VALTIONEUVOSTO
STATSRÅDET

Viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden ja varautumisen arviointia koskevat säädösehdotukset

23.9.2025

Työryhmän loppuraportti

Esipuhe

Valtiovarainministeriö asetti 22.2.24 tietojärjestelmien vaatimustenmukaisuuden arvioinnin ajantasaistamisen ja tehostamisen työryhmän toimikaudeksi 1.3.24–31.12.25. Ryhmä valmisteli ensin Tietojärjestelmien tietoturvallisuuden ja varautumisen vaatimustenmukaisuuden arvioinnin nykytila-arvio ja kehittämisehdotukset -raportin 12.12.24. Yhteiskunnan uudistamisen ministerityöryhmä käsitteli 7.3.25 työryhmän säädösvalmistekohteita. Tähän perustuen työryhmä valmisteli säädösehdotukset hallituksen esityksen muotoon raportiksi. Ehdotuksia on käsitelty työryhmän julkiselle hallinnolle 9.9.25 ja yritysten edustajille 11.9.25 järjestämissä sidosryhmätilaisuuksissa. Sidosryhmätilaisuuksiin osallistui noin 220 julkisen hallinnon ja 30 yritysten edustajaa.

Ehdotusten keskeisinä **tavoitteina** on mahdollistaa kustannustehokkaat viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden ja varautumisen arviointimenettelyt sekä vastata toimintaympäristön ja turvallisuusuhkien muutoksesta johtuvaan arviointitarpeiden kasvuun. Tavoitteena on selkeyttää lainsäädännön tasolla periaatetta siitä, että viranomaisella on vastuu omien tietojärjestelmiensä ja tietoliikennejärjestelyjensä tietoturvallisuudesta ja varautumisesta. Lisäksi tavoitteena on salaustuotteiden ja muiden turvallisuuskriittisten ratkaisujen arvioinnin ja hyväksynnän kautta parantaa yritysten mahdollisuuksia tarjota ratkaisujaan sekä Suomessa että kansainvälisissä yhteyksissä.

Työryhmä ehdottaa, että **Pääesikunnan määrätylle turvallisuusviranomaiselle** säädettäisiin itsenäinen ja riippumaton arviointiviranomaisen tehtävä, mikä vastaisi arviointitarpeiden kasvuun. Nykyisin arviointiviranomaisena toimivan Liikenne- ja viestintäviraston tehtäviä tarkennettaisiin, mikä sujuvoittaisi arviointimenettelyjä ja sitä kautta vastaisi arviointitarpeiden kasvuun kustannustehokkaasti. Liikenne- ja viestintävirastolla olisi yleinen toimivalta toteuttaa turvallisuusluokiteltuja tietoja käsittelevien tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden ja varautumisen arviointeja. Lakiin lisättäisiin seikkoja, jotka viraston tulisi ottaa huomioon asettaessaan tehtäviään tärkeysjärjestykseen ja tehdessään päätöksen siitä, ottaako virasto haetun arvioinnin tehtäväksi. Lain tasolle tuotaisiin Liikenne- ja viestintäviraston neuvontatehtävä. Säädettäisiin arviointiviranomaisten yhteistyöstä ja Liikenne- ja viestintäviraston koordinaatioroolista sekä mahdollistettaisiin arviointiviranomaista avustava tehtävä ja säädettäisiin VTT Oy:n avustavasta arviointitehtävästä.

Tietoturvallisuuden lisäksi arvioitaisiin **varautumista** tietojärjestelmiä ja tietoliikennejärjestelyjä koskeviin häiriötilanteisiin ja kriiseihin. Varautumisen arvioinnin merkitys on kasvanut toimintaympäristön muutosten vuoksi. Kriiseihin varautuminen koskisi esimerkiksi tietojärjestelmien ja tietoliikennejärjestelyjen tietoliikenneyhteyksiä, laitteita, ohjelmistoja ja tiloja sekä niiden kahdentamista ja ylläpitoon tarvittavaa henkilöstöä.

Arviointimenettelyjen osalta laajennettaisiin viranomaisten valinnanvapautta, mikä osaltaan vastaisi arviointitarpeiden kasvuun. Arviointimenettelyjä olisivat viranomaisen toteuttama itsearviointi, viranomaisen toimeksiannosta palveluntarjoajan toteuttama arviointi, tietoturvallisuuden arviointilaitoksen toteuttama arviointi sekä arviointiviranomaisen toteuttama arviointi. Tietojärjestelmän tai tietoliikennejärjestelyn arvioinnissa käytettäisiin riskiarvioinnin ja käsiteltävien tietojen turvallisuusluokan perusteella eri arviointimenettelyitä järjestelmän eri osien arvioinnissa ja järjestelmän elinkaaren aikana. Valtionhallinnon viranomaiset kuitenkin velvoitettaisiin toteuttamaan **vähintään itsearviointeja**, sillä viranomaisen on varmistettava tietoaineistojensa ja tietojärjestelmiensä tietoturvallisuus.

Viranomainen voisi käyttää arviointien tukena markkinatoimijoita, sillä kaikilla luotettavaksi katsotuilla yrityksillä olisi mahdollisuus tarjota korkeintaan **turvallisuusluokan IV** tietoja

käsittelevien tietojärjestelmien ja tietoliikennejärjestelyjen arviointipalveluja viranomaisille. Korkeimpien turvallisuusluokkien tietojen käsittelyn suojaamiseksi kaikki viranomaiset velvoitettaisiin pyytämään arviointiviranomaisen tai hankkimaan tietoturvallisuuden arviointilaitoksen arviointi **turvallisuusluokan III** tietoja käsitteleville tietojärjestelmille ja tietoliikennejärjestelyille, ellei viranomainen päättäisi arvioinnin pyytämisen tai hankkimisen olevan tietojärjestelmän tai tietoliikennejärjestelyn riskiarvioinnin perusteella tarpeetonta. Lisäksi kaikki viranomaiset velvoitettaisiin pyytämään arviointiviranomaisen arviointia **turvallisuusluokan I ja II** tietoja käsitteleville tietojärjestelmille ja tietoliikennejärjestelyille.

Lisäksi ehdotetaan, että **turvallisuuskriittisten ratkaisujen** tietoturvallisuuden arviointia koskeva tehtävä säädettäisiin Liikenne- ja viestintävirastolle suomalaisten valmistajien ratkaisujen julkisen hyväksynnän ja viranomaisten järjestelmissä käytettävien ratkaisujen osalta sekä Pääesikunnan määrätylle turvallisuusviranomaiselle Puolustusvoimien järjestelmien osalta. Turvallisuuskriittisellä ratkaisulla tarkoitettaisiin salaus-, hajasäteilysuojaus- ja muuta tuotetta, jolla suojataan turvallisuusluokiteltua tietoa tietojärjestelmissä ja tietoliikennejärjestelyissä.

Tietoturvallisuuden **arviointilaitoksia** koskevia säännöksiä yksinkertaistettaisiin. Yritysturvallisuusselvitys olisi uutena selvitysmenettelynä arviointilaitokseksi hyväksymisprosessissa, mikä nopeuttaisi hyväksymisprosessia. Liikenne- ja viestintävirasto voisi akkreditoinnille vaihtoehtoisena menettelynä vastata lisäpätevyyksien hyväksymisestä, mikä joustavoittaisi ja nopeuttaisi lisäpätevyyksien hakemista. Alihankinnan reunaehdoista säädettäisiin, mikä mahdollistaisi arviointilaitoksille joustavamman resurssien käytön. Tarkennettaisiin Liikenne- ja viestintäviraston tiedonsaantioikeuksia, mikä tehostaisi arviointilaitosten valvontaa. Varmistettaisiin, että arviointilaitoslaki on ajan tasalla ja linjassa arviointilakiin ehdotettavien muutosten kanssa, jotta arviointeja koskeva sääntely olisi selkeää. Täydennettäisiin lakia rikosoikeudellisen virkavastuun, hallinnon yleislakien soveltamisen ja arviointilaitosten valvonnasta perittävien maksujen osalta.

Hallituksen esitys eduskunnalle laeiksi viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annetun lain, tietoturvallisuuden arviointilaitoksista annetun lain sekä turvallisuusselvityslain muuttamisesta

ESITYKSEN PÄÄASIALLINEN SISÄLTÖ

Esityksessä ehdotetaan muutettavaksi lakia viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista, lakia tietoturvallisuuden arviointilaitoksista sekä turvallisuusselvityslakia.

Lakiin viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista ehdotetuilla muutoksilla selkeytettäisiin viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen arviointimenettelyjä ja parannettaisiin niiden saatavuutta mahdollistamalla nykyistä useampia arviointimenettelyjä. Myös muille luotettaviksi todetuille yrityksille kuin tietoturvallisuuden arviointilaitoksille säädettäisiin mahdollisuus tarjota tietoturvallisuuden ja varautumisen arviointipalveluja viranomaisille korkeintaan turvallisuusluokan IV tietojen käsittelyn arviointiin saakka. Tarkoituksena on, että mahdollisimman moni viranomainen toteuttaisi riskiperusteisesti ja suunnitelmallisesti tietojärjestelmiensä ja tietoliikennejärjestelyjensä arviointeja. Lakiin lisättäisiin valtionhallinnon viranomaisille velvoite arvioida tietojärjestelmänsä ja tietoliikennejärjestelynsä vähintään itsearviointeina. Muiden viranomaisten olisi mahdollista toteuttaa lain mukaisia arviointeja. Viranomaisten tulisi kuitenkin pyytää arviointiviranomaisen arviointia turvallisuusluokan I ja II tietojen käsittelylle. Viranomaisen tulisi pyytää arviointiviranomaisen arviointia tai hankkia tietoturvallisuuden arviointilaitoksen arviointi turvallisuusluokan III tietojen käsittelylle, ellei viranomainen riskiperustaisesti päätä sen olevan tarpeetonta. Ehdotetuilla muutoksilla tehostettaisiin arviointeja korostamalla riskiarvion merkitystä arviointimenettelyn valinnassa ja painotettaisiin viranomaisten vastuuta omien tietojärjestelmiensä ja tietoliikennejärjestelyjensä tietoturvallisuudesta ja varautumisesta sekä käyttöönottopäätöksistä.

Muutoksilla tarkennettaisiin Liikenne- ja viestintäviraston tehtäviä ja säädettäisiin turvallisuuskriittisten tuotteiden valmistajille oikeus hakea arviointia. Lisäksi lakiin lisättäisiin Puolustusvoimille arviointitehtävä, jolla vastattaisiin turvallisuusympäristön muutoksista johtuvaan arviointitarpeiden kasvuun. Muutoksilla tarkennettaisiin ja tehostettaisiin arviointiviranomaisten yhteistyötä, työjakoa ja tiedonsaantioikeuksia sekä mahdollistettaisiin arviointiviranomaista avustava tehtävä.

Lakiin tietoturvallisuuden arviointilaitoksista ehdotetuilla muutoksilla edistettäisiin tietoturvallisuuden arviointilaitosten elinkeinotoiminnan edellytyksiä yksinkertaistamalla ja tehostamalla tietoturvallisuuden arviointilaitosten luotettavuuden sääntelyä ja joustavoittamalla pätevyyksien hyväksyntää.

Lait on tarkoitettu tulemaan voimaan x.x.2026

SISÄLLYS

PERUSTELUT

1 Asian tausta ja valmistelu

1.1 Tausta

Tietoturvallisuuden ja varautumisen arvioinnilla selvitetään säädettyjen ja riskiarvioinnin perusteella valittujen vaatimusten täyttymistä tietojärjestelmissä, tietoliikennejärjestelyissä ja turvallisuuskriittisissä tuotteissa. Julkisen hallinnon tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnin keskeinen sääntely, laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1046/2011) jäljempänä *arviointilaki*, sekä laki tietoturvallisuuden arviointilaitoksista (1045/2011) jäljempänä *arviointilaitoslaki,* on valmisteltu yli 12 vuotta sitten.

Digitalisaation edistyminen ja kehittyvät teknologiat kuten pilvipalvelut, tekoäly ja kvanttilaskenta ovat vaikuttaneet sekä julkisen hallinnon toimintatapoihin että niihin menettelyihin, joilla julkisen hallinnon tietojärjestelmiä toteutetaan. Keskeistä arviointeihin liittyvää kansallista sääntelyä kuten laki julkisen hallinnon tiedonhallinnasta (906/2019), jäljempänä *tiedonhallintalaki,* sekä turvallisuusselvityslaki (726/2014) on valmistunut arviontilain ja arviointilaitoslain jälkeen. Lisäksi tietoturvallisuuden vaatimuksenmukaisuuden arviointia koskeva EU-sääntely on lisääntynyt viime vuosina. Näiden muutosten sekä aikaisemmin tehtyjen selvitysten perusteella on tunnistettu tarve tietoturvallisuuden ja varautumisen arviointia koskevan sääntelyn ajantasaistamiselle ja tehostamiselle.

Suomen uusi kyberturvallisuusstrategia vuosille 2024–2035 on hyväksytty valtioneuvoston periaatepäätöksenä 10.10.2024. Kyberturvallisuusstrategian hyväksymisen jälkeen on valmisteltu sen toimeenpanosuunnitelma, jossa määritellään kehittämistoimet strategian tavoitteiden saavuttamiseksi. Tietojärjestelmien, tietoliikennejärjestelyjen ja turvallisuuskriittisten tuotteiden tietoturvallisuuden arviointia koskevan lainsäädännön ajantasaistaminen kuuluu toimeenpanosuunnitelman priorisoituihin toimenpiteisiin. Valtioneuvoston puolustusselonteossa 2024 (2024:5) todetaan, että tavoitetilassa Puolustusvoimilla on itsenäinen kyky tietojärjestelmien ja salaustuotteiden arviointi- ja hyväksyntätoimintaan. Tämä edellyttää arviointilain muuttamista vastaavasti. Pääministeri Petteri Orpon hallituksen hallitusohjelman mukaan salaustuotteiden hyväksyntäprosessia nopeutetaan, jotta kotimainen kyberteknologia saadaan nopeammin markkinoille. Suomen tavoitteena on hankkia itselleen kansainvälisiä tietoturvahyväksyntöjä myöntävän maan asema EU:ssa. Näiden tavoitteiden edistämiseksi arviointilakia on muutettava.

