VALTIOVARAINMINISTERIÖ **Muistio** **Liite 1**
Lainsäädäntöneuvos X.X.2019
Eeva Lantto

VALTIONEUVOSTON ASETUS ASIAKIRJOJEN TURVALLISUUSLUOKITTELUSTA VALTIONHALLINNOSSA

1 Johdanto

Nykyisin mahdollisuudesta luokitella asiakirjoja sekä luokitusmerkinnöistä säädetään viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999), jäljempänä ”*julkisuuslaki*”, sekä sen nojalla annetussa valtioneuvoston asetuksessa tietoturvallisuudesta valtionhallinnossa (681/2010), jäljempänä ”tietoturvallisuusasetus”. Tietoturvallisuusasetuksen mukaan asiakirjat voidaan luokitella suojaustason mukaan ja asiakirjat voidaan merkitä suojaustasoa koskevalla merkinnällä (ei turvallisuusluokiteltavat asiakirjat) tai turvallisuusluokkaa koskevalla merkinnällä, jos on kyse turvallisuusluokiteltavasta asiakirjasta. Tietoturvallisuusasetuksessa on myös säädetty tarkemmin eri suojaustasoja koskevista tietoturvallisuusvaatimuksista.

Julkisen hallinnon tiedonhallinnasta annetun lain (/), jäljempänä ”*tiedonhallintalaki*”, voimaantulon myötä 1.1.2020 asiakirjojen ja niiden käsittelyn tietoturvallisuusvelvoitteista sekä turvallisuusluokiteltavista asiakirjoista säädetään tiedonhallintalaissa. Laki sisältää vähimmäisvaatimukset asiakirjojen, mukaan lukien salassa pidettävien asiakirjojen tietoturvalliselle käsittelylle. Lain 18 §:n 1 momentin mukaan valtion virastoissa ja laitoksissa toimivien viranomaisten, tuomioistuimen ja valitusasioita käsittelemään perustettujen lautakuntien on turvallisuusluokiteltava asiakirjat ja tehtävä niihin turvallisuusluokkaa koskeva merkintä sen osoittamiseksi, minkälaisia tietoturvallisuustoimenpiteitä asiakirjaa käsiteltäessä noudatetaan. Turvallisuusluokkaa koskeva merkintä on tehtävä, jos asiakirja tai siihen sisältyvä tieto on salassa pidettävä viranomaisten toiminnan julkisuudesta annetun lain 24 §:n 1 momentin 2, 5 tai 7—11 kohdan perusteella ja asiakirjaan sisältyvän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa maanpuolustukselle, poikkeusoloihin varautumiselle, kansainvälisille suhteille, rikosten torjunnalle, yleiselle turvallisuudelle tai valtion- ja kansantalouden toimivuudelle taikka muulla niihin rinnastettavalla tavalla Suomen turvallisuudelle.

2 Asetuksenantovaltuudet

Tiedonhallintalain 18 §:n 4 momentin mukaan valtioneuvoston asetuksella annetaan tarkempia säännöksiä turvallisuusluokittelusta, turvallisuusluokiteltaviin asiakirjoihin tehtävistä merkinnöistä ja turvallisuusluokiteltujen asiakirjojen käsittelyyn liittyvistä tietoturvallisuustoimenpiteistä

3 Keskeiset ehdotukset

Ehdotettu valtioneuvoston asetus sisältäisi nykyistä tietoturvallisuusasetusta mukaillen säännökset turvallisuusluokista, niiden merkitsemisestä ja eri luokkiin kuuluviin asiakirjoihin kohdistettavista tietoturvallisuustoimenpiteistä.

Tiedonhallintalain mukaisesti muita kuin turvallisuusluokiteltavia asiakirjoja ei enää luokiteltaisi, vaan muut salassa pidettävät asiakirjat merkittäisiin yksinomaan julkisuuslain 25 §:n mukaisella salassapitomerkinnällä ja niitä käsiteltäisiin tiedonhallin-

talaissa säädettyjen tietoturvallisuuden vähimmäisvaatimusten mukaisesti – ottaen huomioon lain 13 §:n 1 momentissa säädetty velvollisuus mitoittaa tietoturvallisuustoimenpiteet riskienhallinnan keinoin.

Tästä syystä - ja asetuksenantovaltuuden mukaisesti – ehdotettuun asetukseen ei sisälly muita kuin turvallisuusluokiteltavia asiakirjoja koskevia vaatimuksia. On kuitenkin otettava huomioon, että monet asetuksessa turvallisuusluokan IV asiakirjoille säädettäväksi ehdotetut tietoturvallisuustoimenpiteet soveltuvat myös vähimmäisvaatimuksiksi erityisesti huolehdittaessa salassa pidettävien tai henkilötietoja sisältävien asiakirjojen tietoturvallisuudesta.

4 Yksityiskohtaiset perustelut

4.1 Asetuksen soveltamisala, suhde muuhun lainsäädäntöön ja määritelmät

Asetuksessa säädettäisiin tiedonhallintalain 18 §:n 1 momentissa tarkoitettujen asiakirjojen turvallisuusluokittelusta, turvallisuusluokiteltaviin asiakirjoihin tehtävistä merkinnöistä sekä turvallisuusluokiteltujen asiakirjojen käsittelyä koskevista tietoturvallisuustoimenpiteistä valtionhallinnon viranomaisissa (1 § 1 mom).

Asetuksen 1 §:n 2 momentti sisältäisi informatiivisen viittauksen julkisuuslakiin. Viittauksella on tarkoitus selventää sitä, että asiakirjan merkinnät eivät sellaisenaan tee asiakirjasta salassa pidettävää, vaan salassapidosta säädetään lähtökohtaisesti julkisuuslaissa tai erityislainsäädännössä ja asiakirjan saamista koskeva pyyntö käsitellään julkisuuslain mukaisesti.

Kansainvälisten tietoturvallisuusvelvoitteiden mukaisesti turvallisuusluokitellun asiakirjan salassapitovelvollisuudesta ja kansainvälisten tietoturvallisuusvelvoitteiden toteuttamisesta puolestaan säädetään kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa (588/2004). Asetusta sovellettaisiin ehdotetun 1 §:n 3 momentin mukaan toisen maan viranomaiselta tai kansainväliseltä toimielimeltä saadun asiakirjan käsittelyyn, jollei kansainvälisestä tietoturvallisuusvelvoitteesta muuta johdu. Suomen tekemät tietoturvallisuussopimukset tai muut kansainväliset tietoturvallisuusvelvoitteet saattavat sisältää asetuksesta poikkeavia tietoturvallisuustoimenpiteitä ja menettelyjä, joita on noudatettava asetuksessa säädetyn sijaan tai lisäksi.

