kussakin tapauksessa erikseen hyväksyy.

4.3.1 NATO RESTRICTED

Kyseessä on turvallisuusluokka, jonka mukaan

- **henkilöllä** tulee olla viranomaisen hyväksymä, työtehtävään liittyvä tarve turvallisuusluokiteltuun tietoon (need-to-know) ja hänen tulee **perehtyä** turvallisuusluokan mukaisiin velvoitteisiin

- **toimitiloille** ei aseteta erityisvaatimuksia, mutta NATO RESTRICTED -luokan aineistoa käsiteltäessä tila on pidettävä lukittuna, kun sieltä poistutaan. Kyseinen aineisto tulee säilyttää lukitussa paikassa, eivätkä sivulliset saa päästä tutustumaan aineistoon

- **tietojärjestelmä** tulee erikseen hyväksyttää toimivaltaisella viranomaisella

- tietoa **sähköisesti siirrettäessä** salausmenetelmän tulee olla Naton tai toimivaltaisen viranomaisen hyväksymä
- tietoa ei saa siirtää **Internetin** välityksellä, ellei tieto ole salattu tarkoitukseen erikseen hyväksytyllä salaamismenetelmällä

- saa **kopioida** tavallisella kopiokoneella
- saa **lähettää** postitse läpinäkymättömässä kirjekuoressa
- saa **kuljettaa**, huolehdittava suojauksesta
- saa **hävittää** paperirepijällä tai hävityspalvelua käyttäen, mikäli hävityspalvelu on viranomaisten hyväksymä.

4.3.2 NATO CONFIDENTIAL

Kyseessä on turvallisuusluokka, jonka mukaan

- **henkilöllä** tulee olla viranomaisen hyväksymä, työtehtävään liittyvä **tarve** turvallisuusluokiteltuun tietoon (need-to-know) henkilöllä tulee olla riittävän tasoinen henkilöturvallisuustodistus (**PSC**)
- henkilön tulee **perehtyä** turvallisuusluokan mukaisiin velvoitteisiin
- työnantajan on myönnettävä henkilölle kirjallisesti **oikeus** NATO CONFIDENTIAL -luokan tiedon käsittelyyn

- **toimitilaan** pääsy tulee valvottu ja käsiteltäessä NATO CONFIDENTIAL -luokan aineistoa pääsy tietoihin on suojattava sivullisilta. Tällöin on huolehdittava, ettei tilaan ole näköyhteyttä ulkopuolelta.
- NATO CONFIDENTIAL -luokan tieto tulee säilyttää kansallisesti hyväksytyssä kassakaapissa aina huonetilasta poistuttaessa, ellei tila ole tarkoitukseen hyväksytty, hälytysjärjestelmällä varustettu holvi.
-
- **tietojärjestelmä** tulee erikseen hyväksyttää toimivaltaisella viranomaisella
- mikäli NATO CONFIDENTIAL -luokan tietoa käsitellään sähköisesti, sähkömagneettinen hajasäteily on estettävä riittävän tehokkaasti (ns. TEMPEST-toimet)

- tietoa **sähköisesti siirrettäessä** salausmenetelmän tulee olla Naton tai toimivaltaisen viranomaisen hyväksymä
- tietoa ei saa siirtää **Internetin** välityksellä, ellei tieto ole salattu tarkoitukseen erikseen hyväksytyllä salaamismenetelmällä

- rekisteröitävä ennen lähettämistä ja vastaanotettaessa
- ei saa **kopioida** tavallisella kopiokoneella. Kopiokoneessa ei saa olla verkkoyhteyttä ja sen massamuistin tulee olla työyksikön turvallisuusvastaavan hallinnassa (ei huoltomiestä yksin koneelle).
- saa **lähettää** ainoastaan kuriiritse
- saa **kuljettaa** suljettuna kirjekuoreen, jossa vastaanottajana oma organisaatio. Kuljetusvälinettä (salkku tms.) ei saa jättää vartioimatta.
- saa **hävittää** DIN4-paperirepijällä.

4.3.3 NATO SECRET

Kyseessä on turvallisuusluokka, jonka mukaan

- **henkilöllä** tulee olla viranomaisen hyväksymä, työtehtävään liittyvä **tarve** turvallisuusluokiteltuun tietoon (need-to-know) henkilöllä tulee olla riittävän tasoinen henkilöturvallisuustodistus (**PSC**)
- henkilön tulee **perehtyä** turvallisuusluokan mukaisiin velvoitteisiin
- työnantajan on myönnettävä henkilölle kirjallisesti **oikeus** NATO SECRET -luokan tiedon käsittelyyn.