1.2 Valmistelu

Valtiovarainministeriö asetti 22.2.2024 tietojärjestelmien vaatimustenmukaisuuden arvioinnin ajantasaistamisen ja tehostamisen työryhmän toimikaudeksi 1.3.2024–31.12.2025 (VN/36127/2023). Työryhmän tavoitteena oli arvioida nykyisen arviointilainsäädännön ajantasaistamistarpeet ja arviointien tehostamiskeinot ottaen huomioon itsearviointien hyödyntämisen tarjoamat mahdollisuudet, kustannustehokkuus ja toimintaympäristön muutokset.

Työryhmän puheenjohtajuus oli valtiovarainministeriössä ja jäsenet olivat valtiovarainministeriöstä, valtioneuvoston kansliasta, ulkoministeriöstä, ulkoministeriön kansallinen turvallisuusviranomainen (NSA) -yksiköstä, oikeusministeriöstä, sisäministeriöstä, puolustusministeriöstä, maa- ja metsätalousministeriöstä, liikenne- ja viestintäministeriöstä, kyberturvallisuusjohtajan toimistosta, sosiaali- ja terveysministeriöstä, työ- ja elinkeinoministeriöstä, Tietosuojavaltuutetun toimistosta, Valtion tieto- ja viestintätekniikkakeskus Valtorista, Digi- ja väestötietovirastosta, Liikenne- ja viestintävirastosta, Puolustusvoimista, Hyvinvointialueyhtiö Hyvil Oy:stä ja

Kuntaliitosta. Työryhmä kokoontui 17 kertaa. Työryhmän tukena toimivan asiantuntijasihteeristön jäsenet olivat valtiovarainministeriöstä, puolustusministeriöstä, liikenne- ja viestintäministeriöstä, sisäministeriöstä, Puolustusvoimista ja Liikenne- ja viestintävirastosta sekä lisäksi vuoden 2024 ajan Valtion tieto- ja viestintätekniikkakeskus Valtorista ja Digi- ja väestötietovirastosta. Sihteeristö kokoontui yhteensä 30 kertaa.

Työryhmän tehtävät jaettiin kahteen vaiheeseen. Ensimmäisessä vaiheessa työryhmä valmisteli Tietojärjestelmien tietoturvallisuuden ja varautumisen vaatimustenmukaisuuden arvioinnin nykytila-arvio ja kehittämisehdotukset -raportin 12.12.2024. Ensimmäisen vaiheen raportista järjestettiin sidosryhmätilaisuus julkiselle hallinnolle ja elinkeinoelämälle 21.11.2024.

Yhteiskunnan uudistamisen ministerityöryhmä käsitteli 7.3.2025 työryhmän säädösvalmistekohteita. Tähän perustuen työryhmä valmisteli säädösehdotukset hallituksen esityksen muotoon raportiksi 23.9.2025. Ehdotuksia käsiteltiin työryhmän julkiselle hallinnolle 9.9.2025 ja yritysten edustajille 11.9.2025 järjestämässä sidosryhmätilaisuudessa. Sidosryhmätilaisuuksiin osallistui noin 220 julkisen hallinnon ja 30 yritysten edustajaa.

Hallituksen esityksen luonnos oli lausuntokierroksella xx.xx.xxxx – xx.xx.xxxx. Lausuntoa pyydettiin: [Täydennetään lausuntokierroksen jälkeen]

Hallituksen esityksen valmisteluasiakirjat ovat saatavilla julkisessa palvelussa osoitteessa: https://vm.fi/hankkeet tunnuksella VM167:00/2023.

2 Nykytila ja sen arviointi

Viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arviointi

Viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista säädetään arviointilaissa. Viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen arviointi koskee nykytilassa ainoastaan tietoturvallisuuden arviointia. Arviointilaissa ei määritellä tietoturvallisuutta, mutta lain esitöissä (HE 45/2011 vp) viitataan kansainvälisiin velvoitteisiin, joiden perusteella tietoturvallisuudella voidaan katsoa tarkoitettavan yleisesti tiedon luottamuksellisuuden, eheyden ja saatavuuden turvaamista. Kansainvälisesti korostetaan myös tiedon alkuperän ja kiistämättömyyden merkitystä. Tiedonhallintalaissa säädetään tietoturvallisuustoimenpiteistä, joilla tarkoitetaan tietoaineistojen saatavuuden, eheyden ja luottamuksellisuuden varmistamista hallinnollisilla, toiminnallisilla ja teknisillä toimenpiteillä. Tietoturvallisuustoimenpiteet voivat sisältää myös fyysisiä eli tiloihin liittyviä toimenpiteitä.

Tiedonhallintalain 13 §:ssä säädetään tiedonhallintayksikön tietojärjestelmien tietoturvallisuusvaatimuksista. Tiedonhallintalakiin vuonna 2023 lisätyn 13 a §:n mukaan tiedonhallintayksikön on selvitettävä sen tietoaineistojen käsittelyn, tietojärjestelmien hyödyntämisen sekä niihin perustuvan toiminnan jatkuvuuteen kohdistuvat olennaiset riskit ja varauduttava normaaliolojen ja poikkeusolojen häiriötilanteisiin. Toiminnan jatkuvuus ja varautuminen voivat kattaa monenlaisia toimenpiteitä kuten tärkeiden toimintojen ja tietojärjestelmien tunnistamista, riskien arviointia ja niiden hallintaa esimerkiksi teknisiä komponentteja kahdentamalla sekä resurssien ja toimintojen ja toimitusketjujen tarkastelulla ja hallinnalla ja toiminnan varajärjestelyillä vakavissa häiriötilanteissa, kriiseissä tai poikkeusoloissa. Varautumisen ja tietojärjestelmien hyödyntämisen ja niihin perustuvan toiminnan jatkuvuuden hallintatoimien arvioinnista ei tiedonhallintalain säännöksestä huolimatta säädetä voimassa olevassa arviointisääntelyssä ja soveltamisalaa olisi tarpeen laajentaa tietoturvallisuudesta myös varautumisen arviointiin. Varautumisen merkitys on kasvanut turvallisuusympäristön muutosten vuoksi.

Viranomaisille ei ole voimassa olevassa lainsäädännössä säädetty yleistä tietojärjestelmien ja tietoliikennejärjestelyjen arviointivelvoitetta. Tiedonhallintalain 13 §:n perusteella vastuu tietoaineistojen ja tietojärjestelmien tietoturvallisuuden varmistamisesta kuuluu tiedonhallintayksikölle. Pykälän 2 momentin mukaan viranomaisen tehtävien hoitamisen kannalta olennaisten tietojärjestelmien vikasietoisuus ja toiminnallinen käytettävyys on varmistettava riittävällä testauksella säännöllisesti. Saman pykälän 5 momentin mukaan viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista säädetään erikseen. Arviointi on tarkoituksenmukainen ja tavanomainen tapa varmistua tietoturvallisuus- ja varautumistoimenpiteiden toteuttamisesta ja riittävyydestä. Viranomainen vastaa tietojärjestelmiensä ja tietoliikennejärjestelyjensä turvallisuudesta. Näin ollen muuttuneessa turvallisuustilanteessa olisi perusteltua edellyttää, että valtionhallinnon viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen toteuttamisessa tehdään aina arviointeja. Tällöin olisi tarkasteltava myös arviointimenettelyjä eli sitä, mitkä tahot tekevät arviointeja ja myös arvioinnin sisältöä ja toteutustapoja.

Arviointilain 3 §:ssä säädetään valtionhallinnon viranomaisille sallituista arviointimenettelyistä. Säännöksen mukaan valtionhallinnon viranomaiset saavat käyttää tietojärjestelmiensä ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnissa vain Liikenne- ja viestintävirastoa tai arviointilaitoslain mukaisesti hyväksyttyä tietoturvallisuuden arviointilaitosta. Muiden kuin valtion viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden sallituista arviointimenettelyistä ei säädetä. Valtionhallinnon viranomaisten toteuttamien tietojärjestelmien ja tietoliikennejärjestelyjen itsearviointien suhde arviointilain 3 §:ään on jossain määrin epäselvä ja itsearviointien mahdollisuutta olisi tarpeen selventää.

Arviointivelvoitteita voi sisältyä sektorikohtaiseen lainsäädäntöön. Tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arviointia edellytetään toimialakohtaisesti sosiaali- ja terveydenhuollon asiakastietojen käsittelystä annetussa laissa (703/2023), jäljempänä *asiakastietolaki*, ja sosiaali- ja terveystietojen toissijaisesta käytöstä annetussa laissa (552/2019), jäljempänä *toisiolaki*, sekä valtioneuvoston asetuksessa julkisen hallinnon turvallisuusverkkotoiminnasta (1109/2015), jäljempänä *turvallisuusverkkoasetus*. Lain valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä (1226/2013), jäljempänä *Tori-laki*, mukaan valtion yhteisten tieto- ja viestintäteknisten palveluiden on täytettävä tarpeen mukaiset tietoturvallisuutta ja varautumista koskevat vaatimukset ja lain esitöissä (HE 150/2013 vp s 29) viitataan, että arviointi ja todentaminen voitaisiin tehdä arviointilain mukaisesti.

Viranomaisten tietojärjestelmiin kohdistuu arviointivelvoitteita myös kansainvälisten tietoturvallisuusvelvoitteiden johdosta. EU:n ja Naton turvallisuusluokitellun tiedon suojaamista koskee laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004). Suomi on kansallisesti saattanut voimaan EU:n ja Naton turvallisuusluokitellun tiedon suojaamista koskevat ja arviointivelvoitteita sisältävät turvallisuussäännöt kansainvälisistä tietoturvallisuusvelvoitteista annetun lain säätämisen yhteydessä sekä Pohjois-Atlantin sopimuksen osapuolten välillä tehdyn sopimuksen voimaansaattamisen yhteydessä (SopS 55-56/2023).

Arviointilaissa tai arviointilaitoslaissa ei säädetä millä perusteella arviointimenettely ja arvioinnin toteuttaja tulee valita. Arviointien toteuttamista ei myöskään ole rajattu turvallisuusluokitellun tiedon käsittelyn arviointiin, vaan se koskee yhtäläisesti kaikkia tietojärjestelmiä ja tietoliikennejärjestelyjä, eikä arviointilaissa säädetyissä arviointimenettelyissä ole huomioitu eri tietojärjestelmien ja tietoliikennejärjestelyjen tietojenkäsittelyn riskien eroja. Näin ollen on tunnistettu tarve tarkentaa voimassa olevan lainsäädännön arviointimenettelyjen valintaa turvallisuusluokkiin ja riskiarviointiin perustuvaksi.

Arviointilaissa ei säädetä nimenomaisesti myöskään siitä, että arvioinnissa tulee huomioida tietojärjestelmän tai tietoliikennejärjestelyn riskit. Tiedonhallintalain 13 §:ssä säädetyn velvoitteen

ja turvallisuusluokitteluun sisäänrakennetun riskinäkökulman takia arviointiperusteet määritellään käytännössä riskiperusteisesti ja arviointikriteeristöissä huomioidaan tietoturvallisuusuhkat, joiden toteutumisen todennäköisyys on suuri, ellei niiltä suojauduta riittävillä tietoturvallisuustoimenpiteillä, mutta riskien huomioiminen olisi perusteltua tuoda esille arviointilaissa.

Tietoturvallisuuden arviointien määrä ja kustannukset

Viranomaisten tietojärjestelmien tietoturvallisuuden arviointien työmäärä on viime vuosina kasvanut. Lisääntynyt arviointitarve on aiheuttanut ruuhkautumista arviointitoiminnassa.

- Kansainvälisiin tietoturvallisuusvelvoitteisiin liittyvät tarpeet ovat lisääntyneet etenkin Nato-jäsenyyden myötä. Naton turvallisuusluokitellun tiedon käsittelyyn tarkoitettujen viranomaisten tarkastettavien ja akkreditoitavien tietojärjestelmien lukumäärä on lähes kymmenkertaistunut huhtikuun 2022 ja huhtikuun 2024 välillä. Kansainvälisen tietoaineistojen käsittelyyn käytettävien tietojärjestelmien lukumäärä myös Puolustusvoimissa ja niiden käyttö kansainvälisissä harjoituksissa on kasvanut nopeasti ja merkittävästi.

- Liikenne- ja viestintävirasto tekee vuosittain useita kymmeniä tietojärjestelmäarviointeja. Järjestelmien laajuus ja siten arviointien tekninen laajuus, työmäärä ja kesto vaihtelevat paljon. Osa arvioinneista on muutos- tai määräaikaisarviointeja.

- Valtorin ja Suomen Erillisverkot Oy:n hankkimien vaatimustenmukaisuuden arviointien määrät ovat arviointilakien voimassaolon aikana lisääntyneet. Kasvu johtuu palveluiden kehittämistoimista, uusista palveluista sekä EU- ja Nato -tiedon käsittelytarpeesta. Valtori on vuoden 2021 elokuun ja vuoden 2024 välisenä aikana teettänyt yhteensä 73 arviointia, joista 40 on kohdistunut turvallisuusverkon palveluihin ja 33 valtion yhteisiin tieto- ja viestintäteknisiin palveluihin. Suomen Erillisverkot Oy:ssä on toteutettu noin 20 itsearviointia vuodessa ja se on teettänyt tietoturvallisuuden arviointilaitoksilla useita arviointeja vuodessa.

- Sosiaali- ja terveydenhuollon julkisten ja yksityisten organisaatioiden hyväksytyiltä arviointilaitoksilta hankkimien lakisääteisten tietoturvallisuuden arviointien määrä on ollut lievässä kasvussa vuodesta 2021 lähtien. Kasvu johtuu arviointivelvoitteen piiriin kuuluvien tietojärjestelmien määrän kasvusta. Tällä hetkellä näitä Valviran rekisteriin merkittyjä tietojärjestelmiä ja käyttöympäristöjä on 99. Vuonna 2023 Valviran rekisteriin merkittiin 27 todistusta tietoturvallisuuden arvioinneista.