Asetuksen 2 §:ssä määriteltäisiin valtionhallinnon viranomaiset, joihin asetusta 1 §:n mukaisesti sovelletaan. Valtionhallinnon viranomaisilla tarkoitettaisiin niitä tahoja, joiden on turvallisuusluokiteltava asiakirjat tiedonhallintalain 18 §:n 1 momentin mukaan, eli valtion virastoissa ja laitoksissa toimivia viranomaisia, tuomioistuimia ja valitusasioita käsittelemään perustettuja lautakuntia.

Lisäksi 2 §:ssä määriteltäisiin asiakirjan käsittely, jolla tarkoitettaisiin lähtökohtaisesti kaikkia asiakirjaan kohdistuvia toimenpiteitä: asiakirjan vastaanottamista, laatimista, tallentamista, katselua, muuttamista, luovuttamista, kopiointia, siirtoa, välittämistä, tuhoamista, säilyttämistä ja arkistointia sekä muita asiakirjaan kohdistuvia toimenpiteitä.

Asiakirjan määritelmä sisältyy tiedonhallintalain 2 §:n 4 kohtaan, jonka mukaan asiakirjalla tarkoitetaan julkisuuslain 5 §:n 2 momentissa tarkoitettua viranomaisen

asiakirjaa. Julkisuuslaissa omaksuttu asiakirjan laaja käsite on välineneutraali eli riippumaton siitä, minkälaiselle alustalle tai minkälaisin keinoin tieto on talletettu. Siten asiakirjoilla tarkoitetaan paitsi perinteisiä paperimuotoisia asiakirjoja, myös sähköisesti talletettuja tietoaineistoja riippumatta niiden formaatista.

4.2 Turvallisuusluokittelu ja turvallisuusluokkaa koskevat merkinnät

Asetuksen 3 §:ssä säädettäisiin nykytilaa vastaavasti neliportaisesta asiakirjojen luokittelusta ja merkitsemisestä sillä erolla nykyiseen, että luokittelu koskisi vain tiedonhallintalain 18 §:n 1 momentissa tarkoitettuja turvallisuusluokiteltavia asiakirjoja, jotka ovat salassa pidettäviä salassapitosäännöksessä tarkoitetun yleisen edun takia. Tiedonhallintalain mukaisesti muita kuin turvallisuusluokiteltavia asiakirjoja ei enää luokiteltaisi, vaan muut salassa pidettävät asiakirjat merkittäisiin julkisuuslain 25 §:n mukaisesti salassapitomerkinnällä ja niitä käsiteltäisiin tiedonhallintalaissa säädettyjen tietoturvallisuuden vähimmäisvaatimusten mukaisesti.

Merkintä voitaisiin tehdä asiakirjaan liitettävään erilliseen asiakirjaan, jos merkintöjen tekeminen asiakirjaan tai merkinnän muuttaminen ei ole teknisesti mahdollista tai jos turvallisuusluokkaa vastaavat käsittelyvaatimukset ovat tarpeen vain tietyn lyhyehkön ajan.

Turvallisuusluokitellun asiakirjan kopioon on tehtävä sama merkintä kuin mikä on tehty alkuperäiseen asiakirjaan, jollei luokitus muutoin jo ilmene asiakirjan kopiosta.

Asetuksen 4 § sisältäisi voimassaolevan tietoturvallisuusasetuksen 12 §:ää vastaavan säännöksen turvallisuusluokituksen vastaavuudesta kansainvälisiä tietoturvallisuusvelvoitteita toteutettaessa. Säännös vastaa käytäntöä, joka on syntynyt Suomen tekemissä tietoturvallisuussopimuksissa.

Asetuksen 5 §:ssä säädettäisiin turvallisuusluokkaa koskevan merkinnän poistamisesta ja muuttamisesta nykyistä (tietoturvallisuusasetuksen 10 §:n 3 momentissa säädettyä) vastaavasti siten, että merkinnän poistamisesta ja muuttamisesta on tehtävä asianmukainen merkintä ja merkinnän asianmukaisuus on tarkistettava viimeistään silloin kun viranomainen antaa asiakirjan ulkopuoliselle.

Merkinnän muuttamista koskevaa sääntelyä muutettaisiin nykyisestä siten, että turvallisuusluokkaa koskevan merkinnän saisi poistaa tai muuttaa ainoastaan asiakirjan laatineen viranomaisen tai sen viranomaisen luvalla, jonka käsiteltäväksi asia kokonaisuudessaan kuuluu, jollei olisi selvää, ettei perusteita turvallisuusluokan käytölle enää ole. Muutos on perusteltu siksi, että merkinnän asianmukaisuuden arvioinnin voi parhaiten suorittaa ns. asiakirjasta vastaava viranomainen. Turvallisuusluokittelua koskevan merkinnän ilmeinen perusteettomuus voisi olla esimerkiksi se, että asiakirjan sisältämät tiedot ovat jo tulleet julkisiksi.

Merkinnän poistamisessa ja muuttamisessa on kuitenkin aina noudatettava soveltuvaa kansainvälistä tietoturvallisuusvelvoitetta, mikäli asiakirja on saatu toisen maan viranomaiselta tai kansainväliseltä toimielimeltä. Kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa tarkoitettua turvallisuusluokiteltua asiakirjaa koskeva asia on siirrettävä sille viranomaiselle, jolle sopimuspuoli on asiakirjan toimittanut. On kuitenkin huomattava, että kansainvälisten tietoturvallisuusvelvoitteiden mukai-

sesti vain asiakirjan luovuttanut osapuoli saa muuttaa luokitusta. Tällöin sen viranomaisen, jolle osapuoli on asiakirjan toimittanut, on otettava yhteyttä luovuttaneeseen osapuoleen turvallisuusluokittelua koskevassa asiassa.

Valtionhallinnon viranomaisen olisi varmistuttava siitä, että se on määritellyt vastuut turvallisuusluokkaa koskevan merkinnän muuttamista koskevassa päätöksenteossa - vastaavasti kuin asiakirjan antamista koskevassa päätöksenteossa.

Ehdotettu säännös merkinnän muuttamisesta on sopusoinnussa julkisuuslain 15 §:n 3 momentin kanssa, jonka mukaan, jos viranomaiselta pyydetään turvallisuusluokiteltavaa asiakirjaa, jonka muu viranomainen on laatinut, viranomaisen on siirrettävä asia asiakirjan laatineen viranomaisen ratkaistavaksi. Lisäksi mainitun julkisuuslain säännöksen mukaan kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa tarkoitettua turvallisuusluokiteltua asiakirjaa koskeva asia on siirrettävä sille viranomaiselle, jolle sopimuspuoli on asiakirjan toimittanut.

Salassapitomerkinnän tekemisestä, poistamisesta ja muuttamisesta säädetään julkisuuslain 25 §:ssä. Mainitun säännöksen 2 momentin mukaan, kun asiakirjan tai siinä olevien tietojen salassapidolle ei enää ole perusteita, merkinnän poistamisesta tai muuttamisesta on tehtävä merkintä asiakirjaan, johon alkuperäinen merkintä on tehty. Merkinnän asianmukaisuus on tarkistettava viimeistään asiakirjaa ulkopuoliselle annettaessa.

