



## Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta annetun valtioneuvoston asetuksen 9 §:n muuttamisesta

### 1 Johdanto

Pääministeri Petteri Orpon hallitusohjelmassa todetaan hallituksen käynnistävän julkisen hallinnon digitalisaatioon kytkeytyvän laajan lainsäädännön poikkihallinnollisen uudistusohjelman, jossa tunnistetaan ja kumotaan norminpurun hengessä digitalisaatiota estävät tai vaikeuttavat säädökset. Valtiovarainministeriön johtaman digitalisaation ja tiedon liikkuvuuden esteiden purkamisen hankkeen (VM097:00/2024) työpaketissa 4b: Pilvisiirtymän tukeminen – luokiteltu tieto, on tarkasteltu haasteita, jotka liittyvät turvallisuusluokitellun tiedon käsittelyyn pilvipalveluissa. Työpakettia käsitellyt alatyöryhmä on ehdottanut asiakirjojen turvallisuusluokittelusta valtioneuvoston asetuksen (1101/2019), jäljempänä turvallisuusluokitteluasetus muuttamista siten, että se nykyistä selkeämmin mahdollistaisi turvallisuusluokan IV tietojen käsittelyn pilvipalveluissa.

Julkisen hallinnon tiedonhallinnasta annetussa laissa (906/2019), jäljempänä tiedonhallintalaki, säädetään asiakirjojen ja niiden käsittelyn tietoturvallisuusvelvoitteista sekä turvallisuusluokiteltavista asiakirjoista. Turvallisuusluokitteluasetus on säädetty tiedonhallintalain 18 §:n 4 momentin ja kansainvälisistä tietoturvallisuusvelvoitteista annetun lain (588/2004) 8 §:n 2 momentin asetuksenantovaltuuksien nojalla.

Osa turvallisuusluokiteltua tietoa käsittelevistä organisaatioista on kokenut haasteita turvallisuusluokitteluasetuksen vaatimusten toteuttamisessa pilvipalveluita ja muita kehittyviä teknologioita hyödyntäessään. Erityisesti haasteet ovat liittyneet laintulkintakysymyksiin, jotka liittyvät turvallisuusluokitteluasetuksen 9 §:n mukaisten turvallisuusalueiden määrittelyyn ja toteuttamiseen hajautetuissa tietojenkäsittely-ympäristöissä. Nykyaikaisten teknologioiden toimintamallit haastavat osaltaan perinteisiä omien toimitilojen fyysisen suojaamisen menetelmiin liittyviä tietoturvallisuuden toteuttamistapoja, eivätkä omat fyysiset turvallisuusalueet kaikissa tilanteissa enää vastaa tiedonhallintayksiköiden tarpeita tietoturva- ja tietojärjestelmäarkkitehtuurien toteuttamisessa.

Turvallisuusluokitteluasetuksen tulkintaan liittyvät haasteet voivat osaltaan hidastaa julkisen hallinnon digitalisaatiokehitystä ja tuottavuuden parantumista. Haasteet uusimpien teknologioiden hyödyntämisessä turvallisuusluokitellun tiedon käsittelyssä aiheuttavat tarpeetonta hallinnollista taakkaa ja turvallisuusluokiteltujen tietojen käytettävyyden ja käsittelymahdollisuuksien kaventumista. Nykyaikaisilla teknologioilla on usein mahdollista saavuttaa

parempaa tietoturvallisuuden tasoa, minkä vuoksi niiden laajempi hyödyntäminen myös turvallisuusluokittelun tiedon käsittelyssä voi olla perusteltua.

## 2 Asetuksen muuttamisen valmistelu

Valtiovarainministeriön johtaman digitalisaation ja tiedon liikkuvuuden esteiden purkamisen hankkeen alatyöryhmässä 4b: Pilvisiirtymän tukeminen – luokiteltu tieto, on syksyllä 2024 tarkasteltu haasteita, jotka liittyvät turvallisuusluokittelun tiedon käsittelyyn pilvipalveluissa. Asiaa tarkastellut alatyöryhmä ja hankkeen koordinaatioryhmä ovat päätyneet esittämään, että turvallisuusluokitteluasetusta olisi tarpeen tarkistaa sen tulkintaan liittyvien haasteiden poistamiseksi.