- Kattavaa kuvaa tietoturvallisuuden arviointilaitosten kunnissa tekemistä tietoturvallisuuden arvioinneista ei ole saatavilla. Kuntaliiton arvion mukaan kunnissa ei laajamittaisesti toteuteta arviointilaitosten tai Liikenne- ja viestintäviraston tietojärjestelmien tietoturvallisuuden arviointeja. Suurimmissa kaupungeissa toteutetaan riskiperustaisesti valikoitujen tietojärjestelmien tietoturvallisuuden itsearviointeja, usein yksityisten palveluntarjoajien tukemana. Pienemmissä kunnissa ja kuntayhtymissä tietojärjestelmien tietoturvallisuuden itsearviointeja toteutetaan tapauskohtaisesti.

- Arviointilaitosten toteuttamien arviointien määrästä ei ole saatavilla julkisia tietoja.

Arviointitarpeiden kasvu johtuu toimintaympäristön muutoksista, jotka ovat kasvattaneet tarvetta nostaa viranomaisten tietojärjestelmien turvallisuuden tasoa. Näitä muutoksia ovat teknologioiden ja tiedonhallinnan rooli geopoliittisessa kilpailussa, yhä kehittyneemmät uhkat, verkottuneemmat järjestelmät ja monimutkaisemmat logistiset toimitusketjut. Arvioinnilla

pystytään osaltaan tukemaan kehittyvien tietoturvallisuustoimenpiteiden ja esimerkiksi riittävän salauksen käyttöä osana tiedon suojaamista ja jatkuvuudenhallintaa. Tieto- ja viestintäteknisten järjestelmien käytön lisääntyminen ja turvallisuustarpeet ovat nostaneet järjestelmien kustannuksia suhteessa muuhun viranomaistoiminnan kulurakenteeseen.

Tietoturvallisuuden arviointien kustannuksista on kerätty tietoja Suomen Erillisverkot Oy:stä, Valtorista ja ministeriöistä[1]. Suomen Erillisverkot Oy:ssä on toteutettu noin 20 itsearviointia vuodessa, ja niiden vaatima vuosittainen henkilötyömäärä on ollut noin 300 henkilötyöpäivää ja kustannukset noin 210 000 euroa. Itsearviointien kustannukset ovat siten olleet keskimäärin noin 10 500 euroa/arviointi. Suomen Erillisverkot Oy:n tietoturvallisuuden arviointilaitoksilla teettämien arviointien kustannukset, sekä sisäiset että ulkoiset, ovat olleet noin 57 000 euroa/arviointi. Viranomaisten hakemien tietoturvallisuuden arviointien hinta on keskimäärin ollut yhteensä 60 000–70 000 euroa/arviointi, joista pääsääntöisesti arviointilaitoksilta hankitun ulkoisen arvioinnin osuus on ollut keskimäärin 30 000–40 000 euroa. Esimerkiksi Liikenne- ja viestintäministeriön hallinnonalalla on vuosittain hankittu noin 220–230 henkilötyöpäivää arviointilakien mukaisia arviointipalveluja. Palvelujen hankintakustannusten arvioidaan olevan vuositasolla noin 300 000 euroa. Muilta tietoturvapalveluja tarjoavilta yrityksiltä on hankittu vuosittain noin 720–750 henkilötyöpäivää arviointeihin liittyviä palveluja. Kustannusten arvioidaan olevan vuositasolla noin 650 000 euroa. Arviointilakien mukaiset arvioinnit ovat siten olleet henkilötyöpäivinä noin 20 % ja euromääräisesti noin 30 % kaikista tietoturvallisuuden arvioinneista liikenne- ja viestintäministeriön hallinnonalalla.[1] Arviointien kustannuksiin vaikuttavat arvioinnissa käytetty kriteeristö sekä maksuperustelain tai arvioinnin suorittamisen kilpailutuksen perusteella määräytyvä päivähinta.

Liikenne- ja viestintäviraston tehtävät

Tietojärjestelmien tietoturvallisuuden arviointeihin ja hyväksyntöihin liittyvistä Liikenne- ja viestintäviraston tehtävistä säädetään kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa, turvallisuusselvityslaissa (706/2014) ja arviointilaissa. Arviointilain 3 § mukaan Liikenne- ja viestintävirasto on nykytilassa ainoa viranomainen, joka toteuttaa arviointilain mukaisia viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arviointeja.

Liikenne- ja viestintävirasto antaa turvallisuusluokitellun tiedon tietoturvallisuuden arviointiin liittyvää neuvontaa. Neuvontatehtävästä ei kuitenkaan ole säädetty arviointilaissa, vaikka kyseessä on hallintolain (434/2003) 8 §:ssä säädettyä maksutonta viranomaisneuvontaa laajempi neuvontatehtävä, joka liittyy arvioinnin suunnittelun ja toteuttamisen eri vaiheisiin. Neuvonnan maksullisuudesta on säädetty Liikenne ja viestintäviraston sähköiseen viestintään liittyvistä suoritteista perittävistä maksuista annetussa liikenne- ja viestintäministeriön asetuksessa (1190/2023).

Arviointilain 4 §:n 3 momentin mukaan Liikenne- ja viestintävirasto suorittaa tehtävänsä käytettävissään olevien voimavarojen mukaisesti ottaen huomioon kansainvälisten tietoturvallisuusvelvoitteiden noudattamisen sekä pyydettyjen toimenpiteiden merkityksen viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden yleiseen parantamiseen. Nykytilassa Liikenne- ja viestintävirasto priorisoi viranomaisten kansainvälisiin tietoturvallisuusvelvoitteisiin liittyviä arviointipyyntöjä ja yritysturvallisuusselvityksiin liittyviä turvallisuusselvityslain mukaisia Suojelupoliisin tai Puolustusvoimien Pääesikunnan pyyntöjä sekä

[1] Tietojärjestelmien tietoturvallisuuden ja varautumisen vaatimustenmukaisuuden arvioinnin nykytila-arvio ja kehittämisehdotukset 12.12.2024 -raportti, valtiovarainministeriö.

tarvittaessa kansallisen turvallisuusluokkaan I ja II luokiteltuja tietoja käsittelevien tietojärjestelmien arviointiin liittyviä pyyntöjä, joihin ei ole saatavilla hyväksytyn tietoturvallisuuden arviointilaitoksen arviointeja. Virasto ei nykytilassa juurikaan pysty toteuttamaan muita kuin turvallisuusselvityslain edellyttämiä kansallisen turvallisuusluokkaan III tai IV luokitellun tiedon käsittelyn arviointeja resurssien priorisointitarpeen vuoksi.

Tietoturvallisuuden arviointilaitokset

Arviointilaitoslaissa säädetään julkista hallintotehtävää hoitavien tietoturvallisuuden arviointilaitosten ja niiden pätevyyksien hyväksynnän edellytyksistä ja menettelystä, arviointilaitostoiminnan valvonnasta sekä arviointilaitosten toiminnan vaatimuksista. Tietoturvallisuuden arviointilaitoksilla on merkittävä rooli tietoturvallisuuden arviointipalvelujen tuottajina. Arviointilaitoslailla on pyritty edistämään viranomaisten ja yritysten tietoturvallisuutta luomalla järjestely, jossa Liikenne- ja viestintävirasto hyväksyy hakemuksesta tietoturvallisuuden arviointilaitokset ja niiden pätevyysalueet sekä valvoo niiden toimintaa.

Arviointilaitoslain 1 §:n mukaan lain tarkoitus on säätää menettelystä, jonka avulla yritykset voivat osoittaa luotettavasti ulkopuolisille, että niiden toiminnassa on toteutettu määrätty tietoturvallisuuden taso. Tämän toteuttamiseksi arviointilaitos arvioi lain 9 §:n mukaan huolellisesti arvioinnin kohteen tietojärjestelmien ja tietoliikennejärjestelyjen sekä toimitilojen tietoturvallisuutta suhteessa ennalta määriteltyihin tietoturvallisuusvaatimuksiin. Laissa ei kuitenkaan säädetä siitä, mitkä tahot arviointeja voivat hyväksytyiltä arviointilaitoksilta hankkia. Siten ei ole estettä sille, että viranomainen hankkii arvioinnin arviointilaitokselta ja arviointilain 3 §:n mukaankin valtionhallinnon viranomaisen yhtenä arviointimenettelyvaihtoehtona on hyväksytty tietoturvallisuuden arviointilaitos.

Arviointilaitoslain 3 §:n mukaan arviointilaitos voi hakea Liikenne- ja viestintäviraston hyväksyntää. Hyväksynnän edellytyksistä ja hakemuksen käsittelystä säädetään lain 4 ja 5 §:ssä. Arviointilaitoslain 5 §:n 1 momentin 1–3 kohtien mukaan tietoturvallisuuden arviointilaitoksen hyväksymisen edellytyksenä on, että 1) laitos on toiminnallisesti ja taloudellisesti riippumaton arvioinnin kohteesta; 2) laitoksen henkilökunnalla on hyvä tekninen ja ammatillinen koulutus sekä riittävän laaja-alainen kokemus toimintaan kuuluvissa tehtävissä; 3) laitoksella on toiminnan edellyttämät laitteet, välineet ja järjestelmät. Laissa säädetään vain yksi mahdollinen menettely näiden riippumattomuus- ja pätevyysvaatimusten selvittämiselle ja hyväksymiselle. Lain 5 §:n 2 momentin nojalla riippumattomuus- ja pätevyysvaatimusten täyttäminen on osoitettava vaatimustenmukaisuuden arviointipalvelujen pätevyyden toteamisesta annetussa laissa (920/2005) säädetyn menettelyn avulla eli kansallisen akkreditointielimen FINAS-akkreditointipalvelun akkreditoinnilla. Liikenne- ja viestintäviraston hyväksyntäpäätös perustuu näiltä osin akkreditointitodistukseen. FINAS seuraa pätevyyttä pääsääntöisesti kerran vuodessa tehtävillä määräaikaisarvioinneilla, jotka kohdistetaan eri kerroilla toiminnan eri osa-alueisiin. Koko akkreditointi tulee uusia neljän vuoden välein. Tietoturvallisuuden arviointilaitoksen pätevyyden akkreditointiin sisältyy yleensä näyttöarviointi, jonka avulla FINASin käyttämä asiantuntija arvioi arviointilaitoksen arviointipätevyyden riittävyyttä. Turvallisuusluokitellun tiedon käsittelyn arvioinnin pätevyyksissä FINASin asiantuntijana on toiminut käytännössä Liikenne- ja viestintäviraston tietoturvallisuusasiantuntija.

Akkreditointimenettely perustuu Euroopan unionin sääntelymalliin, jota sovelletaan vaatimustenmukaisuuden arviointilaitosten tai ilmoitettujen laitosten pätevyyden osoittamiseen useissa EU-säädöksissä. Niissä voi kuitenkin olla vaihtoehtoisena menettelynä myös se, että toimivaltainen viranomainen hyväksyy pätevyyden selvityksen perusteella. Esimerkiksi laissa eräitä tuoteryhmiä koskevista ilmoitetuista laitoksista (278/2016) säädetään, että jos arviointilaitos ei voi toimittaa akkreditointitodistusta, sen on toimitettava viranomaiselle tarpeelliset

asiakirjatodisteet, joiden avulla viranomainen voi arvioida hakijan täyttävän unionin yhdenmukaistamislainsäädäntöön perustuvat ilmoitetuksi laitokseksi hyväksymistä koskevat vaatimukset.

Pätevyyden akkreditoinnin lisäksi arviointilaitoksen hyväksyntä edellyttää arviointilaitoslain 5 §:n 1 momentin 4–5 kohtien mukaan, että vastuuhenkilöiden luotettavuus ja tietojenkäsittelyn ja toimitilojen turvallisuus on varmistettu ja että laitoksella on asianmukaiset ohjeet toimintaansa ja sen seurantaa varten. Tietojenkäsittelyn turvallisuuden Liikenne- ja viestintävirasto selvittää tarkastuksella. Lisäksi virasto tarkistaa 5 §:n 1 momentin 5 kohdassa edellytettyjen ohjeiden asianmukaisuuden. Toimitilojen turvallisuuden varmistaa joko Suojelupoliisi tai Liikenne- ja viestintävirasto. Viraston on arviointilaitoslain 4 §:n mukaan ennen tietoturvallisuuden arviointilaitoksen hyväksymistä varattava Suojelupoliisille tilaisuus lausua arviointilaitoksen vastuuhenkilöiden luotettavuudesta ja sen toimitilojen turvallisuudesta. Vastuuhenkilöistä Suojelupoliisi tekee henkilöturvallisuusselvityksen Liikenne- ja viestintäviraston hakemuksesta.

Tietoturvallisuuden arviointilaitokseksi pääsy ja pätevyyksien hyväksyntä on koettu hankalaksi ja se on voinut kestää kauan. Turvallisuusluokitellun tiedon käsittelyn pätevyyksien hyväksynnässä Liikenne- ja viestintäviraston asiantuntemukselle on tarve myös akkreditoinnissa. Voimassa olevan arviointilaitoslain menettelyissä yrityksen luotettavuuden varmistamisessa ei hyödynnetä turvallisuusselvityslain yritysturvallisuusselvityksen menettelyjä kuin osittain. Laissa ei säädetä tietoturvallisuuden arviointilaitokseksi hakeutuvan yrityksen sijaintivaltiosta. Arviointilaitoksen henkilökunnan luotettavuudesta ei säädetä ja tietoturvallisuuden arviointilaitoksen mahdollisuus hankkia henkilöturvallisuusselvitys työntekijöistä on ollut tulkinnanvarainen tai se ei ole ollut mahdollista, jolloin jokainen arviointilaitoksen viranomaisasiakas on joutunut hankkimaan turvallisuusselvityksen tietojärjestelmiään tai tietoliikennejärjestelyjään arvioivista arviointilaitoksen työntekijöistä.