4.3 Turvallisuusluokiteltujen asiakirjojen käsittelyn tietoturvallisuusvaatimukset

Asetuksen pykälissä 6 – 15 säädettäisiin turvallisuusluokiteltujen asiakirjojen käsittelyn tietoturvallisuusvaatimuksista eli asiakirjojen käsittelyssä toteutettavista tietoturvallisuustoimenpiteistä, jotka liittyisivät kansainvälisiä tietoturvallisuusvelvoitteita ja asiakirjan elinkaarta mukaillen asiakirjan antamisen edellytyksiin (6 §), monitasoiseen suojaukseen (7 §), käsittelyoikeuden antamiseen ja käsittelyoikeuksien luettelointiin (8 §), fyysiseen turvallisuuteen (9 ja 10 §), sähköiseen käsittelyyn ja asiakirjan siirtämiseen tietoverkon kautta (11 ja 12 §), asiakirjan kuljettamiseen (13 §), asiakirjan käsittelyn seuraamiseen (14 §) ja asiakirjan tuhoamiseen (15 §).

Myös turvallisuusluokiteltujen asiakirjojen käsittelyssä on noudatettava, mitä tiedonhallintalaissa on säädetty tietoturvallisuustoimenpiteistä ja niiden mitoittamisesta riskiarvioinnin mukaisesti. Esimerkiksi tiedonhallintalain 13 §:n mukainen riskienhallinnan keinoin toteutettavia tietoturvallisuustoimenpiteitä ja tietoaineistojen koko elinkaaren huomioon ottamista koskeva säännös on merkittävä myös turvallisuusluokiteltujen asiakirjojen käsittelyssä. Turvallisuusluokiteltujen asiakirjojen luottamuksellisuuden vaarantuminen aiheuttaa merkittävämpää vahinkoa, mitä korkeamman luokan asiakirjasta on kyse. Korkeammalle luokiteltujen asiakirjojen tietoturvallisuuteen kohdistuu lähtökohtaisesti vakavampia uhkia kuin alemman turvallisuusluokan asiakirjoihin tai salassa pidettäviin asiakirjoihin, mikä on otettava huomioon tietoturvallisuustoimenpiteitä toteutettaessa. Tietoturvallisuusriskillä tarkoitettaan jonkinlaisen haitan tai vahingon todennäköisyyttä ja sen seurauksia. Tietoturvallisuusturvariskeillä tarkoitettaisiin sellaisia tahattomia tai tahallisia tekijöitä, jotka toteutuessaan vaarantaisivat viranomaisen toimintaan ja tiedonhallintaan liittyvien suojattavien kohteiden luottamuksellisuutta, eheyttä tai saatavuutta. Tietoturvallisuusris-

kin erottaa tietoturvallisuusuhasta sillä, että riskin todennäköisyyttä ja vaikutuksia on arvioitu.

Asetuksen 6 §:ssä säädettäisiin turvallisuusluokitellun asiakirjaan antamiseen liittyvistä velvoitteista. Säännöksen mukaan valtionhallinnon viranomaisen olisi ennakolta varmistuttava siitä, että turvallisuusluokitellun asiakirjan suojaamisesta huolehditaan asianmukaisesti, kun se antaa turvallisuusluokitellun asiakirjan muulle kuin valtionhallinnon viranomaiselle. Pykälän 2 momentissa on informatiivinen viittaussäännös julkisuuslain yleiseen, kaikkia viranomaisia koskevaan velvollisuuteen ennakolta varmistua, että tietojen salassapidosta ja suojaamisesta huolehditaan asianmukaisesti, kun viranomainen antaa tiedon salassa pidettävästä asiakirjasta lukuunsa suoritettavaa tehtävää varten.

Ehdotettuun 7 §:ään sisältyy useissa kansainvälisissä tietoturvallisuusvelvoitteissa omaksuttu ns. syvyyssuuntaisen tietoturvallisuuden toteuttamisen velvollisuus huolehdittaessa tuvallisuusluokiteltujen asiakirjojen käsittelyyn käytettävän tietojärjestelmän, tietoliikennejärjestelyn tai fyysisesti suojatun turvallisuusalueen tietoturvallisuudesta. Syvyyssuuntainen tietoturvallisuus edellyttää monitasoisen suojauksen toteuttamista suojasta vaarantavia tekoja ennaltaehkäisevillä, estävillä, havaitsevilla, rajaavilla ja korjaavilla tietoturvallisuustoimenpiteillä. Tarkoitus ei ole, että kaikkien viiden tason toimenpiteitä käytettäisiin aina, vaan toimenpiteiden tarpeellisuus tulisi arvioida riskienhallinnan keinoin. Suojauksessa tulee riskiarvioinnin mukaisesti huomioida, että merkittävä määrä turvallisuusluokiteltuja tietoja eli niin sanottu tietojen kasauma esimerkiksi yhdessä tietojärjestelmässä voi edellyttää joiltain osin korkeampaan turvallisuusluokkaan kuuluvien tietojen suojaamiseen sovellettavien vaatimusten noudattamista.

Ehdotetun 8 §:n mukaan turvallisuusluokitellun asiakirjan käyttöoikeus voidaan antaa vain sille, jolla työtehtäviensä vuoksi on tarve saada tietoja asiakirjasta tai muutoin käsitellä sitä ja jolle on selvitetty turvallisuusluokiteltujen tietojen suojaamista koskevat ohjeet ja menettelyt ja joka tuntee asiakirjojen käsittelyä koskevat velvoitteet. Vastaava ns. need to know –periaatetta koskeva säännös on voimassa olevassa tietoturvallisuusasetuksessa (5 §:n 1 mom 5 kohta ja 13 §:n 1 mom). Velvoitetta on täsmennetty vastaamaan kansainvälisissä tietoturvallisuusvelvoitteissa omaksuttuja muotoiluja vastaavasta periaatteesta. Mikäli kansainvälisessä tietoturvallisuusvelvoitteessa on pidemmälle meneviä vaatimuksia (esimerkiksi asiakirjoja käsittelevän henkilön kirjallinen vakuutus asiakirjojen käsittelyä koskevien velvoitteiden ymmärtämisestä), on niitä noudatettava kyseisen velvoitteen piiriin kuuluvien asiakirjojen käsittelyssä.