Luonnos valtioneuvoston asetukseksi turvallisuusluokitteluasetuksen muuttamisesta on valmisteltu valtiovarainministeriön virkatyönä perustuen kuitenkin digitalisaation ja tiedon liikkuvuuden esteiden purkamisen hankkeessa tehtyyn pohjatyöhön. Valmistelua on tehty tiiviissä yhteistyössä keskeisimpien turvallisuusluokiteltujen tietojen käsittelyn asiantuntijaviranomaisten kanssa. Pohjatyöhön ja keskusteluihin ovat osallistuneet erityisesti Liikenne- ja viestintävirasto Traficom, Valtioneuvoston kanslia ja Puolustusvoimat.

Asetusluonnos oli lausuntokierroksella xx.xx.-xx.xx.xxxx. Lausuntoja saatiin yhteensä x kappaletta. [täydennetään lausuntokierroksen jälkeen]

## 3 Nykytilan kuvaus ja arviointi

Turvallisuusluokitteluasetuksen 9 §:ssä on määritelty turvallisuusalueet, joita ovat turva-alue ja hallinnollinen alue. Turvallisuusluokan IV tietojen käsittelyyn tarkoitetut järjestelmät on turvallisuusluokitteluasetuksen 10 §:n perusteella sijoitettava vähintään hallinnolliselle alueelle.

Hallinnollisen alueen vaatimuksena on turvallisuusluokitteluasetuksen 9 §:n 1 kohdan perusteella, että sillä on selkeästi määritetyt näkyvät rajat ja vain valtionhallinnon viranomaisen valtuuttamilla henkilöillä on alueelle pääsy ilman saattajaa. Turvallisuusluokitteluasetuksen perustelumuition (28.11.2019) mukaan (s.9) hallinnollisella alueella voidaan tarkoittaa esimerkiksi toimistotilaa tai useista eri toimistotiloista muodostuvaa kokonaisuutta, jonne on itsenäinen pääsy ainoastaan tilaa hallinnoivan viranomaisen ennalta valtuuttamilla henkilöillä. Hallinnollista aluetta rajaavalle rakenteelle ei aseteta erityisiä vaatimuksia.

Turvallisuusluokitteluasetus on tarkoitettu teknologianeutraaliksi. Tiedonhallintalain esitöiden mukaan asetuksen tasolla on ollut tarkoituksena mahdollistaa alimman turvallisuusluokan asiakirjojen käsittely noudattaen tiedonhallintalaissa säädettäviä tiedonhallinnan perusvaatimuksia (HE 284/2018 vp s.98). Osa turvallisuusluokiteltua tietoa käsittelevistä organisaatioista on katsonut, että hallinnollisen alueen vaatimukset voi viranomaisen toimeksiannosta toteuttaa myös pilvipalveluntarjoaja tai muu palveluntarjoaja.

Osa organisaatioista on puolestaan kokenut haasteita hallinnollisen alueen vaatimusten täyttämässä pilvipalveluissa. Erityisesti pääsyoikeuksien rajaamisen vain valtionhallinnon viranomaisen valtuuttamiin henkilöihin on joissakin tapauksissa katsottu olevan haastavaa tai jopa mahdotonta.

Julkisen hallinnon tietoturvallisuuden arviointikriteeristö Julkrissa (VM 2023:46) on esitetty keinoja, joiden avulla hallinnollisen alueen vaatimukset voi viranomaisen toimeksiannosta toteuttaa myös fyysisen tilan hallinnasta vastaava palvelun tuottaja, kuten esimerkiksi pilvipalvelun toimittaja. Tästä huolimatta fyysisten turvallisuusalueiden vaatimusten toteuttamiseen hajautetuissa palveluympäristöissä on liittynyt epävarmuutta, jolla on ollut vaikutusta julkisen hallinnon digitalisoitumiseen ja tuottavuuden kehittämiseen.