Arviointilaitoslain mukaisesti Liikenne- ja viestintäviraston hyväksymiä tietoturvallisuuden arviointilaitoksia on neljä. Kaikilla tietoturvallisuuden arviointilaitoksilla on hyväksytty pätevyys tehdä ISO/IEC 27001 standardin mukaisia tietoturvallisuuden johtamisjärjestelmän arviointeja, mutta näiden arviointien kysyntä ei ole ollut suurta. Kolmella tietoturvallisuuden arviointilaitoksella on lisäksi pätevyys tehdä turvallisuusluokkaan IV ja III luokitellun tiedon käsittelyn arviointeja kansallisen turvallisuusauditointikriteeristön (Katakri) mukaisesti.

Arviointilaitosten Katakri-pätevyyksien hyväksyntöjen aikatauluun ovat vaikuttaneet se, milloin arviointilaitokset ovat hakeneet pätevyyttä ja kehittäneet kyvykkyytensä ja menettelynsä tarvittavalle tasolle, pakollisen FINAS-akkreditoinnin ja siinä tarvittavien asiantuntijoiden järjestäminen ja Liikenne- ja viestintäviraston vastuulle kuuluvien selvitysten ja tarkastusten tekeminen. Pätevyyksien hyväksyminen on puolestaan vaikuttanut arviointien saatavuuteen ja arviointeja hankkivien viranomaisten ja yritysten mahdollisuuteen kilpailuttaa arviointeja. Katakrin edellisen 2015 version mukaiset pätevyydet akkreditoitiin ja hyväksyttiin vuosina 2016–2019 Nixu Certification Oy:lle ja KPMG IT Sertifiointi Oy:lle. Katakri 2020 -pätevyydet turvallisuusluokissa III ja IV hyväksyttiin heinäkuussa 2021 Nixu Certification Oy:lle ja kesäkuussa 2022 KPMG IT Sertifiointi Oy:lle. Vuosina 2021–2022 oli siten lähes vuoden ajanjakso, jona ajantasaisen pätevyyden mukainen arviointi oli saatavilla vain yhdeltä arviointilaitokselta ja tilanteen voidaan arvioida heijastuneen paitsi saatavuuteen myös hinnoitteluun. Kolmannen arviointilaitoksen, Into Certification Oy:n, Katakri 2020 -pätevyyden akkreditointi ja hyväksyntä on tehty alkuvuonna 2025.

Viranomaisilla on ollut käytettävissä tietoturvallisuuden arviointipalvelujen hankintaa varten Hansel Oy:n Tietoturvallisuuden arviointilaitosten arviointipalvelut 2021–2028 dynaaminen

hankintajärjestely, johon hyväksytyillä sopimustoimittajilla tulee olla arviointilaitoslain mukainen Liikenne- ja viestintäviraston hyväksyntä tietoturvallisuuden arviointilaitokseksi. Viranomaisten pitkäkestoisten hankintasopimusten takia kolmannen tarjoajan vaikutuksia arviointien tarjontaan ja hintoihin ei vielä ole mahdollista todeta.

Arviointeja hankkivien viranomaisten näkemyksen ja kokemuksen mukaan hyväksytyillä tietoturvallisuuden arviointilaitoksilla on ollut niin runsaasti kysyntää arvioinneille, että ne eivät ole pystyneet tarjoamaan arviointipalveluja kysyntää vastaavasti. Valtorin palvelujen ja niihin liitettyjen tieto- ja viestintäteknisten palvelujen arvioinneissa on tarvittu Valtorin henkilöstön tukea, jolloin myös Valtorissa käytettävissä olevat henkilöresurssit ovat vaikuttaneet arviointien toteutusaikatauluihin. Tietoturvallisuuden arviointilaitokset ovat palautteessaan tuoneet esille, että henkilöiden rekrytointi julkisen hallinnon turvallisuusluokiteltujen tietojen käsittelyn tietoturvallisuuden arviointitehtäviin on haastavaa. Suomessa on rajallisesti teknisesti tarpeeksi kyvykkäitä henkilöitä. Työtä ei myöskään pääsääntöisesti voi tehdä etätyönä, mikä laskee sen houkuttelevuutta. Edellä kuvattujen tietoturvallisuuden arviointien toteuttamisen haasteiden johdosta on tarve parantaa arviointien saatavuutta.

Käytännön toiminnassa on lisäksi tunnistettu tarve tarkentaa arviointilaitoksia koskevaa lainsäädäntöä esimerkiksi arviointiin liittyvien menettelytapojen, ohjauksen ja tiedonsaantioikeuksien osalta. Arviointilaitoslain 9 §:n 2 momentissa säädetään todistuksen antamisesta, jos arvioitavan kohteen toimitilat ja toiminta on selvityksen perustana olleiden arviointiperusteiden mukainen. Todistuksessa tulee yksilöidä arvioinnissa käytetyt tietoturvallisuuden arviointiperusteet ja arvioinnin laajuus. Arviointiraportista ei säädetä erikseen, mutta arviointitoiminnan käytäntöihin ja akkreditoituun pätevyyteen kuuluu asianmukainen dokumentointi. Asiakastietolaissa ja toisiolaissa säädetään velvollisuudesta hankkia tietyille toiminnoille hyväksytyn tietoturvallisuuden arviointilaitoksen todistus. Näissä laeissa säädetään myös todistuksen voimassaolosta, ylläpidosta ja peruuttamisesta.

Arviointilaitoslain 13 §:ssä säädetään hyvää hallintoa koskevien säännösten soveltamisesta tietoturvallisuuden arviointilaitosten toiminnassa. Pykälässä ei kuitenkaan säädetä tietoturvallisuuden arviointilaitosten henkilöstön toimimisesta virkavastuulla. Arviointilaitoslaissa ei myöskään säädetä arviointiin liittyvien tehtävien alihankintana teettämisen reunaehdoista.

Arviointilaitoslaissa, asiakastietolaissa tai toisiolaissa ei säädetä ohjaus- tai valvontatoimivallan jakautumisesta Liikenne- ja viestintäviraston ja sosiaali- ja terveysalan viranomaisten, Terveyden ja hyvinvoinnin laitoksen (THL), Sosiaali- ja terveysalan lupa- ja valvontaviraston (Valvira), Sosiaali- ja terveysalan tietolupaviranomaisen (Findatan) ja Kansaneläkelaitoksen (Kela) välillä, kun arviointilaitos suorittaa arvioinnin sosiaali- ja terveysalan viranomaisten määräysten perusteella. Viranomaiset tekevät asiassa tarpeen mukaan yhteistyötä hallintolain 10 §:n yleisen yhteistyösäännöksen mukaisesti. Arviointilaitoslaissa säädetään Liikenne- ja viestintäviraston oikeudesta saada arviointilaitoksilta ne tiedot, jotka ovat tarpeen sen valvomiseksi, että laitos täyttää toimintaansa koskevat vaatimukset. Tiedonsaantioikeutta ei ole säädetty salassapitosäännösten estämättä eikä tiedonsaantioikeus koske muilta viranomaisilta tai arviointilaitoksen arvioinnin kohteilta pyydettäviä tietoja, jotka olisivat välttämättömiä sen valvomiseksi, että laitos täyttää toimintaansa koskevat vaatimukset.

Puolustusvoimien tehtävät

Puolustusvoimien tietoturvallisuuden arviointien tarve ja määrä on viime vuosina ollut kasvussa. Puolustusvoimien suuresta arviointitarpeesta huolimatta puolustushallintoon ei ole nykytilassa säädetty erikseen toimivaltaa arvioida ja hyväksyä tietojärjestelmiä ja salaustuotteita. Kansallisen turvallisuusluokitellun tiedon osalta arviointitoiminta perustuu tiedonhallintalaissa

ja turvallisuusluokitteluasetuksessa säädettyihin tiedonhallintayksikön ja valtionhallinnon viranomaisen velvoitteisiin huolehtia tietoaineistojen ja tietojärjestelmien tietoturvallisuudesta ja vaatimuksista. Puolustusvoimissa on sisäiset menettelyt ja kyvykkyydet arvioida sen omia tietojärjestelmiä ja salaustuotteita. Arviointi- ja hyväksyntätehtävät jakautuvat Puolustusvoimissa eri toimijoille, eikä arviointitoimintaa ole tällä hetkellä järjestetty riippumattomaksi ja itsenäiseksi toiminnoksi. Puolustusvoimien nykyiset arviointi- ja hyväksyntäresurssit on mitoitettu kansallisten järjestelmien tietoturvavaatimusten perusteella keskittyen ylimpiin turvallisuusluokkiin. Nato-jäsenyyden ja lisääntyneen harjoitustoiminnan takia Pääesikunta on sopinut Liikenne- ja viestintäviraston kanssa kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 5 §:n perusteella joidenkin arviointitehtävien hoitamisesta. Pääesikunta on myös sopinut Liikenne- ja viestintäviraston kanssa tiettyjen salausteknisen materiaalin jakeluun ja hallintaan liittyvistä tehtävistä, joihin Puolustusvoimilla on toimivat menettelyt.

Salaustuotteiden ja muiden turvallisuuskriittisten ratkaisujen arviointi

EU:n ja Naton turvallisuussäännöissä on vaatimuksia ja velvoitteita salausratkaisujen ja hajasäteilysuojauksen (TEMPEST) arvioinnille sekä eräiden muiden turvallisuuskriittisten tuotteiden arviointiin. Myös valtioiden kahden- tai monenvälisissä tietoturvallisuussopimuksissa valtioiden välisissä sähköisissä tiedonsiirtoyhteyksissä salausratkaisuista sopiminen on keskeinen sopimusmääräys ja -käytäntö.

Liikenne- ja viestintävirasto tekee tuotearviointeja ja -hyväksyntöjä kansainvälisten tietoturvallisuusvelvoitteiden mukaisesti. Tuotearvioinnit kohdistuvat salaustuotteisiin tai muihin turvallisuuskriittisiin tuotteisiin. Ne perustuvat Liikenne- ja viestintäviraston kansainvälisistä tietoturvallisuusvelvoitteista annetun lain mukaiseen tehtävään toimia kansallisen turvallisuusviranomaisen asiantuntijana tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuutta koskevissa asioissa. Salaustuotteilla varmistetaan tiedon luottamuksellisuus ja eheys erilaisilla salausmekanismeilla. Salaustuotteita ovat esimerkiksi VPN-tuotteet ja kiintolevyn tai massamuistin salausratkaisut. Salaustarpeet voivat liittyä esimerkiksi puheen ja tietoliikenteen salaamiseen langallisilla tai langattomilla yhteyksillä. Turvallisuuskriittiset tuotteet ovat muutoin tietojärjestelmien turvallisuuden kannalta keskeisiä komponentteja, kuten yhdyskäytävätuotteita tai tiedon tuhoamiseen käytettäviä ylikirjoitustuotteita.

Kansallisen turvallisuusluokitellun tiedon suojaamisessa ei ole säädetty salausratkaisuille tai muille turvallisuuskriittisille tuotteille ja ratkaisuille arviointi- tai hyväksyntävelvollisuutta, joten Liikenne- ja viestintävirasto tekee niiden arviointeja viranomaisen pyynnöstä arviointilain nojalla osana viranomaisen tietojärjestelmää tai tietoliikennejärjestelyä. Viranomaisten pyytämiä järjestelmäkohtaisia arviointeja ei julkaista.

Liikenne- ja viestintävirastolle ei ole arviointilaissa säädetty tehtävää tehdä tuotearviointeja valmistajien pyynnöstä, eivätkä turvallisuuskriittisiä ratkaisuja tarjoavat yritykset tai valmistajat voi itsenäisesti tehdä arviointilain mukaisia arviointipyyntöjä. Voimassa olevassa lainsäädännössä ei siten säädetä myöskään siitä millä edellytyksillä valmistaja voi saada turvallisuuskriittisten ratkaisunsa toimivaltaisen viranomaisen arvioitavaksi tai millä edellytyksillä yritys voi saada tuotteelleen viranomaisen hyväksynnän.

Viranomaisten tarpeiden tukemiseksi Liikenne- ja viestintävirasto kuitenkin tekee jonkin verran tuotekohtaisia arviointeja suomalaisten valmistajien tuotteille myös sopimusperusteisesti ja laatii näistä arvioinneista lausuntoja. Sopimusmalli perustuu Liikenne- ja viestintävirastosta annetussa laissa Kyberturvallisuuskeskukselle säädettyyn sopimusvaltuuteen ja sopimusperusteinen arviointi edellyttää virastolle säädettyjen tehtävien takia aina jonkin viranomaisen tarvetta. Sopimusperusteisesti Liikenne- ja viestintävirasto tekee arviointeja vain suomalaisten valmistajien

Suomessa valmistamille tuotteille ja arviointien tarkoitus on pystyä varmistumaan tuotteen luotettavuudesta siinä määrin, että Liikenne- ja viestintävirasto voi julkaista tiedon. Viraston verkkosivuilla julkaistulla listalla on tällä hetkellä kymmenkunta arvioitua salaustuotetta ja viitisen muuta arvioitua tuotetta. Uusia arviointeja tai tuotepäivitysten arviointeja on yleensä samanaikaisesti käynnissä alle kymmenen.

Tiedonvaihto, yhteistyö ja avustavat tehtävät

Arviointilaissa ei nykytilassa säädetä viranomaisten yhteistyöstä. Liikenne- ja viestintävirasto on tarvittaessa tehnyt yhteistyötä muiden viranomaisten kanssa hallintolain 10 §:n nojalla. Turvallisuusselvityslain ja kansainvälisistä tietoturvallisuusvelvoitteista annetun lain mukaisesti toteutettujen arviointien osalta säädetään Liikenne- ja viestintäviraston tehtävien lisäksi suojelupoliisin ja Puolustusvoimien Pääesikunnan tehtävistä. Näissä laeissa säädetään myös toimivaltaisten viranomaisten tiedonvaihto- ja yhteistyövelvoitteista sekä mahdollisuudesta sopia tietyn toiselle kuuluvan tehtävän hoitamisesta.