Lisäksi valtionhallinnon viranomaisen olisi pidettävä luetteloa henkilöistä, joilla on oikeus käsitellä turvallisuusluokan I, II tai III asiakirjoja. Luettelossa olisi mainittava henkilön työtehtävä, johon turvallisuusluokitellun tiedon käsittelytarve perustuu. Vastaava vaatimus on turvallisuusluokan I ja II asiakirjojen osalta voimassa olevassa tietoturvallisuusasetuksessa (13 §). Käsittelyoikeuksien luettelointia koskevat velvoitteet ulotettaisiin kansainvälisiä tietoturvallisuusvelvoitteita vastaavasti myös turvallisuusluokan III asiakirjoihin. Valtionhallinnon viranomaisen olisi rekrytoinnissa tai henkilön tehtäviä muutettaessa tiedettävä, minkä turvallisuusluokan tietoihin henkilöllä on tarve saada käsittelyoikeus. Viranomaisen ei tarvitsisi pitää erillisiä luetteloja henkilöistä ja työtehtävistä, vaan henkilöt ja heidän työtehtävänsä voidaan luetel-

la samassa asiakirjassa. Vaatimuksella on liityntä tiedonhallintalain 12 §:n tietoturvallisuusvelvoitteeseen, jonka mukaan tiedonhallintayksikön on tunnistettava ne tehtävät, joiden suorittaminen edellyttää sen palveluksessa olevilta tai sen lukuun toimivilta henkilöiltä erityistä luotettavuutta.

Nykyistä tietoturvallisuusasetusta vastaavasti säädettäisiin 3 momentissa myös velvollisuudesta pitää huolta, että se, joka ei enää toimi työtehtävissä, joihin oikeus luokiteltujen asiakirjojen käsittelyyn perustuu, palauttaa asiakirjat tai tuhoaa ne asianmukaisella tavalla.

Fyysistä turvallisuutta koskevat säännökset ehdotetaan uudistettavaksi vastaamaan paremmin EU:n neuvoston turvallisuussääntöjen (2013/488/EU) velvoitteita. Ehdotetussa 9 §:ssä on yleinen fyysistä turvallisuutta koskeva säännös, jonka mukaan viranomaisen on toteutettava tilojen suojaamiseksi tarpeelliset tietoturvallisuustoimenpiteet turvallisuusluokiteltujen asiakirjojen tietoturvallisuuden varmistamiseksi.

Lisäksi viranomaisen olisi turvallisuusluokiteltujen asiakirjojen säilyttämiseksi ja käsittelemiseksi ehdotetussa 10 §:ssä tarkoitetulla tavalla määritettävä fyysisesti suojatut turvallisuusalueet:

1) hallinnolliset alueet, joilla on selkeästi määritellyt näkyvät rajat ja joihin vain viranomaisen asianmukaisesti valtuuttamilla henkilöillä on pääsy ilman saattajaa;

2) turva-alueet, joilla on selkeästi määritellyt ja suojatut rajat, joilla valvotaan kaikkea kulkua sisään ja ulos kulkuluvin tai henkilökohtaisesti tunnistamalla ja joihin on pääsy ilman saattajaa vain henkilöillä, joiden luotettavuus on varmistettu ja joilla on erityinen lupa tulla alueelle tiedonsaantitarpeensa perusteella.

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.

Turva-alueella voidaan tarkoittaa esimerkiksi tilaa tai useista eri tiloista muodostuvaa kokonaisuutta, jonne on itsenäinen pääsy ainoastaan tilaa hallinnoivan viranomaisen ennalta valtuuttamilla henkilöillä. Lisäksi henkilöstä tulee mahdollisuuksien mukaan hakea tarvittavan tason henkilöturvallisuusselvitys. Erityisenä ehtona tilaan pääsylle on henkilön työtehtäviin liittyvä tarve. Turva-alueella voi olla erillinen tila, jossa turvallisuusluokiteltu tieto säilytetään. Esimerkiksi turva-alue voi olla perustettu siten, että siellä työskentelevillä henkilöillä on oikeus käsitellä turvallisuusluokan III tietoja, mutta turva-alueella olevaan, turvallisuusluokan II tietoja sisältävään kassakaappiin sijoitettuun asiakirjaan on pääsy vain niillä henkilöillä, joilla on työtehtäviensä perusteella tarve käsitellä kyseistä asiakirjaa. Turva-aluetta rajaavan rakenteen ja monitasoisen suojauksen vaatimukset perustuvat alueella säilytettävien tietojen turvallisuusluokkaan, niiden muotoon ja määrään, kiinteistön ympäristöön ja rakenteeseen sekä uhka-arvioon.

Viittaus 10 §:ään tarkoittaa esimerkiksi sitä, että viranomaisen, joka ei käsittele turvallisuusluokkaa IV korkeammalle luokiteltuja asiakirjoja, ei välttämättä tarvitse pe-

rustaa turva-alueita, koska turvallisuusluokan IV asiakirjoja voidaan käsitellä ja ne voidaan myös säilyttää hallinnollisella alueella.

Ehdotetun 10 §:n mukaan turvallisuusluokan IV—II asiakirjojen käsittely on mahdollista hallinnollisella alueella, jos pääsy turvallisuusluokiteltuihin tietoihin on suojattu sivullisilta. Tällä tarkoitetaan tiedon suojaamista sekä henkilöiltä, joilla ei ole tiedonsaantitarvetta (need-to-know) kyseiseen tietoon, että laittomalta tiedustelulta. Suojaaminen tarkoittaa käytännössä tiedon tai tietoa sisältävän laitteen jatkuvaa valvontaa ja suoran näköyhteyden estämistä turvallisuusluokiteltuun tietoon. Laittomalta tiedustelulta suojaaminen liittyy erityisesti turvallisuusluokan I-III tietojen suojaamiseen tekniseltä tiedustelulta tiedon käsittelyn tapahtuessa sähköisesti tai puhumalla.

Mainittujen asiakirjojen käsittely on mahdollista myös hallinnollisen alueen ja turva-alueen ulkopuolella, mikäli on toteutettu hallinnollisen alueen vaatimuksia korvaavia toimenpiteitä sen varmistamiseksi, että pääsy turvallisuusluokiteltuihin tietoihin on suojattu sivullisilta. Tilanteissa, joissa turvallisuusluokan III tai II tietoa käsitellään sähköisessä muodossa hallinnollisella alueella, tulisi esimerkiksi pitää huolta, että hajasäteilyyn ja elektroniseen tiedusteluun liittyviä riskejä on pienennetty riittävästi. Käsittelyssä on huomioitava myös esimerkiksi toiminta työskentelytaukojen aikana, jolloin aineisto on vietävä esimerkiksi turva-alueen kassakaappiin tauon ajaksi. Lisäksi on otettava huomioon näkyvyyden rajoittaminen tilaan (esimerkiksi mahdollisten ikkunoiden peittäminen) ja käsittelytilaan pääsyn rajaaminen vain viranomaisen ennalta valtuuttamiin henkilöihin.