Turvallisuusluokitteluasetuksen selkeyttämistarve on noussut esiin myös tietoturvallisuuden tason parantamisen näkökulmasta. Useimmat uudet teknologiat perustuvat hajautettuun palvelutuotantotapaan. Uusimmilla teknologioilla on monessa tilanteessa mahdollista saavuttaa kokonaisuutena ja etenkin tiedon saatavuuden näkökulmasta parempaa tietoturvallisuuden tasoa kuin perinteisillä toteutustavoilla. Turvallisuusluokiteltua tietoa käsittelevillä organisaatioilla onkin nykytilassa ollut halu hyödyntää turvallisuusluokittelun tiedon käsittelyssä nykyistä laajemmin esimerkiksi pilvipalveluita ja muita kehittyviä palvelutuotantotapoja.

Turvallisuusluokitteluasetuksessa on säädetty fyysisten turvallisuusalueiden toteuttamisen lisäksi myös monista muista turvallisuusluokittelun tiedon käsittelyyn liittyvistä vaatimuksista. Digitalisaation ja tiedon liikkuvuuden esteiden purkamisen hankkeen yhteydessä ei kuitenkaan näiden vaatimusten osalta noussut esiin sellaisia esteitä tai haasteita, jotka vaikuttaisivat kehittyvien teknologioiden hyödyntämiseen.

#### **4 Asetuksenantovaltuudet**

Tiedonhallintalain 18 §:n 4 momentin mukaan turvallisuusluokittelusta, turvallisuusluokiteltaviin asiakirjoihin tehtävistä merkinnöistä ja turvallisuusluokiteltujen asiakirjojen käsittelyyn liittyvistä tietoturvaluustoimenpiteistä säädetään tarkemmin valtioneuvoston asetuksella.

#### **5 Keskeiset ehdotukset**

Turvallisuusluokitteluasetuksen 9 §:ää muutettaisiin siten, että pykälän sanamuodonkin perusteella olisi nykyistä selkeämpää, että tiedonhallintayksikkö voi määrittää pykälässä tarkoitetut turvallisuusalueet yhteistyössä käyttämänsä palveluntarjoajan kanssa. Lisäksi pykälän 1 kohtaa muutettaisiin selkeämmäksi siten, että myös palveluntarjoaja voi viranomaisen ennalta määrittelemällä tavalla valtuuttaa henkilöiden pääsyn hallinnolliselle alueelle ilman saattajaa. Muutosten tarkoituksena on erityisesti helpottaa ja yhdenmukaistaa näiden säännösten

tulkintaa, sillä tulkintaerojen on tunnistettu aiheuttavan haasteita viranomaisten toiminnassa. Muutoksen ei kuitenkaan tulisi vaikuttaa tulkintaa rajaavasti asetuksen muihin säännöksiin, joiden osalta käytännössä ei ole nykyiselläänkään tunnistettu haasteita.

## 6 Yksityiskohtaiset perustelut

**9 §. Turvallisuusalueet.** Pykälän johdantokappaleeseen tehtäisiin muutos, jolla selvennettäisiin sitä, että tiedonhallintayksikkö voi toteuttaa turvallisuusalueiden, eli hallinnollisten alueiden ja turva-alueiden, vaatimukset myös yhteistyössä palveluntarjoajan kanssa. Tiedonhallintayksikön olisi itsenäisesti tai yhteistyössä palveluntarjoajan kanssa määritettävä fyysisesti suojatut turvallisuusalueet turvallisuusluokiteltujen asiakirjojen käsittelyn ja tietojärjestelmien suojaamiseksi 10 §:ssä tarkoitetulla tavalla. Pykälässä tarkoitettuja turvallisuusalueita olisivat jatkossakin hallinnolliset alueet ja turva-alueet.