Arviointilain tiedonsaantioikeuksia sekä tilojen ja tietojärjestelmien pääsyoikeuksia koskevan 6 §:n mukaan oikeudet koskevat sekä virastoa että sen toimeksiannosta toimivaa asiantuntijaa. Arviointilaissa ei kuitenkaan ole säädetty Liikenne- ja viestintäviraston mahdollisuudesta käyttää arviointitehtävässä avustavia yksityisiä luonnollisia tai oikeushenkilöitä. Virasto ei ole tehnyt toimeksiantoja yksityisille tahoille, eikä voimassa olevan arviointilain voi katsoa täyttävän edellytyksiä julkisen hallintotehtävän antamisesta muille kuin viranomaiselle. Arviointiviranomaisten toteuttamissa arvioinneissa on kuitenkin tunnistettu tarve mahdollistaa yksityisiltä markkinoilta hankittu henkilötyövoiman käyttö avustavassa roolissa.

Arviointiperusteet ja -kriteerit

Arviointilain 7 §:ssä ja arviointilaitoslain 10 §:ssä säädetään arviointiperusteista, joita Liikenne- ja viestintävirasto tai hyväksytty tietoturvallisuuden arviointilaitos voi käyttää viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arviointiperusteina. Arviointiperusteiden luettelo mahdollistaa laajasti eri säädösten, ohjeiden ja standardien käyttämisen arviointiperusteina. Arviointilaissa ei säädetä millä perusteella tai kenen toimesta arvioinnissa käytettävät arviointiperusteet valitaan. Arviointilaitoslain 10 §:n mukaan arvioinnin kohde valitsee arviointiperusteet, mutta arviointilaitoksen hyväksytyt pätevyydet vaikuttavat siihen, mitä arviointeja arviointilaitos voi tehdä.

Nykytilassa käytetyt arviointiperusteet ja kriteerit voivat perustua kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa tarkoitetun kansallisen turvallisuusviranomaisen (NSA) antamiin kansainvälisten tietoturvallisuusvelvoitteiden toteuttamista koskeviin ohjeisiin, eli käytännössä kansalliseen turvallisuusauditointikriteeristöön (Katakri), jota kansallisen turvallisuusviranomaisen antaman ohjeen mukaisesti sovelletaan kansainvälisten tietoturvallisuusvelvoitteiden hoitamisessa. Katakrissa on huomioitu EU:n ja Naton turvallisuusluokitellun tiedon käsittelyn vaatimukset sekä tiedonhallintalain ja turvallisuusluokitteluasetuksen vaatimukset, joten sitä voidaan hyödyntää monissa tilanteissa. Katakria käytetään etenkin kansainvälisiin velvoitteisiin liittyvissä arvioinneissa, mutta myös monissa kansallisissa tilanteissa, kuten lain julkisen hallinnon turvallisuusverkkotoiminnasta (10/2015) mukaisten palveluiden arvioinneissa ja yritysturvallisuusselvityksiin liittyvissä arvioinneissa. EU:n ja Naton turvallisuusluokitellun tiedon suojaamisen arvioinnissa laaditaan nykykäytännössä järjestelmäkohtaiset turvallisuusvaatimusmäärittelyt, joissa käytetään apuna soveltuvin osin turvallisuussääntöjä ja Katakria.

Arviointilaitoslain säännös arviointiperusteista on samansisältöinen arviointilain kanssa. Arviointilaitoslain nojalla arviointiperusteena on käytetty myös vahvistettua kansainvälistä

standardia eli ISO/IEC 27001-standardia. Asiakastietolain ja toisiolain edellyttämissä arvioinneissa on käytettävä arviointiperusteena Terveyden- ja hyvinvoinnin laitoksen ja Sosiaali- ja terveysalan tietolupaviranomaisen määräyksiä.

Arviointikriteerien määrittämisessä hyödynnetään myös tiedonhallintalautakunnan suositusta julkisen hallinnon tietoturvallisuuden arviointikriteeristöstä (Julkri). Julkrin suunnittelun lähtökohtana oli arviointikriteeristön asettaminen käyttötapauskohtaisesti riskiperusteisesti. Julkri sisältää Katakrin kriteeristön lukuun ottamatta EU:n ja Naton turvallisuusluokitellun tiedon suojaamisen vaatimuksia. Julkriin on kerätty myös julkisten ja salassa pidettävien tietojen, joitakin turvallisuusluokkaa I olevien tietojen sekä tietojen eheyden ja saatavuuden ja jatkuvuudenhallinnan (varautumisen) arviointikriteerejä. Sitä voidaan käyttää apuna arvioitaessa tiedonhallintalaissa, turvallisuusluokitteluasetuksessa sekä osin myös tietosuoja-asetuksessa säädettyjen tietoturvallisuutta koskevien vaatimusten täyttymistä.

Julkria ei ole voinut hyödyntää arviointilaitoslain mukaisissa tietojärjestelmien tietoturvallisuuden arvioinneissa, sillä Julkri-pätevyyksiä ei ole haettu, akkreditoitu ja myönnetty arviointilaitoslain mukaisesti hyväksytyille tietoturvallisuuden arviointilaitoksille, koska Julkrin soveltamisen osaamisvaatimuksia ei ole vielä määritelty. Sekä tiedonhallintalain vaatimukset että arviointikriteeristöt kuten Katakri koetaan tulkinnanvaraisiksi. Arviointikriteeristöjen tulkinnanvaraisuutta voi vähentää soveltamisesimerkeillä, mutta tietotekniikan luonteen ja toteutusten monimuotoisuuden ja joustavuuden takia tulkinnanvaraa on väistämättä. Käytännössä on välttämätöntä, että pätevyysalueen arviointiperustasta on olemassa konkreettiset työohjeet ja ennalta määritelty perusteiden soveltamistapa, jotta arviointitoiminta on tasapuolista ja tasalaatuista. Julkri-kriteeristön osalta on haasteena ollut se, mikä taho määrittelisi kriteerien mukaisen riittävän käytännön ja sen, millaisilla menetelmillä arvioijan tulisi todentaa kriteerien toteutuminen julkisen, salassa pidettävän tai turvallisuusluokitellun tiedon käsittelyssä tai varautumistoimenpiteiden arvioinnissa. Tämän tahon tai näiden tahojen edustajan tulisi myös pystyä toimimaan FINASin asiantuntijana, jos jokin yritys haluaisi hakea arviointilaitoslain mukaisesti hyväksytyn arviointilaitoksen pätevyyttä kriteeristöön. Julkrin tietosuojakriteerien osalta toimivaltainen viranomainen on tietosuojavaltuutettu. Edellä kuvatuista syistä Julkria ei ole toimeenpantu arviointilaitosten pätevöitymisalueeksi, vaikka se täyttää kriteeristönä arviointilaitoslain 10 §:n edellytykset.

Arviointiperusteina on aikaisemmin myös käytetty valtionhallinnon tietoturvallisuudesta annettua valtioneuvoston asetusta (681/2010) ja valtiovarainministeriön sen täytäntöönpanosta antamia ohjeita (Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta, VAHTI), mutta asetus on kumottu ja ohjeet ovat vanhentuneet. Asetuksen on korvannut tiedonhallintalaki ja sen perusteella annettu turvallisuusluokitteluasetus.

Varautumisen arviointiin ei ole käytössä vakiintuneita yleispäteviä perusteita. Edellä mainituista Julkri-kriteeristön varautumisen ja jatkuvuuden hallinnan (VAR) perusteet eivät ole siinä määrin vakiintuneet, että niistä olisi laajaa soveltamiskäytäntöä.

Todistus vaatimusten täyttymisestä

Arviointilain 8 § mukaan Liikenne- ja viestintävirasto voi pyydettäessä antaa todistuksen tietoturvallisuutta koskevat vaatimukset täyttävästä tietojärjestelmästä tai tietoliikennejärjestelystä. Todistukseen liittyy myös arviointilain 9 §:ssä säädetty tietoturvallisuuden tason ylläpito- ja seurantavelvollisuus, jonka mukaisesti todistuksen saajan on sitouduttava tietoturvallisuustason säilyttämiseen ja ilmoitettava Liikenne- ja viestintävirastolle muutoksista, joilla on vaikutusta tietoturvallisuustasoon. Arviointilain 10 §:ssä säädetään todistuksen peruuttamisesta.

Arviointilain 8 a §:ssä säädetään mahdollisuudesta säätää valtioneuvoston asetuksella velvollisuudesta hankkia todistus valtionhallinnon viranomaisen määräysvallassa olevasta tietojärjestelmästä tai tietoliikennejärjestelystä, jossa käsitellään turvallisuusluokkaan I tai II kuuluviksi luokiteltuja asiakirjoja. Tätä asetuksenantovaltuutta ei ole käytetty, joten Liikenne- ja viestintäviraston arvioinnin tai todistuksen pyytäminen kansallisen turvallisuusluokitellun tiedon käsittelyssä on vapaaehtoista. Arviointilain 8 § mukaisesti pyydetyt Liikenne- ja viestintäviraston antamat todistukset ovat koskeneet kansallisesti turvallisuusluokiteltuja tietoja käsitteleviä tietojärjestelmiä ja todistuksia on pyydetty ja annettu erittäin harvoin. Todistus liittyy vaatimustenmukaisuuteen, mikä tarkoittaa arviointiprosessin kannalta sitä, että arviointia on jatkettava, kunnes arvioinnissa havaitut poikkeamat on korjattu. Jos arviointiprosessissa on tarpeen selvittää tietoturvallisuuden taso, arviointiraporttiin ja arvioinnin kohteeseen voi jäädä poikkeamia, joiden käsittelystä järjestelmän haltija päättää.

Todistuksen luonteinen päätös tai lausunto voidaan kuitenkin antaa kansainvälisistä tietoturvallisuusvelvoitteista annetun lain tarkoittamissa tilanteissa tai muutoin kansainvälisten velvoitteiden sitä edellyttäessä. EU:n ja Naton tietoturvallisuusvelvoitteiden mukaisista arvioinneista turvallisuussäännöissä edellytetty hyväksyntälausunto on arviointilain menettelyn valossa todistuksen luonteinen. Tällöin viranomaisen oman riskiarvion liikkumavara käyttöönottopäätöksissä on rajoitetumpi kuin kansallisen turvallisuusluokitellun tiedon suojaamisessa, jossa vastuu tietojärjestelmien riittävästä suojaamisesta, riskienhallinnasta ja käyttöönottopäätöksistä on tiedonhallintalain 13 §:n mukaisesti kullakin viranomaisella.

Turvallisuusselvityslain mukaisissa yritysturvallisuusselvityksissä Liikenne- ja viestintävirasto tekee suojelupoliisin tai Pääesikunnan pyynnöstä selvityksen tietojärjestelmän tietoturvallisuudesta. Tämäkin selvitys on todistuksen luonteinen sinä mielessä, että selvitys annetaan vain vaatimukset täyttävästä järjestelmästä, mutta itse yritysturvallisuusselvitystodistuksen antaa turvallisuusselvityslain mukaan suojelupoliisi tai Pääesikunta ja kansainvälisten tietoturvallisuusvelvoitteiden tapauksessa ulkoministeriön kansallinen turvallisuusviranomainen. Yritysturvallisuusselvitystodistus voi siis liittyä joko kansallisiin tai kansainvälisiin tietoturvallisuusvelvoitteisiin.

Arvioinnista laaditaan käytännössä aina arviointiraportti, jossa kuvataan, miten arvioinnin perusteeksi otetut kriteerit toteutuvat arvioinnin kohteessa ja onko tietoturvallisuustoimenpiteiden arvioinnissa havaittu poikkeamia tai puutteita. Arviointiraportista ei säädetä voimassa olevassa arviointilaissa.

Euroopan unionin oikeus

Tieto- ja viestintäjärjestelmien tieto- ja kyberturvallisuuden vaatimustenmukaisuuden arviointia koskeva Euroopan unionin sääntely on viime vuosina lisääntynyt. Euroopan unionin sääntely koskee kuitenkin pääsääntöisesti palveluiden ja tuotteiden sertifiointia niiden tullessa markkinoille, eikä siten vaikuta suoraan jäsenvaltioiden kansalliseen viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden ja varautumisen arviointiin. Sertifioinnilla ja sertifikaatilla tarkoitetaan Euroopan unionin sääntelyssä yleisesti ottaen tiettyjen säädettyjen arviointielimien tietyille tuotteille, palveluille tai prosesseille tarkkarajaisesti säädettyjen vaatimusten perusteella tekemää arviointia ja arvioinnin tulosten perusteella annettuja sertifikaatteja, joiden tarkoitus on osoittaa Euroopan unionin sisämarkkinoilla tuotteen, palvelun tai prosessin ominaisuudet. Viranomaisten tietojärjestelmien tietoturvallisuuden ja varautumisen kansallinen arviointisääntely kohdistuu viranomaisen määräämisvallassa olevan tai hankittavaksi suunnitteleman tietojärjestelmän tai tietoliikennejärjestelyn tietoturvallisuuden ja varautumisen tapauskohtaiseen arviointiin, ei siis markkinoilla yleisesti tarjottavien tuotteiden, palveluiden tai prosessien vaatimuksiin. Viranomaisen tietojärjestelmässä voidaan kuitenkin hyödyntää EU:n

markkinoilla saatavilla olevia sertifioituja tuotteita siltä osin, kun niiden turvallisuus vastaa viranomaisen tarpeita. Arviointilain mukaisissa arvioinneissa voi olla mahdollista hyödyntää Euroopan unionin sääntelyn mukaisen sertifioinnin tuloksia siltä osin, kun sertifioinnin perusteet ja kriteerit ovat soveltuvia.