Huomioitavaa on myös että, käsittelymahdollisuus hallinnollisella alueella edellyttää kuitenkin sitä, että tiedon käsittelyyn käytettävän tietojärjestelmän tai tietoliikennejärjestelyn tulee olla kyseisen turvallisuusluokan mukaisesti suojattu. Turvallisuusluokan III mukaisesti suojattu päätelaite voitaisiin esimerkiksi tuoda hallinnolliselle alueelle, josta päätelaite ottaa turvallisuusluokan III mukaisella liikennesalauksella suojatun yhteyden turva-alueella sijaitsevaan turvallisuusluokan III tietovarantoon tietojen käsittelyn ajaksi. Tässäkin esimerkissä turvallisuusluokan III mukaisesti suojattu päätelaite voitaisiin palauttaa käsittelyn jälkeen säilytettäväksi turva-alueelle. Käsittely hallinnollisen alueen ulkopuolella voisi olla mahdollista myös esimerkiksi siten, että turvallisuusluokan IV tiedon käsittelyyn käytetään kyseisen turvallisuusluokan mukaisesti suojattua etäkäyttöön tarkoitettua päätelaitetta, jota käytettäisiin vain sellaisessa fyysisessä tilassa, jossa ulkopuolisilla ei olisi mahdollisuutta päästä havaitsemaan päätelaitteella käsiteltäviä tietoja.

Turvallisuusluokan I asiakirjan käsittely olisi kansainvälisiä tietoturvallisuusvelvoitteita vastaavasti mahdollista vain turva-alueella.

Turvallisuusluokan IV asiakirja olisi säilytettävä hallinnollisella alueella tai turva-alueella. Turvallisuusluokan III—I asiakirja olisi säilytettävä turva-alueella.

Asiakirjan sähköistä käsittelyä koskeva 11 § sisältäisi turvallisuusluokiteltujen asiakirjojen käsittelyyn tai tallentamiseen käytettäviä tietojärjestelmiä ja tietoliikennejärjestelyjä koskevat vähimmäisvaatimukset. Vähimmäisvaatimukset on, joskin tietyiltä osin paljon yleisemmällä tasolla, kirjattu myös tiedonhallintalakiin koskien kaikkia viranomaisen tietojärjestelmiä. Tästä syystä sääntelyssä on jonkinasteista päällekkäi-

syyttä, mikä kuitenkin on perusteltua siksi, että turvallisuusluokiteltuja asiakirjoja sisältävien tietojärjestelmien ja tietoliikennejärjestelyjen vaatimukset olisivat koottu riittävän täsmällisesti lainsäädäntöön.

Pykälän 1 kohdan mukaan tietojärjestelmät ja tietoliikennejärjestelyt, joissa käsitellään turvallisuusluokan IV—II asiakirjoja, tulisi olla kyseiselle turvallisuusluokalle riittävän luotettavasti erotettu matalamman turvallisuustason tietojärjestelmistä tai tietoliikennejärjestelyistä.

Säännös ei estäisi esimerkiksi turvallisuusluokan IV asiakirjan käsittelyä tai tallentamista samassa tietojärjestelmässä, jossa käsitellään viranomaisen muitakin asiakirjoja. Vähimmäisvaatimukset on tiedonhallintalain mukaisesti mitoitettava riskienhallinnan keinoin ja myös tiedonhallintalaissa on ehdotettuja vähimmäisvaatimuksia vastaavia, mutta yleisemmällä tasolla ilmaistuja velvoitteita kaikkien tai salassa pidettävien asiakirjojen tietoturvallisuudesta huolehtimiseksi. Ehdotettuja tarkemmin muotoiltuja sähköisen käsittelyn vaatimuksia tulisikin esimerkiksi tiedonhallintalain tietoturvallisuusvaatimusten toteuttamista ohjaavien VAHTI 100 ohjeiden mukaan lähtökohtaisesti noudattaa riskienhallinnan keinoin myös muiden kuin turvallisuusluokiteltujen asiakirjojen käsittelyyn käytettävien tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuudesta huolehdittaessa.

Kyseiselle turvallisuusluokalle riittävän luotettavalla erottamisella tarkoitetaan jotain menetelmää salassa pidettävän tiedon käsittely-ympäristön erottamiseen muista ympäristöistä. Erottelun voisi toteuttaa riskiperusteisesti esimerkiksi palomuurilla (ainakin turvallisuusluokan IV osalta) tai luotettavammalla yhdyskäytäväratkaisulla. Sanamuotoilu on tarkoituksella jätetty riskiperusteisesti harkintavaraa jättäväksi, jotta se soveltuisi kaikille turvallisuusluokille erilaisiin käyttötapauksiin ja olisi myös aikaa kestävä.

Tietojärjestelmiä ja tietoliikennejärjestelyjä, joissa käsitellään turvallisuusluokan I asiakirjoja, ei 1 kohdan mukaan saisi kytkeä matalamman turvallisuustason tietojärjestelmiin tai tietoliikennejärjestelyihin.

Ehdotetun 11 §:n vaatimuksiin sisältyisi myös velvollisuus suojautua yleisiä tietojärjestelmän tai tietoliikennejärjestelyn tietoturvallisuutta vaarantavia sähköisiä viestejä eli yleisiä verkkohyökkäyksiä vastaan. Sähköinen viesti on määritelty sähköisen viestinnän palveluista annetussa laissa (917/2014), jonka 3 §:n 22 kohdan mukaan sähköisellä viestillä tarkoitetaan tietoa, jota välitetään tai jaetaan sähköisesti. Käytännössä sähköiset viestit ovat siis mitä hyvänsä tietoverkossa liikkuvaa dataa. Tätäkin säännöstä on tulkittava riskiperusteisesti siten, että korkeamman turvallisuusluokan järjestelmissä suojaaminen on toteutettava ottaen huomioon tiedon luottamuksellisuuden vaarantumisesta aiheutuva vahinko ja tietoon lähtökohtaisesti kohdistuvat edistyneemmät hyökkäysmenetelmät ja niitä vastaan suojautumisen keinot. Suojautuminen verkkohyökkäyksiä vastaan sinänsä on jo tiedonhallintalain 13 §:n 1 momentissa säädetyn tietojärjestelmien tietoturvallisuudesta huolehtimisen velvoitteenkin nojalla toteutettava jollain tasolla kaikissa viranomaisen tietojärjestelmissä jo pelkästään tiedon eheyden ja saatavuuden turvaamiseksi.

Kohdan 3 mukaan tietojärjestelmien ja tietoliikennejärjestelyjen suojauksista ja niiden tarkoituksenmukaisesta toiminnasta tulisi huolehtia niiden koko elinkaaren ajan.

Myös tämä velvoite koskee (riskienhallinnan keinoin toteutettuna) muitakin kuin turvallisuusluokiteltujen asiakirjojen käsittelyyn käytettäviä tietojärjestelmiä ja tietoliikennejärjestelyjä. Elinkaaren ajan kestävään suojaamiseen sisältyy oleellisesti esimerkiksi ohjelmistohaavoittuvuuksien hallintamenettelyt, pitäen turvallisuuden näkökulmasta keskeiset ohjelmistot turvallisuuspäivitysten tasalla, sekä muun muassa muutostenhallintaan ja varmuuskopiointiin liittyvät menettelyt.

Kohdan 4 mukaan tietojärjestelmän ja tietoliikennejärjestelyn käyttäjille olisi annettava vain ne tiedot, oikeudet tai valtuudet, jotka ovat tehtävien suorittamiseksi välttämättömiä.