- **toimitilaan** pääsyä tulee valvoa siten, että järjestelyllä estetään muita kuin NATO SECRET -luokan aineiston käsittelyoikeuden omaavia pääsemään tilaan valvomatta. Tila tulee olla erikseen hyväksytty NATO SECRET -luokan tiedon käsittelyyn ja se tulee olla varustettu kulunvalvontajärjestelmällä
- NATO SECRET -luokan tieto tulee säilyttää kansallisesti hyväksytyssä kassakaapissa aina huonetilasta poistuttaessa, ellei tila ole tarkoitukseen hyväksytty, hälytysjärjestelmällä varustettu holvi.
- on huolehdittava, ettei tilaan ole näköyhteyttä ulkopuolelta silloin, kun siellä käsitellään NATO SECRET -luokan aineistoa

- **tietojärjestelmä** tulee erikseen hyväksyttää Naton sotilaskomitealla
- mikäli NATO SECRET -luokan tietoa käsitellään sähköisesti, sähkömagneettinen hajasäteily on estettävä riittävän tehokkaasti (ns. TEMPEST-toimet)

- tietoa **sähköisesti siirrettäessä** salausmenetelmän tulee olla Naton sotilaskomitean erikseen hyväksymä
- tietoa ei saa siirtää **Internetin** välityksellä, ellei tieto ole salattu Naton sotilaskomitean tähän nimenomaiseen tarkoitukseen erikseen hyväksymällä salaamismenetelmällä

- **Rekisteröitävä** ennen lähettämistä, vastaanottaessa ja hävitettäessä
- ei saa **kopioida** tavallisella kopiokoneella. Kopiokoneessa ei saa olla verkkoyhteyttä ja sen massamuistin tulee olla työyksikön turvallisuusvastaavan hallinnassa (ei huoltomiestä yksin koneelle). Jokainen kopio on numeroitava ja rekisteröitävä.
- saa **lähettää** ainoastaan kuriiritse
- saa **kuljettaa** kuriirivelvoittein ja -dokumentaatioin varustettuna suljetussa kirjekuoressa, jossa vastaanottajana oma organisaatio. Kuljetusvälinettä (salkku tms.) ei saa jättää missään oloissa vartioimatta. Lähetys tulee avata dokumentoidusti.
- **hävitetään** vähintään DIN4-paperirepijällä arkistonhoidollisin toimenpitein (Rekisterinpitäjä)

4.3.4 NATO (COSMIC) TOP SECRET

NATO COSMIC TOP SECRET -asiakirjojen luovuttaminen Naton jäsenmaiden ulkopuolelle on hyvin harvinaista ja edellyttää erillistä hyväksymisprosessia.

5. MUIDEN VALTIOIDEN JA KANSAINVÄLISTEN JÄRJESTÖJEN TIETOAINEISTON KÄSITTELY

Kansainvälisissä turvallisuusluokiteltuja tietoja koskevissa sopimuksissa osapuolet sitoutuvat turvallisuusluokitellun tiedon vastavuoroiseen suojaamiseen: toisen osapuolen turvallisuusluokitellulle tiedolle annetaan samantasoinen suoja kuin omalle vastaavaan turvallisuusluokkaan kuuluvalle tiedolle. Tätä varten sopimuksissa määritetään turvallisuusluokkien vastaavuudet ja yleiset periaatteet turvallisuusluokitellun tiedon vaihtamisesta. Sopimuksissa rajoitetaan turvallisuusluokitellun tiedon käyttö vain siihen tarkoitukseen, jota varten se on luovutettu. Sopimuksissa määritellään, missä tilanteissa sopimuspuolten lainsäädännön alaisuuteen kuuluvista yrityksistä ja yhteisöistä sekä henkilöistä laaditaan turvallisuusselvitys edellytyksenä turvallisuusluokiteltujen tietojen käsittelylle. Henkilöille myönnettävistä turvallisuustodistuksista käytetään nimitystä PSC (*Personal Security Clearance*) tai PSCC (*Personal Security Clearance Certificate*). Vastaavasti yrityksille ja muille yhteisöille myönnettävä turvallisuustodistus kantaa nimitystä FSC (*Facility Security Clearance*).