Kyberturvallisuusasetuksen (Euroopan parlamentin ja neuvoston asetus (EU) 2019/881 Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista sekä asetuksen (EU) N:o 526/2013 kumoamisesta) artiklan 1 mukaan asetuksen kohde on sisämarkkinoiden asianmukaisen toiminnan varmistaminen ja kyberturvallisuuden, kyberresilienssin ja luottamuksen korkea taso unionissa. Tässä tarkoituksessa asetuksessa vahvistetaan kehys kyberturvallisuuden sertifiointijärjestelmien perustamiselle tieto- ja viestintätekniikan tuotteille, palveluille ja prosesseille sekä tietoturvapalveluille. Kehyksillä vältetään sisämarkkinoiden hajautuminen kyberturvallisuuden sertifiointijärjestelmien osalta. Asetus ei 1 artiklan 2 alakohdan mukaan rajoita jäsenvaltioiden toimivaltaa yleisen turvallisuuden, puolustuksen ja kansallisen turvallisuuden alalla eikä yksittäistä valtiota koskevan rikosoikeuden toimissa.

Ensimmäisenä sertifiointijärjestelmänä on vastikään komission täytäntöönpanosäädöksellä (EU) 2024/482 annettu EU:n Common Criteria -skeema (EUCC). Skeema soveltuu esimerkiksi älykorttien ja tietoturvabokseilla varustettujen laitteiden, allekirjoituksen luontivälineiden, sähköisesti luettavien matkustusasiakirjojen ja ajopiirtureiden sertifiointiin. Valmistelussa ovat muun ohessa pilvipalveluita (EUCS, European Union Cybersecurity Certification Scheme for Cloud Services) ja 5G-verkkoja koskevat sertifiointiskeemat. Mahdollisia tulevia työkohteita ovat komission työohjelman mukaan (Work Programme for European cybersecurity certification, SWD (2024) 7.2.2024) digitaalisen identiteetin lompakkosovellus, tietoturvallisuuden hallintapalvelut ja yleisesti CRA:n puitteissa tarvittavat skeemat ja teollisuuden automaatiojärjestelmät. Kyberturvallisuusasetuksen mukaisen sertifioinnin hakeminen on palvelun tai tuotteen tarjoajalle vapaaehtoista.

Euroopan parlamentin ja neuvoston asetus (EU) 2024/2847 digitaalisia elementtejä sisältävien tuotteiden horisontaalisista kyberturvallisuusvaatimuksista ja asetusten (EU) n:o 168/2013 ja (EU) 2019/1020 ja direktiivin (EU) 2020/1828 muuttamisesta, jäljempänä kyberkestävyyssäädös tai CRA, Cyber Resilience Act, annettiin 23.10.2024 ja sen voimaantuloon liittyy siirtymäaikoja. Asetuksella vahvistetaan säännöt digitaalisia elementtejä sisältävien tuotteiden asettamiselle saataville EU-markkinoilla, jotta tuotteiden kyberturvallisuus varmistetaan. CRA on horisontaalinen tuoteturvallisuusasetus, jonka vaatimusten toteutuminen taataan tulevaisuudessa osana CE-merkintää. Asetuksen mukaisten turvallisuusvaatimusten täyttyminen on jatkossa markkinoille pääsyn edellytys EU:ssa. Asetusta ei 2 artiklan 7 alakohdan mukaan sovelleta digitaalisia elementtejä sisältäviin tuotteisiin, jotka on kehitetty tai joita on muutettu yksinomaan kansalliseen turvallisuuteen tai puolustukseen liittyviin tarkoituksiin, eikä tuotteisiin, jotka on erityisesti suunniteltu turvallisuusluokiteltujen tietojen käsittelyä varten.

Euroopan parlamentin ja neuvoston asetus (EU) 2024/1689 tekoälyä koskevista yhdenmukaistetuista säännöistä ja asetusten (EY) N:o 300/2008, (EU) N:o 167/2013, (EU) N:o 168/2013, (EU) 2018/858, (EU) 2018/1139 ja (EU) 2019/2144 sekä direktiivien 2014/90/EU, (EU) 2016/797 ja (EU) 2020/1828 muuttamisesta (tekoälysäädös) säätelee tekoälyjärjestelmiä niiden aiheuttamien riskien perusteella. Asetus kieltää erittäin haitalliset tekoälyn käyttötavat ja asettaa tietyille korkeariskiseksi luokiteltaville tekoälyjärjestelmille tiukennettuja vaatimuksia, joihin kuuluvat muun muassa tietoturvallisuuden varmistaminen koko järjestelmän elinkaaren ajan, mukaan lukien suunnittelu, kehitys, käyttöönotto ja ylläpito. Asetuksessa vahvistetaan yhdenmukaistetut säännöt tekoälyjärjestelmien markkinoille saattamiselle, käyttöönotolle ja käytölle

unionissa. Asetus edellyttää, että suuririskisille tekoälyjärjestelmille tehdään vaatimustenmukaisuuden arviointi ennen kuin ne saatetaan markkinoille tai otetaan käyttöön.

Julkishallinnon toimijoiden kyberturvallisuusriskien hallinnan vaatimuksia puolestaan on yhtenäistänyt NIS2-direktiivi eli toimenpiteistä yhteisen korkeatasoisen kyberturvallisuuden varmistamiseksi koko unionissa annettu Euroopan parlamentin ja neuvoston direktiivi, (EU) 2022/2555, joka on pantu Suomessa täytäntöön julkishallinnon osalta tiedonhallintalain uudessa 4 a -luvussa. Tiedonhallintalain NIS2-sääntely ei koske kuntia ja tiettyjä muita viranomaisia.

Salaustuotteiden, turvallisuuskriittisten tuotteiden ja TEMPEST-tuotteiden ja -mittauspalveluiden arviointi- ja hyväksyntätarpeet liittyvät ennen kaikkea kansainvälisten tietoturvallisuusvelvoitteiden toteuttamiseen erityissuojattavien tietoaineistojen sähköisessä käsittelyssä ja kansallisen turvallisuusluokitellun tiedon sähköisen käsittelyn suojaamiseen. Turvallisuusluokittelun perusteiden voi yleisesti katsoa liittyvän kansalliseen turvallisuuteen ja joissain tapauksissa nimenomaisesti esimerkiksi varautumiseen tai puolustukseen. Siten EU:n sisämarkkinoita koskeva sertifiointisääntely ei näyttäisi estävän vaatimusten ja arviointimenettelyjen asettamista näihin tarkoituksiin kansallisen sääntelyn mukaisesti ja kansainvälisten tietoturvallisuusvelvoitteiden mukaisesti.

3 Tavoitteet

Esityksen tavoitteena on mahdollistaa kustannustehokkaat viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden ja varautumisen arviointimenettelyt. Ehdotuksella vastataan arviointitarpeiden kasvuun, joka johtuu toimintaympäristön ja turvallisuusuhkien muutoksesta. Tavoitteena on parantaa arviointien saatavuutta, sujuvoittaa arviointimenettelyä, selkeyttää arviointiperusteita sekä tehostaa viranomaisyhteistyötä. Tavoitteena on, että viranomaiset hyödyntäisivät tietojärjestelmiensä ja tietoliikennejärjestelyjensä tietoturvallisuus- ja varautumistoimenpiteiden mitoittamisessa tilanteeseen soveltuvaa arviointimenettelyä turvallisuuden edistämiseksi.

Esityksen tavoitteena on lisäksi selkeyttää lainsäädännön tasolla periaatetta siitä, että viranomaisella on vastuu omien tietojärjestelmiensä ja tietoliikennejärjestelyjensä tietoturvallisuudesta ja varautumisesta sekä käyttöönottopäätöksestä. Viranomainen vastaa tietojärjestelmiensä tietoturvallisuudesta ja varautumisesta ja riippumaton arvioinnin toteuttaja vastaa arvioinnin laadusta.

Esityksen tavoitteena on turvallisuuskriittisten ratkaisujen arvioinnin ja hyväksynnän kautta parantaa yritysten mahdollisuuksia tarjota ratkaisujaan sekä Suomessa että kansainvälisissä yhteyksissä. Tavoitteena on myös nopeuttaa tietojärjestelmien ja tietoliikennejärjestelyjen arviointia, kun viranomaisilla on mahdollisuus valita tietojärjestelmiinsä ja tietoliikennejärjestelyihinsä ratkaisuja, jotka on jo arvioitu ja hyväksytty.

Esityksen tavoitteena on edistää tietoturvallisuuden arviointilaitosten elinkeinotoiminnan edellytyksiä yksinkertaistamalla ja tehostamalla tietoturvallisuuden arviointilaitosten luotettavuuden sääntelyä sekä joustavoittamalla pätevyyksien hyväksyntää. Tavoitteena on, että arviointilaitoksilla olisi edellytykset tarjota nykyistä useampiin arviointiperusteisiin ja kriteeristöihin perustuvia arviointeja.

4 Ehdotukset ja niiden vaikutukset

4.1 Keskeiset ehdotukset

Viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen arviointi laajennettaisiin koskemaan tietoturvallisuuden lisäksi varautumista sekä turvallisuuskriittisten ratkaisujen tietoturvallisuuden arviointia. Turvallisuuskriittisellä ratkaisulla tarkoitettaisiin salaus-, hajasäteilysuojaus- ja muuta tieto- ja viestintäteknistä ratkaisua eli tuotetta, toteutusta tai palvelua, jolla suojataan turvallisuusluokiteltua tietoa tietojärjestelmissä ja tietoliikennejärjestelyissä.

Arviointiviranomaiseksi säädettäisiin Liikenne- ja viestintäviraston lisäksi Pääesikunnan määrätty turvallisuusviranomainen. Puolustusvoimille säädettäisiin itsenäinen ja riippumaton arviointiviranomaisen tehtävä, jolla olisi toimivalta arvioida Puolustusvoimien omia järjestelmiä ja niihin kuuluvia turvallisuuskriittisiä ratkaisuja.

Liikenne- ja viestintävirastolle säädettäisiin uusi kotimaisten turvallisuuskriittisten ratkaisujen arviointitehtävä. Suomalaisille valmistajille säädettäisiin mahdollisuus hakea Liikenne- ja viestintävirastolta arviointia ja hyväksyntää julkiseen luetteloon turvallisuuskriittisille ratkaisuille. Lisäksi Liikenne- ja viestintäviraston tehtäviä tarkennettaisiin tietoturvallisuuden arviointiin liittyvän neuvonnan ja tehtävien priorisoinnin osalta.

Valtionhallinnon viranomaisille säädettäisiin velvoite riskiarvioinnin perusteella toteuttaa tietojärjestelmien ja tietoliikennejärjestelyjen arviointi käyttäen arviointilaissa tarkoitettuja arviointimenettelyjä. Myös muut viranomaiset, kuten kuntien ja hyvinvointialueiden viranomaiset, voisivat käyttää arviointilaissa säädettyjä arviointimenettelyjä tietojärjestelmiensä ja tietoliikennejärjestelyjensä arvioinnissa. Korkeampien turvallisuusluokkien tietoja käsittelevien tietojärjestelmien ja tietoliikennejärjestelyjen arviointivelvoitteesta säädettäisiin tarkemmin. Järjestelmästä, jossa käsitellään turvallisuusluokkaan I tai II luokiteltuja tietoja, olisi pyydettävä arviointiviranomaisen arviointi. Järjestelmistä, jossa käsitellään turvallisuusluokkaan III luokiteltuja tietoja, olisi pyydettävä arviointiviranomaisen tai hankittava tietoturvallisuuden arviointilaitoksen arviointi, jollei viranomainen päättäisi sen olevan riskiarvioinnin perusteella tarpeetonta.

Arviointien sujuvoittamiseksi ja saatavuuden parantamiseksi sekä sääntelyn selkeyttämiseksi arviointilakiin lisättäisiin arviointimenettelyiksi viranomaisen toteuttama itsearviointi ja viranomaisen toimeksiannosta palveluntarjoajan toteuttama arviointi. Viranomaisen toimeksiannosta toimiva palveluntarjoaja voisi arvioida tietojärjestelmiä, joissa käsitellään julkisia, salassa pidettäviä ja korkeintaan turvallisuusluokkaan IV luokiteltuja tietoja. Tietoturvallisuuden arviointilaitos voisi arvioida tietojärjestelmiä, joissa käsitellään korkeintaan turvallisuusluokkaan III luokiteltuja tietoja.

Arviointilakiin lisättäisiin arviointiviranomaisten yhteistyötä, työjakoa ja tiedonsaantioikeuksia koskevaa sääntelyä sekä turvattaisiin arviointiviranomaisten toiminnan resurssien riittävyyttä säätämällä arviointiviranomaista avustavasta tehtävästä. Arviointilaissa säädettyjä arviointiperusteita selkeytettäisiin ja niistä säädettäisiin vähemmän yksityiskohtaisesti. Vaatimustenmukaisuudesta annettava todistus korvattaisiin arviointiraportilla lukuun ottamatta tilanteita, joissa kansainväliset tietoturvallisuusvelvoitteet tai kansainvälinen yhteistyö taikka muu sääntely edellyttäisi hyväksyntäpäätöksen tai -lausunnon antamista arvioinnista. Tarkoituksena on säätää ja tarkentaa lain tasolle jo nykyisin käytössä olevat menettelyt ja toimintatavat. Ehdotukset ovat yhteensopivia kansainvälisten tietoturvallisuusvelvoitteiden kanssa eivätkä myöskään vaikuta niihin tulevaisuudessa mahdollisesti harkittaviin muutoksiin.

Arviointilaitoksena toimivan yrityksen luotettavuuden varmistamista yksinkertaistettaisiin ja tehostettaisiin säätämällä yritysturvallisuusselvityksen tekemisestä, jos arviointilaitos hakee pätevyyttä turvallisuusluokitellun tiedon käsittelyn arviointiin. Nykyisen sääntelyn mukainen suojelupoliisin mahdollisuus lausua vastuuhenkilöiden ja toimitilojen osalta koskisi jatkossakin niitä arviointilaitoksia, jotka eivät hae turvallisuusluokiteltuun tietoon liittyviä pätevyyksiä. Laissa säädettäisiin myös millä edellytyksillä arviointilaitos voisi käyttää arviointitehtäviensä suorittamisessa alihankkijaa. Julkiseen hallintotehtävään liittyvien hallinnon yleislakien luetteloa täydennettäisiin vastaamaan nykytilaa ja lakiin lisättäisiin säännös rikosoikeudellisesta virkavastuusta. Arviointilaitoksen tulisi olla Suomeen sijoittautunut oikeushenkilö.