Kohdan 5 mukaan tietojen luvaton muuttaminen tai käsittely olisi estettävä käyttöoikeushallinnalla ja muilla tarvittavilla turvallisuusjärjestelyillä Vaatimukset sisältyvät yleisemmällä tasolla, kaikkia viranomaisen tietojärjestelmiä koskevana myös tiedonhallintalakiin, jonka 16 §:n mukaan viranomaisen on määriteltävä tietojärjestelmän käyttöoikeudet. Käyttöoikeudet on määriteltävä käyttäjän tehtäviin liittyvien käyttötarpeiden mukaan ja ne on pidettävä ajantasaisina. Edelleen lain 13 §:ään sisältyy yleinen velvollisuus huolehtia tietojärjestelmien tietoturvallisuudesta mukaan lukien tietojen eheydestä.

Kohdan 6 mukaan tietojärjestelmien ja tietoliikennejärjestelyjen käyttäjien ja laitteistojen tunnistamiseksi tulisi toteuttaa riittävät menetelmät. Vastaava vaatimus sisältyy salassa pidettävien asiakirjojen siirtämisen osalta tiedonhallintalain 14 §:n 1 momenttiin, jonka mukaan viranomaisen on toteutettava tietojensiirto yleisessä tietoverkossa salattua tai muuten suojattua tiedonsiirtoyhteyttä tai -tapaa käyttämällä, jos siirrettävät tiedot ovat salassa pidettäviä. Lisäksi tietojensiirto on järjestettävä siten, että vastaanottaja varmistetaan tai tunnistetaan riittävän tietoturvallisella tavalla ennen kuin vastaanottaja pääsee käsittelemään siirrettyjä salassa pidettäviä tietoja.

Kohdan 7 mukaan tietojärjestelmissä ja tietoliikennejärjestelyissä tulisi ottaa käyttöön vain käyttövaatimusten kannalta välttämättömät toiminnallisuudet. Tämäkin velvoite sisältyy yleiseen velvollisuuteen huolehtia tietojärjestelmän tietoturvallisuudesta. On toki otettava huomioon, että mitä korkeamman turvallisuusluokan tietojärjestelmästä tai tietoliikennejärjestelystä on kyse, sitä huolellisemmin on arvioitava, mitkä toiminnallisuudet oikeasti on oltava käytössä ja millä edellytyksillä.

Kohdan 8 mukaan tietojärjestelmän ja tietoliikennejärjestelyn salausratkaisujen tulisi olla kyseiselle turvallisuusluokalle riittävän turvallisia. Säännöksellä on liityntä esimerkiksi asiakirjan siirtämistä tietoverkossa koskevaan 12 §:ään ja asiakirjan kuljettamista koskevaan 13 §:ään, joissa säädetään sähköisen asiakirjan salaamisesta. Salaus olisi toteutettava turvallisuusluokalle riittävän turvallisella salauksella.

Kohdan 9 mukaan tietojärjestelmässä ja tietoliikennejärjestelyssä tulisi toteuttaa riittävät menettelyt turvallisuuteen liittyvien tapahtuminen jäljittämiseksi sekä turvallisuuspoikkeamien havaitsemiseksi. Säännöksessä on turvallisuusluokiteltavia asiakirjoja sisältävien tietojärjestelmien ja tietoliikennejärjestelyjen osalta tarkennettu tiedonhallintalain 13 §:n 1 momenttiin sisältyvää viranomaisen velvollisuutta seurata toimintaympäristönsä tietoturvallisuuden tilaa ja varmistetaan tietoaineistojen ja tietojärjestelmien tietoturvallisuus. Tiedonhallintalain 17 §:ssä puolestaan säädetään velvollisuus kerätä tietojärjestelmistä ns. lokitietoa.

Kohdan 10 mukaan tietojärjestelmän ja tietoliikennejärjestelyn fyysinen ympäristö tulisi suojata riittävästi. Säännöksellä on liityntä fyysistä turvallisuutta koskeviin vaatimuksiin 9 ja 10 §:ssä. Tietojärjestelmissä ja tietoliikennejärjestelyissä fyysisellä suojauksella tarkoitetaan lähes poikkeuksetta kyseisen turvallisuusluokan tiedon säilyttämiseen edellytettävien fyysisten suojausten toteuttamista. Vaikka tieto siirrettäisiin tietojärjestelmässä tai tietoliikennejärjestelyssä käsittelyn jälkeen toiseen, turva-alueelle sijaitsevaan tietojärjestelmän tai tietoliikennejärjestelyn osaan, tulisi koko tietojärjestelmä tai tietoliikennejärjestely suojata eheyden varmistamiseksi myös fyysisen turvallisuuden menetelmin käsiteltävän turvallisuusluokan mukaisesti. Poikkeuksena on tilanne, jossa tietojärjestelmä tai tietoliikennejärjestely voidaan fyysisesti siirtää tiedon käsittelyn ajaksi eri fyysiseen tilaan, kuin missä sitä säilytetään käsittelyn päätyttyä. Mikäli tietovälineen tietosisältö olisi luottamuksellisuuden osalta turvallisuusluokan III mukaisella salauksella suojattuna, ja tietovälineen eheys pystyttäisiin varmistamaan turvallisuusluokan III mukaisilla menetelmillä, turvallisuusluokan III tietovälinettä voitaisiin myös säilyttää hallinnollisella alueella. Nykytekniikalla eheyden turvallisuusluokalle III riittävä varmistaminen on usein luottamuksellisuutta haastavampaa, mutta asetuksella ei halua poissulkea tätä mahdollisuutta tekniikan kehittymisen myötä.

Ehdotettuun 11 §:n 2 momenttiin sisältyisi voimassaolevan tietoturvallisuusasetuksen 16 §:n 4 momenttia vastaava, mutta hieman täsmennetty, sähköiseen käsittelyyn liittyvä ns. TEMPEST –vaatimus. Säännöksen mukaan käsiteltäessä turvallisuusluokan III—I asiakirjoja sähköisesti, on pidettävä huolta, että hajasäteilyyn ja elektroniseen tiedusteluun liittyviä riskejä on pienennetty riittävästi. Riskien pienentämiseksi toteutettavat tietoturvallisuustoimenpiteet olisi suhteutettava tietojen hyväksikäytön riskiin ja turvallisuusluokan tasoon.

Ehdotetussa 12 §:ssä säädettäisiin vaatimukset asiakirjan siirtämiselle tietoverkon kautta. Turvallisuusluokiteltuja asiakirjoja voitaisiin siirtää viranomaisen fyysisesti suojatun turvallisuusalueen ulkopuolelle tai kyseistä turvallisuusluokkaa matalamman turvallisuustason tietojärjestelmän tai tietoliikennejärjestelyn kautta vain salatussa muodossa. Jos turvallisuusluokiteltujen tietojen siirtäminen tapahtuu turva-alueilla tai hallinnollisilla alueilla ja tietojen riittävä suojaus voidaan toteuttaa fyysisen suojaamisen menetelmin, voidaan käyttää salaamatonta siirtoa tai alemman tason salausta.