Linkki voimassa oleviin tietoturvallisuussopimuksiin

LYHENTEET

CAA	Crypto Approval Authority, Suomessa viestintäviraston NCSA-FI:ssa
DSA	Designated Security Authority, määrätty turvallisuusviranomainen
FSC	Facility Security Clearance, yhteisöturvallisuusselvitys
NSA	National Security Authority, kansallinen turvallisuusviranomainen
PSC	Personnel Security Clearance, henkilöturvallisuustodistus
PSCC	Personnel Security Clearance Certificate, ks. PSC
SAA	Security Accreditation Authority, Suomessa viestintäviraston NCSA-FI:ssa

EU:ssa JA SEN JÄSENMAISSA KÄYTETTÄVIEN TURVALLISUUSLUOKKIEN VASTAAVUUS

EU-TURVALLISUUS-LUOKKA	**TRES SECRET UE / EU TOP SECRET**	**SECRET UE / EU SECRET**	**CONFIDENTIEL UE / EU CONFIDENTIAL**	**RESTREINT UE / EU RESTRICTED**
Alankomaat	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Belgia	Très Secret (Loi 11.12.1998) Zeer Geheim (Wet 11.12.1998)	Secret (Loi 11.12.1998) Geheim (Wet 11.12.1998)	Confidentiel (Loi 11.12.1998) Vertrouwelijk (Wet 11.12.1998)	*ks. huomautus 1*
Bulgaria	Строго секретно	Секретно	Поверително	За служебно ползване
Espanja	SECRETO	RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
Irlanti	Top Secret	Secret	Confidential	Restricted
Italia	Segretissimo	Segreto	Riservatissimo	Riservato
Itävalta	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Kreikka	Άκρως Απόρρητο Abr: ΑΑΠ	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Kypros	Άκρως Απόρρητο Abr: (ΑΑΠ)	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Kroatia	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Latvia	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Liettua	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Luxemburg	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Malta *ks. huomautus 2*	L-Ogħla Segretezza Top Secret	Sigriet Secret	Kunfidenzjali Confidential	Ristrett Restricted
Portugali	Muito Secreto	Secreto	Confidencial	Reservado
Puola	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Ranska	Très Secret Défense	Secret Défense	Confidentiel Défense	*ks. huomautus 3*
Romania	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu

Ruotsi *ks. huomautus 4*	HEMLIG/TOP SECRET HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG/SECRET HEMLIG	HEMLIG/CONFIDENTIAL HEMLIG	HEMLIG/RESTRICTED HEMLIG
Saksa	STRENG GEHEIM	GEHEIM	VS — VERTRAULICH (*ks. huomautus 5)*	VS — NUR FÜR DEN DIENSTGEBRAUCH
Slovakia	Prísne tajné	Tajné	Dôverné	Vyhradené
Slovenia	STROGO TAJNO	TAJNO	ZAUPNO	INTERNO
Suomi	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Tanska	YDERST HEMMELIGT	HEMMELIGT	FORTROLIGT	TIL TJENESTEBRUG
Tsekin tasavalta	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Unkari	Szigorúan titkos!	Titkos!	Bizalmas!	Korlátozott terjesztésű!
Viro	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Yhdistynyt kuningaskunta	UK TOP SECRET	UK SECRET	UK CONFIDENTIAL *ks. huomautus 6*	UK RESTRICTED

HUOMAUTUKSET

1: Diffusion Restreinte / Beperkte Verspreiding ei ole Belgiassa turvaluokka. Belgia käsittelee ja suojaa RESTREINT UE/EU RESTRICTED -tiedot vähintään yhtä tiukasti kuin Euroopan unionin neuvoston turvallisuussäännöissä kuvatut vaatimukset ja menettelyt edellyttävät.
2: Maltassa voidaan käyttää sekä maltan- että englanninkielisiä merkintöjä..
3: Ranska ei käytä turvallisuusluokkaa RESTREINT kansallisessa järjestelmässään. Ranska käsittelee ja suojaa RESTREINT UE/EU RESTRICTED -tiedot vähintään yhtä tiukasti kuin Euroopan unionin neuvoston turvallisuussäännöissä kuvatut vaatimukset ja menettelyt edellyttävät.
4: Ruotsi: ylemmällä rivillä olevia turvaluokitusmerkintöjä käytetään puolustusvoimissa, ja alemmalla rivillä olevia merkintöjä käyttävät muut viranomaiset.
5: Saksa: VS = Verschlusssache.
6: Yhdistynyt kuningaskunta siirtyy 1.4.2014 kolmiportaiseen turvallisuusluokitteluun. Yhdistynyt kuningaskunta luopuu UK CONFIDENTIAL turvallisuusluokasta ja käsittelee CONFIDENTIEL UE/EU CONFIDENTIAL –tiedot UK SECRET turvallisuusluokkaa koskevien turvatoimien mukaisesti. UK RESTRICTED muuttuu sitä vastaavaksi UK OFFICIAL-SENSITIVE turvallisuusluokaksi.