Arviointilaitoksen arviointipätevyyden osoittamisen menettelyjä joustavoitettaisiin. Pätevyysalue liittyisi aina arviointilaitoslain 10 §:ssä säädetyn arviointiperusteen kuten säädöksen, ohjeen tai standardin tuntemukseen. Sen lisäksi, että pätevyyden voi osoittaa FINASin akkreditoinnilla, ja jokaisella hyväksytyllä arviointilaitoksella tulisi olla jokin pätevyyden ja riippumattomuuden osoittava akkreditointi, Liikenne- ja viestintävirastolle säädettäisiin toimivalta päättää uusien pätevyysalueiden hyväksynnästä kuultuaan pätevyyden hyväksymisen kannalta keskeisiä viranomaisia.

Arviointilaitoslakiin tehtäisiin lisäksi muutokset, joita sen yhdenmukaisuus arviointilain kanssa edellyttää, jotta lait muodostavat myös jatkossa yhteentoimivan kokonaisuuden.

4.2 Pääasialliset vaikutukset

4.2.1 Taloudelliset vaikutukset

Esityksessä ei ehdoteta resurssilisäyksiä.

4.2.1.1 Yritykset

Tietoturvallisuuden arviointilaitokset

Arviointilaitoslakiin ehdotetut muutokset tehostaisivat tietoturvallisuuden arviointilaitosten luotettavuuden varmistamista ja joustavoittaisivat pätevyyksien hyväksymistä, mikä kasvattaisi arviointipalvelujen tarjontaa. Arviointilaitoslain päivittäminen tietyiltä osin yhdenmukaisesti arviointilakiin ehdotettujen muutosten kanssa säilyttäisi arviointiviranomaisten ja tietoturvallisuuden arviointilaitosten tekemien arviointien yhteiset piirteet arvioinnin hakijan kannalta selkeänä.

Arviointilakiin ehdotettava uusi mahdollisuus toteuttaa julkisia, salassa pidettäviä ja turvallisuusluokkaan IV luokiteltuja tietoja käsittelevien tietojärjestelmien ja tietoliikennejärjestelyjen arviointi viranomaisen toimeksiannosta palveluntarjoajan toteuttamana arviointina vaikuttaa tietoturvallisuuden arviointilaitosten toimintaan etenkin turvallisuusluokkaan IV luokiteltuja tietoja käsittelevien tietojärjestelmien ja tietoliikennejärjestelyjen arvioijina ja voi vähentää niiltä tilauksia.

Turvallisuusluokkaan IV luokiteltuja tietoja käsittelevien tietojärjestelmien ja tietoliikennejärjestelyjen arvioinneissa tietoturvallisuuden arviointilaitosten kilpailuedellytyksiin voi vaikuttaa se, että muita palveluntarjoajia eivät koske arviointilaitoslaissa säädetyt arvioinnin pätevyys- ja menettelyvaatimukset. Tietoturvallisuuden arviointilaitoksilta edellytetään myös riippumattomuutta, mikä rajoittaa niiden mahdollisuutta konsultoida toteutusten suunnittelua. Tämä vaikuttaa tietoturvallisuuden arviointilaitosten mahdollisuuteen kilpailla hinnoittelulla muiden

palveluntarjoajien kanssa ja voi siten luoda painetta siirtää tietoturvallisuuden arviointilaitoksena toimivan yrityksen toimintaa valvotun pätevyyden ulkopuolella tarjottaviin palveluihin.

Vuonna 2023 kahden tietoturvallisuuden arviointilaitoksen liikevaihdot olivat yhteensä noin 6 miljoonaa euroa liikevoiton ollessa yhteensä noin 1,8 miljoonaa euroa. Syksyllä 2024 järjestetyn sidosryhmätilaisuuden yhteydessä pyydetyn tietoturvallisuuden arviointilaitosten edustajilta saadun kirjallisen palautteen perusteella vain osa edellä mainitusta liikevaihdosta perustuu julkisen hallinnon hankkimiin tietoturvallisuuden arviointipalveluihin. Viranomaisten ja yritysten tilaamien turvallisuusluokiteltujen tietojen käsittelyn tietoturvallisuuden arviointipalvelujen markkinoiden suuruudeksi arvioitiin noin kaksi miljoonaa euroa vuonna 2023. Tämän euromääräisen arvon voidaan katsoa olevan esityksen enimmäisvaikutus tietoturvallisuuden arviointilaitoksille. [2]

Syksyn 2024 tietoturvallisuuden arviointilaitosten kirjallisessa palautteessa korostetaan, että arviointimarkkinat ovat pienet.[1] Valtion tieto- ja viestintätekniikkakeskus Valtori on nykytilassa velvoitettu käyttämään tietoturvallisuuden arviointilaitosten arviointipalvelua turvallisuusluokkaan IV ja III luokiteltuja tietoja käsittelevien tietojärjestelmien arvioinneissa. Puolustusvoimissa on tarvittaessa hankittu turvallisuusluokkiin III ja IV luokiteltuja tietoja käsittelevien tietojärjestelmien arviointeja ostopalveluina. Tietoturvallisuuden arviointilaitosten edustajat ovat ilmaisseet huolensa liiketoimintamahdollisuuksien heikentymisestä, mikäli Puolustusvoimille suunniteltu arviointiviranomaistehtävä toteutuu ja turvallisuusluokkaan IV luokiteltuja tietoja käsittelevien järjestelmien arviointi olisi mahdollista teettää muilla palveluntarjoajilla. Tietoturvallisuuden arviointilaitokset ovat todenneet, että jos Puolustusvoimien tilaukset tietoturvallisuuden arviointilaitoksille päättyvät, arviointitoiminta ei ole enää houkuttelevaa liiketoimintaa. Puolustusvoimien omalla kyvykkyydellä on kuitenkin tarkoitus arvioida ensisijaisesti turvallisuusluokkien I ja II tietoja käsitteleviä tietojärjestelmiä, jolloin Puolustusvoimien arviointiviranomaistehtävällä ei ole ratkaisevaa merkitystä ostopalveluina hankittavien turvallisuusluokkien III ja IV tietoa käsittelevien tietojärjestelmien arviointipalvelujen markkinoihin.

Arviointitoiminnan ja -palvelujen kysynnän ennakoidaan yleisesti ottaen edelleen kasvavan tulevaisuudessa toimintaympäristön ja EU-sääntelyn muutosten vuoksi. EU-sääntelyn mukainen sertifiointitoiminta myös avaa suomalaisille yrityksille mahdollisuuksia EU:n laajuiseen sertifiointipalvelujen tarjoamiseen. Tämä edellyttää EU:n sertifiointisääntelyn mukaisten osa-alueiden osaamisen ja menettelyjen kehittämistä ja EU:n sääntelyn mukaisen vaatimustenmukaisuuden arviointilaitoksen tai ilmoitetun laitoksen aseman hankkimista.

Tietoturvallisuuden arviointilaitosten elinkeinotoiminnan mahdollisuuksiin vaikuttaa myös muu niiden toteuttamia arviointeja koskeva sääntely. Tähän sisältyvät asiakastietolain ja toisiolain vaatimukset hankkia hyväksytyn tietoturvallisuuden arviointilaitoksen todistus tietyille toiminnoille, valtiovarainministeriön määräykset turvallisuusverkon arvioinnista ja NIS2-direktiivin täytäntöönpanossa kyberturvallisuuslaissa (124/2025) ja tiedonhallintalain 4 a luvussa säädetyt mahdollisuudet käyttää hyväksyttyjä arviointilaitoksia valvontaviranomaista avustavassa tehtävässä.

Arviointipalveluita tarjoavat yritykset

Markkinoilla toimii tietoturvallisuuden arviointilaitosten lisäksi yrityksiä, jotka tarjoavat tietoturvallisuuden ja varautumisen asiantuntijapalveluja kuten sertifiointi-, katselmointi- ja

[2] Tietojärjestelmien tietoturvallisuuden ja varautumisen vaatimustenmukaisuuden arvioinnin nykytilaarvio ja kehittämisehdotukset 12.12.2024 -raportti, valtiovarainministeriö.

todentamispalveluja tai tietojärjestelmien suunnitteluun ja kehittämiseen liittyviä tietoturvallisuuden ja varautumisen kehittämisen palveluja. Esitys mahdollistaa vastaavia palveluita tarjoaville, luotettaviksi todetuille yrityksille arviointilain mukaisten julkisia, salassa pidettäviä ja turvallisuusluokan IV tietoja käsittelevien tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden ja varautumisen arviointipalvelujen tarjoamisen viranomaisille. Arviointipalveluja tarjoavien yritysten määrän odotetaan lisääntyvän ja arviointipalvelujen tarjonnan kasvavan. Yritysten ennakoidaan edistävän entistä laajemmin arviointipalvelujen tuotteistamista ja laadun parantamista.

Esitys kasvattaa muiden markkinatoimijoiden kuin tietoturvallisuuden arviointilaitosten osuutta arviointitoiminnan kokonaisuudesta, sillä arviointipalveluja tarjoavien yritysten palveluja on mahdollista käyttää sekä viranomaisen toimeksiannosta että arviointiviranomaista avustavissa tehtävissä. Arviointipalveluja tarjoavien yritysten liikevaihto voi kasvaa enemmän kuin mitä on arvioitu tietoturvallisuuden arviointilaitosten arviointilaitostoiminnan liikevaihdon olevan, koska arviointipalvelujen tarjonnan kasvattaminen voi tuoda näkyväksi myös patoutuneen arviointipalvelujen kysynnän.

Turvallisuuskriittisten ratkaisujen valmistajat

Turvallisuuskriittisten ratkaisujen arvioinnin ehdotettu sääntely parantaa suomalaisten valmistajien liiketoiminnan mahdollisuuksia tuotteiden ja palveluiden arviointi- ja hyväksyntäprosessin kautta. Sääntely lisäisi ennakoitavuutta siitä, millä edellytyksillä arviointeja voidaan tehdä, minkä on arvioitu vähentävän yritysten hallinnollista taakkaa. Julkiselle listalle hyväksyntään tähtäävän kotimaisen valmistajan ratkaisun arviointitehtävän säätäminen Liikenne- ja viestintävirastolle selkeyttää valmistajan kannalta arvioinnin hakemista yhden luukun periaatteella. Toisaalta arviointiviranomaisten yhteistyön, tiedonvaihdon ja tehtävistä sopimisen sääntely mahdollistaa arviointiviranomaisten tarkoituksenmukaisen työnjaon arvioinnissa, minkä arvioidaan sujuvoittavan arviointeja ja tukevan valmistajien mahdollisuuksia saada ratkaisuja nopeammin markkinoille. Tämä yhdessä yhtenäisen soveltamiskäytännön koordinoinnin sääntelyn kanssa edistää sitä, että arviointiperusteet ovat yhdenmukaiset, vaikka ratkaisun arviointi tehtäisiin ensin vain Pääesikunnan määrätyn turvallisuusviranomaisen toimesta Puolustusvoimien tarpeisiin ja hakemus julkiseen luetteloon hyväksymisestä tulisi ajankohtaiseksi vasta myöhemmin.

Turvallisuuskriittisten ratkaisujen kotimaisten valmistajien mahdollisuus hakea arviointia ja hyväksyntää edistää osaltaan näiden yritysten mahdollisuuksia hakeutua myös EU:n ja Naton turvallisuusluokitellun tiedon suojaamisessa tarvittavien ratkaisujen tarjoajaksi.

4.2.2 Muut ihmisiin kohdistuvat ja yhteiskunnalliset vaikutukset

4.2.2.1 Viranomaiset

Arviointeja hankkivien viranomaisten toiminta ja palveluiden tuottaminen

Tiedonhallintalain 9 §:ssä säädetyn lausuntomenettelyn ja sitä tarkentavan valtioneuvoston asetuksen lausuntomenettelystä tiedonhallinnan muutosta koskevissa asioissa (1301/2019) perusteella valtionhallinnon viranomaiset ovat jo vuodesta 2021 lähtien olleet velvoitettuja tekemään vähintään tietoturvallisuuden ja varautumisen itsearvioinnin jokaiselle uudelle tai merkittävästi muutetulle tietojärjestelmälle. Valtionhallinnon viranomaisen toteuttamassa tietoturvallisuuden ja varautumisen itsearvioinnissa ei siis olisi kyse täysin uusista tehtävistä.

Turvallisuusluokkaan I ja II luokiteltuja tietoja käsittelevien tietojärjestelmien ja tietoliikennejärjestelyjen arviointien hakemisesta arviointiviranomaisilta aiheutuu kustannuksia, jotka ovat

välttämätön osa järjestelmien rakentamis- ja elinkaarikustannuksia. Turvallisuusluokkaan III luokiteltuja tietoja käsittelevien tietojärjestelmien ja tietoliikennejärjestelyjen arviointien hakemisesta tietoturvallisuuden arviointilaitoksilta aiheutuu nykytilassa kustannuksia, joita riskiarvioinnin perusteella on mahdollista pienentää toteuttamalla arviointi itsearviointina. Toisaalta tällöin mahdollisesti heikentyvä tietojärjestelmän tai tietoliikennejärjestelyn tietoturvallisuuden tai varautumisen taso voi aiheuttaa riskejä, mukaan lukien riskejä kansalliselle turvallisuudelle tai kustannuksia häiriötilanteissa tai kriiseissä.