Säännös koskisi siis asiakirjan siirtämistä tietoverkon kautta. Mikäli asiakirjaa kuljetetaan sähköisessä muodossa tietojärjestelmässä (esimerkiksi kannettavassa tietokoneessa taikka muulla tallennusvälineellä), tulisi noudattaa, mitä asiakirjan kuljettamisesta säädetään 13 §:ssä.

Jos turvallisuusluokiteltua tietoa on kiireellisesti välttämätöntä siirtää tietoverkossa esimerkiksi vakavan vaaratilanteen torjumiseksi, mutta tietoa ei ole siirron osapuolten välillä puuttuvien salausratkaisujen vuoksi mahdollista salata asianmukaisesti, tietojen siirto voi olla (ilman teon rangaistavuutta) mahdollista rikoslain 4 luvun 5 §:n pakkotilaa koskevan sääntelyn perusteella ilman salausta tai muulla kuin kyseiselle turvallisuusluokalle käytetyllä salausmenetelmällä. Tiedon siirron toteuttamisessa on otettava luonnollisesti huomioon, kuuluuko tieto kansainvälisen tietoturvallisuusvelvoitteen piiriin ja johtuuko kyseisestä velvoitteesta jotain erityisiä vaatimuksia tiedon siirrolle.

Ehdotetussa 13 §:ssä säädettäisiin asiakirjan kuljettamisesta viranomaisen fyysisesti suojatun turvallisuusalueen – eli käytännössä 9 §:ssä tarkoitettujen turvallisuusalueiden ulkopuolella. Ehdotetussa 1 momentissa säädettäisiin sähköisten tiedon tallennusvälineiden suojaamisesta (kyseiselle turvallisuusluokalle) riittävällä salauksella. Mikäli tiedon tallennusväline olisi riittävästi salattu, se voitaisiin lähettää esimerkiksi postitse vastaanottajalle

Ehdotetussa 2 momentissa säädettäisiin salaamattomien asiakirjojen (joko paperisten tai sähköisten) kuljettamisesta. Turvallisuusluokan III — I salaamaton asiakirja olisi kuljettamista varten pakattava asianmukaisesti sekä kuljetettava se jatkuvan valvonnan alaisuudessa vastaanottajalle. Pakkaamisessa tulee huomioida muun muassa se, että pakkaus ei ulkoisesti paljasta sisältävänsä turvallisuusluokiteltua tietoa, pakkauksen ulkokuoressa on osoite, jonne pakkaus tulee toimittaa (esimerkiksi kuljetuksen aikana tapahtuneen liikenneonnettomuuden seurauksena) ja pakkauksen ulkokuoren sisällä vasta ilmaistaan pakkauksen sisällön sisältävän turvallisuusluokiteltua tietoa. Asiakirja voitaisiin kuljettaa vastaanottajalle myös muulla viranomaisen hyväksymällä turvallisella tavalla, jolla asiakirjan luottamuksellisuus ja eheys varmistetaan.

Salaamattoman asiakirjan kuljettamista koskevat vaatimukset eivät koske turvallisuusluokan IV asiakirjoja, joten niitä sisältäviä tiedon tallennusvälineitä sekä paperisia asiakirjoja on mahdollista kuljettaa myös salaamattomina ja antaa esimerkiksi postin kuljetettavaksi, ellei riskienhallinnan perusteella päädytä muuhun ratkaisuun.

Asetuksen 14 §:ssä säädettäisiin voimassa olevan tietoturvallisuusasetuksen 17 §:n 1 momenttia, 18 §:n 2 momenttia ja 20 §:ää vastaavasti asiakirjan käsittelyn kirjaamisesta, kopioinnista ja kopioiden kirjaamisesta. Erityisesti asiakirjan kopiointiin saattaa johtua lisävaatimuksia kansainvälisistä tietoturvallisuusvelvoitteista, tästä syystä säännöksen alkuun on lisätty sen soveltuvan, ellei kansainvälisestä tietoturvallisuusvelvoitteesta muuta johdu.

Ehdotetun 14 §:n 1 momentin 1 kohdan mukaan turvallisuusluokan III—I asiakirjan käsittely olisi kirjattava sähköiseen lokiin, tietojärjestelmään, asianhallintajärjestelmään, manuaaliseen diaariin tai asiakirjaan.

Ehdotetun 14 §:n 1 momentin 2 kohdan mukaan turvallisuusluokan III—I asiakirjan lähettäminen ja vastaanottaminen olisi myös kirjattava. Lähettämistä ja vastaanottamista koskeva kirjaamisvelvoite on kansainvälisiä tietoturvallisuusvelvoitteita mukaillen laajennettu koskemaan turvallisuusluokan I ja II asiakirjojen lisäksi myös turvallisuusluokan III asiakirjoja. Kirjaamisvelvollisuus koskisi sitä, kun asiakirja saapuu organisaatioon tai lähtee sieltä. Sisäisen käsittelyn kirjaamisvelvoite sisältyisi 1 momenttiin.

Ehdotetun 14 §:n 1 momentin 3 kohdan mukaan turvallisuusluokan II—I asiakirjaa ei saisi kopioida ilman sen laatineen viranomaisen antamaa lupaa. Kansainvälisissä tietoturvallisuusvelvoitteissa saatetaan edellyttää kirjallista lupaa, mikä on otettava huomioon näiden asiakirjojen kopioinnissa.

Kohdan 4 mukaan turvallisuusluokan II—I asiakirjojen kopiot ja niiden käsittelijät olisi luetteloitava.

Ehdotettu 2 momentti sisältäisi informatiivisen viittauksen sähköisen kopioinnin osalta sähköistä käsittelyä koskevaan 11 §:ään.

Tiedonhallintalain 21 §:n 2 momentin mukaan säilytysajan päättymisen jälkeen tietoaineistot on arkistoitava tai tuhottava viipymättä tietoturvallisella tavalla. Asetuksen 15 §:ssä täsmennettäisiin tietoturvallisen tuhoamisen vaatimusta turvallisuusluokiteltujen asiakirjojen osalta. Ehdotetun 15 §:n 1 momentin mukaan turvallisuusluokiteltu asiakirja olisi tuhottava tavalla, jolla estetään tietojen palauttaminen sekä kokoaminen uudelleen kokonaan tai osittain. Kyseiselle turvallisuusluokalle riittävän luotettavalla tuhoamisella tarkoitetaan esimerkiksi silppuamista, polttamista, sulattamista tai jotain muuta soveltuvaa menetelmää. Esimerkiksi tiedon silppuamisessa tulee huomioida, että riskiperusteisesti riittävät silppukoot eroavat turvallisuusluokittain.