Pykälän 1 kohdan mukaan vain valtionhallinnon viranomaisen valtuuttamalla henkilöllä voi olla pääsy hallinnolliselle alueelle ilman saattajaa. Pykälän 1 kohtaa muutettaisiin siten, että sen sanamuodosta ilmenisi nykyistä selkeämmin, että pääsyn hallinnolliselle alueelle voisi myöntää myös valtionhallinnon viranomaisen käyttämä palveluntarjoaja viranomaisen ennalta määrittelemällä tavalla. Tällainen palveluntarjoaja voi olla esimerkiksi fyysisen tilan hallinnasta vastaava pilvipalvelun toimittaja. Tiedonhallintayksikkö voisi sopia palveluntarjoajan kanssa pääsyn rajaamisen menetelmistä, joita voivat olla esimerkiksi mekaaniset, elektroniset tai henkilökohtaiseen tunnistautumiseen perustuvat menetelmät.

Hallinnolliselle alueelle ei edelleenkään asetettaisi erityisiä vaatimuksia, vaan sillä voitaisiin edelleen tarkoittaa esimerkiksi toimistotiloja, konesaleja, niiden osia, tai useista eri tiloista muodostuvia kokonaisuuksia. Tiedonhallintayksikkö voisi määrittää alueen rajat ja pääsyoikeuden valvonnan joko itsenäisesti tai esimerkiksi sopimuksellisiin menettelyihin perustuen yhdessä käyttämänsä palveluntarjoajan kanssa. Palveluntarjoaja voisi siis tiedonhallintayksikön toimeksiannosta vastata hallinnollisen alueen toteuttamisesta käytännössä. Tiedonhallintayksikön olisi edelleen tiedonhallintalain 13 §:n 4 momentin mukaisesti varmistettava hankinnoissaan, että hankittavaan tietojärjestelmään on toteutettu asianmukaiset tietoturvaluustoimenpiteet ja siten tiedonhallintayksikkö olisi vastuussa riittävien sopimuksellisten vastuiden asettamisesta palveluntarjoajille.

Turvallisuusalueiden määrittämisen tarkoituksena on huolehtia tietojen suojaamisen fyysisestä ulottuvuudesta. Fyysisen suojauksen menetelmät eivät sellaisenaan riitä pilvipalveluiden, hajautettujen järjestelmien ja verkkopohjaisten tietojärjestelmien turvallisuuden varmistamiseen. Perinteiset fyysiset suojaukset ovat kuitenkin edelleen keskeinen osa turvallisuusluokiteltujen tietojen käsittelyn turvallisuuden varmistamista. Tästä syystä turvallisuusalueita koskevasta

sääntelystä ei luovuttaisi. Pykälään ehdotettavien muutosten myötä olisi kuitenkin nykyistä selkeämpää, että tiedonhallintayksikkö voi huolehtia turvallisuusalueiden toteuttamisesta yhteistyössä käyttämänsä palveluntarjoajan kanssa. Turvallisuusluokitellun tiedon suojaamiseen liittyvistä muista menetelmistä kuten tietojärjestelmiä ja tietoliikennejärjestelyjä koskevista vaatimuksista säädetään turvallisuusluokitteluasetuksen muissa pykälissä.

Nykytilassa on vallinnut jonkin verran epäselvyyttä siitä, onko hallinnollisen alueen tai turva-alueen mukaisia vaatimuksia mahdollista toteuttaa hajautetuissa järjestelmissä, kuten esimerkiksi pilvipalveluissa. Ehdotettavien muutosten tarkoituksena on aiempaa selkeämmin mahdollistaa alihankinnan ja kehittyvien teknologioiden hyödyntäminen myös turvallisuusluokiteltujen tietojen käsittelyssä ja näin osaltaan parantaa julkisen hallinnon digitalisaatiota ja tuottavuutta. Erityisesti muutosten tarkoituksena on selventää entisestään sitä, että pääsyoikeuden hallinnolliselle alueelle tai turva-alueelle voi tiedonhallintayksikön kanssa sovituin menettelyin myöntää tai valtuuttaa myös palveluntarjoaja.