Tarpeettomaksi käyneen turvallisuusluokan II—I asiakirjan kopio tulee tuhota, jollei sitä palauteta asiakirjan laatineelle viranomaiselle. Tuhoamisessa on otettava huomioon 14 §:ään sisältyvä vaatimus käsittelyn kirjaamisesta. Myös asiakirjan tuhoaminen olisi kirjattava. Tuhoamisesta on ilmoitettava asiakirjan laatineelle viranomaiselle. Tuhoamisen saisi suorittaa vain henkilö, jonka viranomainen on tähän tehtävään määrännyt ja jolla on oikeus käsitellä asiakirjaa työtehtäviensä perusteella. Asiakirjan valmisteluvaiheen versiot voi tuhota ne laatinut henkilö. Säännöstä sovellettaessa on otettava huomioon, että kansainvälisissä tietoturvallisuusvelvoitteissa voidaan edellyttää esimerkiksi turvallisuusluokan I ja II asiakirjojen tuhoamista todistajan läsnä ollessa ja sekä sitä, että sekä todistajan että tuhoajan tulee allekirjoittaa tuhoamisesta todistus, joka tallennetaan määriteltyyn kirjaamoon. Lisäksi kansainvälisissä tietoturvallisuusvelvoitteissa saatetaan edellyttää, että käsittelytarpeen lisäksi sekä tuhoajalla että todistajalla on oltava tuhottavan tiedon tasoinen turvallisuusselvitys (personnel security clearance, PSC) voimassa.

Asetuksen 15 §:n 3 momentti sisältäisi informatiivisen viittaussäännöksen arkistolakiin (831/1994).

Asetuksen 16 §:ään sisältyisi voimaantulosäännöksen lisäksi siirtymäsäännökset. Asetus tulisi voimaan 1.1.2020.

Ehdotetun 2 momentin mukaan turvallisuusluokittelua koskevan merkinnän tarve arkistoitujen tai valtionhallinnon viranomaisella säilytettävänä olevien asiakirjojen osalta olisi arvioitava siinä vaiheessa, kun valtionhallinnon viranomainen ottaa asiakirjan uudelleen käsittelyyn.

Ehdotetun 3 momentin mukaan valtionhallinnon viranomaisen olisi saatettava turvallisuusluokiteltujen asiakirjojen käsittely vastaamaan tässä asetuksessa säädettyjä vaatimuksia kolmen vuoden kuluessa asetuksen voimaantulosta.

Pykälän 4 momentin mukaan valtionhallinnon viranomaisen asetuksen voimaan tullessa käytössä olevien toimitilojen olisi täytettävä asetuksessa säädetyt vaatimukset tilojen turvallisuudelle kolmen vuoden kuluessa asetuksen voimaantulosta. Sama koskee toimitiloja, jotka on otettu käyttöön ennen kuin on kulunut kaksi vuotta asetuksen voimaantulosta.

5 Vaikutukset

Turvallisuusluokittelun vaikutuksia ja taloudellisia vaikutuksia on arvioitu hallituksen esityksessä 284/2018 eduskunnalle laiksi julkisen hallinnon tiedonhallinnasta sekä eräiksi siihen liittyviksi laeiksi. Ehdotukseen sisältyvän sääntelyn on hallituksen esityksessä todettu lähinnä korvaavan ja tarkentaen voimassa olevaa sääntelyä. Lisäksi on todettu, että ehdotukseen sisältyvien velvoitteiden toteuttaminen voidaan kattaa olemassa olevien voimavarojen uudelleen järjestelyillä.

Ehdotetulla asetuksella ei ole hallituksen esityksestä eriäviä taloudellisia vaikutuksia. Ehdotuksella ei arvioida olevan merkittäviä vaikutuksen valtiontalouteen.

Tietoturvallisuutta ja tietojen turvallisuusluokittelua koskevat säännösehdotukset vastaavat pääosin valtion viranomaisia koskevaa voimassa olevaa sääntelyä tosin sillä erolla, että turvallisuusluokittelun tekeminen on tähän mennessä ollut valtionhallinnon viranomaisellekin vapaaehtoista.

Siirtymäsäännösten johdosta niillä viranomaisilla, jotka eivät ole tähän mennessä luokitelleet asiakirjoja, on kolme vuotta aikaa toteuttaa asetuksessa säädetyt tietoturvallisuustoimenpiteet. Valtaosalla viranomaisia ei ole kuin enintään turvallisuusluokan IV asiakirjoja, joiden käsittelyn tietoturvallisuustoimenpiteiden toteuttaminen ei edellytä merkittävästi pidemmälle meneviä toimenpiteitä kuin salassa pidettävän tiedon tai henkilötietojen suojaaminen. Monet niistä viranomaisista, jotka käsittelevät merkittävässä määrin turvallisuusluokkaa IV ylemmän luokan asiakirjoja, ovat jo soveltaneet voimassa olevan tietoturvallisuusasetuksen velvoitteita. Näitä velvoitteita ei ole tarkoitus olennaisesti tiukentaa tällä asetuksella.

6 Asetuksen valmistelu

Tiedonhallintalain tietoturvallisuussäännöksiä sekä asetuksessa ehdotettua turvallisuusluokittelua koskevaa sääntelyä on valmisteltu ensin valtiovarainministeriön asettamassa tietoturvallisuuden säädöstön valmistelun ohjausryhmässä 11.4.2016 - 28.2.2017. Tämän jälkeen valmistelua on tehty tiedonhallintalain valmistelun osana julkisen hallinnon tiedonhallinnan kehittämistä selvittävässä työryhmässä (toimikausi 17.11.2016—31.5.2017) sekä valtiovarainministeriön asettamassa tiedonhallintalain valmistelutiimissä 10.1.-31.9.2018 sekä tiiviissä yhteistyössä turvallisuusluokiteltujen asiakirjojen käsittelyn asiantuntijaviranomaisten kanssa.

Asetus toimitettiin lausunnoille 13.6.-30.8.2019. Lausuntoja saatiin yhteensä [X]. Lausunnoissa kiinnitettiin huomiota [X]. Saatujen kommenttien johdosta [X].

[Asetusehdotuksen suomen- ja ruotsinkielinen versio on tarkastettu oikeusministeriön lainvalmisteluosaston laintarkastusyksikössä.]

7 Voimaantulo

Tarkoitus on esittää tiedonhallintalain voimaantuloajaksi 1.1.2020. Samaan aikaan tulee voimaan julkisuuslain asiakirjojen luokittelua ja tietoturvallisuusvaatimuksia sekä asetuksenantovaltuutta koskevien säännösten kumoaminen, jonka johdosta kumoutuu myös asetuksenantovaltuuksien nojalla annettu tietoturvallisuusasetus. Kansainvälisten tietoturvallisuusvelvoitteiden noudattamisen näkökulmasta on tärkeää,

että turvallisuusluokiteltuja asiakirjoja koskevat tietoturvallisuusvaatimukset tulevat voimaan samaan aikaan kun edelliset vaatimukset lakkaavat olemasta voimassa.

Asetus ehdotetaan tulemaan voimaan 1 päivänä tammikuuta 2020.