Turvallisuusalueiden määrittämisen lisäksi tiedonhallintayksikön tulisi edelleen huolehtia myös muista kuin tietojen fyysisen suojaamisen menetelmistä ja varmistua esimerkiksi tietojen eheydestä, luottamuksellisuudesta, saatavuudesta asianmukaisin tietoturvaluustoimenpitein.

Ehdotettavien muutosten tarkoituksena on aiempaa selkeämmin mahdollistaa modernien ja kehittyvien teknologioiden ja palvelutuotantomallien hyödyntäminen turvallisuusluokitellun tiedon käsittelyssä. Turvallisuusluokitteluasetuksen 9 §:n tulkintaan on liittynyt jonkin verran epäselvyyksiä, mistä on seurannut haittaa julkisen hallinnon pilvisiirtymälle ja sitä kautta laajemminkin tuottavuuden ja digitalisaation edistymiselle. Asetuksen muotoilua selventämällä on tarkoitus poistaa turvallisuusalueiden määrittämisen käytännön toteuttamisen mahdollisuuksiin liittyvää tulkinnanvaraisuutta, joka on hidastanut tiedonhallintayksiköiden riskiperusteista päätöksentekoa uusien teknologioiden hyödyntämisessä.

## **7 Vaikutukset**

Turvallisuusluokitteluasetuksen 9 §:ään ehdotettavilla muutoksilla arvioidaan olevan julkisen hallinnon digitalisaation ja tuottavuuden edistämisen edellytyksiä parantavia vaikutuksia. Nykytilaan on liittynyt tulkintaepäselvyyksiä siitä, onko voimassa olevan turvallisuusluokitteluasetusten mukaisten turvallisuusalueiden toteuttaminen mahdollista silloin kun hyödynnetään hajautettuja ja verkkopohjaisia tietojärjestelmiä. Ehdotettujen muutosten tarkoitus on poistaa tätä epäselvyyttä, millä arvioidaan olevan positiivisia vaikutuksia turvallisuusluokiteltuja asiakirjoja käsittelevien viranomaisten mahdollisuuksiin lisätä toimintansa tehokkuutta.

Ehdotettavien muutosten ei arvioida vaikuttavan heikentävästi olemassa olevien järjestelmien ja tietovarantojen tietoturvallisuuteen tai kansalliseen turvallisuuteen. Uusimmilla ja kehittyvillä teknologioilla on monissa tilanteissa mahdollista saavuttaa kokonaisuutena ja etenkin tiedon saatavuuden näkökulmasta parempaa tietoturvallisuuden tasoa. Tältä osin edellytysten kansallisen turvallisuuden kannalta tärkeiden tietojen suojaamiselle voidaan arvioida joiltain osin parantuvan.

Turvallisuusluokitteluasetykseen ehdotettavilla lisäyksillä ja muutoksilla ei arvioida olevan suoria taloudellisia vaikutuksia. Ehdotetut muutokset eivät tiukentaisi tiedonhallintayksiköille asetettuja turvallisuusluokitellun tiedon käsittelyvelvollisuuksia. Ehdotetut muutokset selventäisivät entisestään sitä, että tiedonhallintayksikön on mahdollista toteuttaa turvallisuusluokan IV tietojen käsittelyyn liittyvät vaatimukset yhteistyössä palveluntarjoajan kanssa.

[Täydennetään lausuntokierroksen jälkeen]

## **8 Lausuntopalaute ja jatkovalmistelu**

[Täydennetään lausuntokierroksen jälkeen]

## **9 Voimaantulo**

Valtioneuvoston asetuksen ehdotetaan tulevan voimaan...