Valtionhallinnon viranomaisille arviointilaissa ehdotettujen arviointivelvoitteiden mukaisten arviointien toteuttamisesta arvioidaan aiheutuvan niille jonkin verran kustannuksia, jotka katetaan olemassa olevien määrärahojen puitteissa. Niissä valtionhallinnon viranomaisissa, joissa ei ole kattavasti arvioitu tietojärjestelmien ja palveluiden tietoturvallisuuden ja varautumisen vaatimustenmukaisuuden toteutumista hallinnollinen taakka kasvaisi, mutta toisaalta arviointien toteuttamisen arvioitaisiin pienentävän tietoturvallisuuden häiriö- ja poikkeamatilanteiden hallinnan hallinnollista taakkaa, ja sitä kautta tietojärjestelmien elinkaarikustannuksia. Sellaiselle julkisen hallinnon toimijalle, joka ylläpitää useiden viranomaisten hyödyntämiä tai laajasti käytössä olevia tietojärjestelmiä, esityksestä aiheutuvan hallinnollisen taakan määrä ja kustannukset ovat suurempia, kuin muussa julkisessa hallinnossa.[2]

Arviointilakiin ehdotetut muutokset mahdollistavat taloudellisten näkökulmien huomioimisen arviointimenettelyn valinnassa. Itsearviointien ja toimeksiannosta toteutettujen arviointien laajemman hyödyntämisen mahdollistamisen sekä arviointilain mukaisia arviointipalveluja tarjoavien yritysten määrän ennakoidun kasvun arvioidaan helpottavan arviointien saatavuutta ja hillitsevän arviointien kustannusten kasvua. Esimerkiksi Valtion tieto- ja viestintätekniikkakeskus Valtorissa tehdyn laskelman mukaan kahden henkilön rekrytoiminen tekemään tietojärjestelmien itsearviointeja säästää vuositasolla noin 458 000 euroa verrattuna siihen, että palvelut ostettaisiin ulkopuolisilta arviointilaitoksilta[2].

Vaikka viranomaisille aiheutuisi itsearviointeja laajemmista tietoturvallisuuden ja varautumisen arvioinneista nykytilaa enemmän kustannuksia, arviointien avulla on mahdollista saavuttaa korkeampi tietoturvallisuuden taso sekä siten parempi varautumis- ja reagointikyky tietoturvahäiriöihin ja -loukkauksiin. Tällä tavoin pystytään ehkäisemään tietoturvaloukkauksia ja niiden haitallisia vaikutuksia, jotka voivat aiheuttaa kustannuksia sekä viranomaisille että laajemminkin yhteiskunnassa tahoille, jotka käyttävät viranomaisten palveluita. Esimerkiksi jos tietovuodon seurauksena luottamus viranomaiseen tai palvelun turvallisuuteen menetetään, kustannukset voivat olla merkittävästi arvioinneista aiheutuvia kustannuksia suurempia. NIS2 -direktiivin täytäntöönpanon yhteydessä säädetyt vaatimukset tiedonhallintalain 4 a luvussa ovat jo tarkentaneet kyberturvallisuusriskien hallinnan ja sitä kautta tietoturvallisuuden hallinnan ja toimenpiteiden vaatimuksia niissä viranomaisissa, joita sääntely koskee. Siten sen arviointi, millaista tietoturvallisuuden arviointia tunnistetut riskit edellyttäisivät, voidaan yhdistää samaan prosessiin ja hyödyntää samaa osaamista.

Tieto- ja kyberturvallisuuden sekä varautumisen varmistamisen kustannukset lukeutuvat useimmiten laajemmin viranomaisten ICT-kustannuksiin, jolloin puhtaasti tieto- ja kyberturvallisuuteen ja varautumiseen liittyviä kustannuksia on vaikea erotella ja erotteleminen on usein tulkinnanvaraista. Tieto- ja kyberturvallisuuskustannuksiin voidaan lukea laajasti erilaisia menolajeja, kuten laitteistot, ohjelmistot ja tietoliikenneyhteydet. Muita tieto- ja kyberturvallisuutta ja varautumista edistäviä kustannuksia voivat olla hallinnolliset kulut, henkilöstö- ja toimitilaturvallisuuden kulut, koulutukset ja harjoitukset. Tietoturvaloukkauksilla voi olla merkittäviä negatiivisia taloudellisia vaikutuksia sekä tietojärjestelmän välityksellä palveluja tarjoavalle viranomaisille että palveluja käyttäville tahoille.

Tietoturvahäiriöistä aiheutuvia kustannuksia voidaan arvioida karkeasti sen pohjalta, mitä tosiasialliset tietoturvahäiriötilanteet ovat organisaatioille kustantaneet. Häiriötilanteiden kustannuksiin vaikuttavat monet eri tekijät, kuten häiriön laatu, laajuus, vaikutukset toimijan ja toiminnan jatkuvuuteen sekä miten nopeasti toimija toipuu häiriöstä. Häiriötilanteista voi aiheutua sekä suoria selvitys- ja korjauskustannuksia, että epäsuoria kustannuksia esimerkiksi toiminnan keskeytymisen tai mainehaitan vuoksi. Esimerkiksi vuonna 2019 Lahden kaupunkiin kohdistuneen kyberhyökkäyksen suorat kustannukset olivat 685 670 euroa[3]. Eksponentiaalisesti lisääntyneiden tietoturvahäiriöiden vuoksi niiden aiheuttamat kustannukset ovat myös kokonaisuudessaan kasvaneet.

Arviointimenettelyjen selkeyttämisen ja saatavuuden parantamisen ennakoidaan lisäävän arviointien hyödyntämistä tiedonhallintalain tarkoittamina tietoturvallisuustoimenpiteinä. Tämän odotetaan laajentavan arviointien kattavuutta ja tihentävän niiden toteutusväliä sekä parantavan arviointien ajantasaisuutta, mikä kasvattaisi viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden ja varautumisen tasoa. Arviointien toteuttaminen ei kuitenkaan välttämättä yleisty eikä arviointien positiivisia vaikutuksia saavuteta kaikilla hallinnon tasoilla, sillä muu kuin valtionhallinnon viranomainen voi päättää olla tekemättä tietoturvallisuuden ja varautumisen arviointia edes itsearviointina. Toisaalta kunnille ehdotuksen arvioidaan olevan mahdollistava ja kuntien erityispiirteet huomioiva, joten sen voidaan katsoa tukevan kuntien tietoturvatyötä ja tietoturvallisuuden tason nostamista kustannustehokkaalla tavalla.

Viranomaisilta edellytetään osaamista ja resursseja, kun ne hankkivat arviointipalveluita yrityksiltä, sillä yritykselle on asetettava turvallisuus- ja osaamisvaatimukset. Viranomaiselta edellytettävä osaamis- ja resurssitarve riippuvat käytettävästä hankintamenettelystä sekä arvioivan kohteen turvajärjestelyjen ja tietosisällön mahdollisesta salassapidosta ja turvallisuusluokasta.

Arviointilain soveltamisalan laajentaminen tietoturvallisuuden arvioinnin lisäksi varautumiseen tukee valmiuslain 12 §:ssä säädettyä viranomaisen varautumisvelvollisuutta varmistaa tehtäviensä hoitaminen myös poikkeusoloissa. Varautumisen arvioinnin huomioiminen saattaa lisätä viranomaisten hallinnollista taakkaa. Samalla arviointikohteiden toiminnan jatkuvuus kuitenkin paranee, mikä vähentää hallinnollista taakkaa ja kustannuksia häiriötilanteissa ja poikkeusoloissa.

Turvallisuuskriittisten ratkaisujen arviointia koskevilla ehdotuksilla lisätään viranomaisten mahdollisuuksia hankkia turvallisia ja luotettavia ratkaisuja. Hyväksyttyjen ratkaisujen valitseminen turvallisuusluokitellun tiedon suojaamiseen tietojärjestelmissä ja tietoliikennejärjestelyissä vähentää tarvetta tapauskohtaisille tuotearvioinneille ja nopeuttaa osaltaan tietojärjestelmän ja tietoliikennejärjestelyn arviointia, minkä arvioidaan pääsääntöisesti pienentävän viranomaisten arviointikustannuksia.

Arviointiviranomaisten toiminta ja palveluiden tuottaminen

Ehdotetuilla Liikenne- ja viestintäviraston tehtävillä ei ole olennaisia resurssi- tai kustannusvaikutuksia siltä osin, kun tehtävät koskevat tietojärjestelmien ja tietoliikennejärjestelyjen arviointeja, neuvontaa ja arviointiviranomaisten koordinointia. Nämä tehtävät ovat hoidettavissa olemassa olevilla resursseilla, joita virasto voi kohdentaa arviointitehtävän priorisointia koskevan sääntelyn mukaisesti. Viraston arviointi- ja neuvontatehtävät on säädetty maksullisiksi.

[3] YLE (2019) Kyberhyökkäys on maksanut Lahden kaupungille lähes 690 000 euroa https://yle.fi/a/3-10914550

Suomalaisille turvallisuuskriittisten ratkaisujen valmistajille ehdotettava oikeus hakea itse arviointia ja hyväksyntää Liikenne- ja viestintävirastolta ei kasvata resurssitarpeita. Turvallisuuskriittisten ratkaisujen arvioinnissa käytettävissä olevat resurssit vaikuttavat kuitenkin siihen, kuinka nopeasti ja tehokkaasti Liikenne- ja viestintävirasto pystyy tukemaan arvioinneilla ja hyväksynnöillä suomalaisia valmistajia ja kuinka laajasti vastaamaan viranomaisten pyyntöihin erilaisten tuotteiden ja ratkaisujen arvioinnissa. Hajasäteilyyn liittyviä ratkaisuja tarjoavien TEMPEST-yritysten mahdollisuus hakea hyväksyttyä asemaa olisi uudenlainen hyväksyntäohjaus- ja valvontatehtävä, jolla voi olla maltillisia vaikutuksia resurssien kohdentamiseen kokonaisuutena. Turvallisuuskriittisten ratkaisujen tuottaminen on syvällistä teknistä osaamista sekä investointeja vaativa erityistoimiala, joten yritysten määrä on pieni, mikä vuorostaan pienentää mahdollisia resurssivaikutuksia.

Puolustusvoimille ehdotettava arviointitehtävä olisi uusi, ja näin ollen myös sen resurssivaikutukset olisivat merkittävämpiä. Puolustusvoimien arviointiviranomaisen tehtävien muodostamisessa voitaisiin hyödyntää jonkin verran Puolustusvoimien nykyisiä resursseja, joita on käytetty Puolustusvoimien velvoitteisiin huolehtia tietoaineistojen ja tietojärjestelmien tietoturvallisuudesta ja kansallisista vaatimuksista. Lisäresursseja kuitenkin tarvittaisiin varsinaisen arviointitoiminnan lisäksi tukeviin toimintoihin, kuten johtamiseen, oikeudelliseen osaamiseen ja hallinnolliseen tietoturvallisuuteen. Puolustusvoimat toteuttaa lisäresurssien kohdentamisen kehysten ja Puolustusvoimille muutoin annettavien määrärahojen puitteissa. Kun Puolustusvoimat saa rakennettua arviointikyvykkyyden arviointiviranomaisen tehtävässä, muutos luo myös valmiuksia kansainvälisten tietoturvallisuusvelvoitteiden edellyttämiin arviointeihin. Tämä voisi ajan mittaan vapauttaa Liikenne- ja viestintävirastolta resursseja muille arvioinnin hakijoille ja parantaa esityksen tavoitteiden mukaisesti myös arviointiviranomaisen arviointien saatavuutta. Puolustusvoimien tehtäväkentän laajentaminen kansainvälisten järjestelmien arviointiin edellyttää lisähenkilöstöä ja osaamisen kehittämistä.

Viranomaisten ja niiden palveluntuottajina olevien yritysten tietojärjestelmien hajasäteilysuojauksen arviointi on osa tietojärjestelmien tietoturvallisuuden arviointia ja voi perustua joko vyöhykkeisiin tai tilojen tai laitteiden kykyyn estää tahatonta hajasäteilyä. Liikenne- ja viestintäviraston tai Puolustusvoimien arviointitehtävien sääntelyllä ehdotetulla tavalla ei ole välitöntä vaikutusta resurssitarpeisiin. Tehtävistä huolehditaan käytännössä usean viranomaisen yhteistyöllä ja näiden viranomaisten arvion mukaan vyöhyke- ja tilamittauksiin liittyy nähtävissä oleviin operatiivisiin tarpeisiin vastaamiseksi vähäistä henkilöresurssien lisäystä. Salaustuote- ja TEMPEST-tehtäviin liittyy myös laboratoriokyvykkyyden tarve, jonka resurssivaikutukset riippuvat valittavista toteutusmalleista.

Ehdotetulla arviointiviranomaista avustavilla tehtävillä ei katsota olevan merkittäviä kustannusvaikutuksia. Kustannusvaikutuksia ei katsota myöskään olevan ehdotetuilla sääntelyllä arviointiviranomaisten yhteistyöstä ja tehtävien jakamisesta.

Tietojärjestelmien ja tietoliikennejärjestelyjen varautumisen arviointi on sisällöltään uusi osaalue. Arviointiviranomaisten voimavarat vaikuttavat siihen, missä määrin varautumisen osaamista ja johdonmukaisia kriteerien valinnan ja tulkinnan sekä todentamisen käytäntöjä on mahdollista kehittää.

Muiden viranomaisten toiminta ja palveluiden tuottaminen

Suojelupoliisin työmäärää voi jossain määrin lisätä yritysturvallisuusselvityksen tekeminen turvallisuuskriittisten ratkaisujen valmistajista ja tietoturvallisuuden arviointilaitoksista, jotka hakevat turvallisuusluokitellun tiedon käsittelyn arvioinnin pätevyyttä. Arviointilaitosten ja turvallisuuskriittisiä ratkaisuja valmistavien ja tarjoavien yritysten määrä ei ole suuri, joten

vaikutus suojelupoliisiin tehtäviin olisi vähäinen. Arviointilaitosten osalta suojelupoliisi tekee nykyisellääänkin vastuuhenkilöiden henkilöturvallisuusselvityksiä ja voi lausua toimitiloista, mutta tehtävä laajentuisi yrityksen luotettavuuteen ja seurantaan.

FINASin tehtäviin voisi vähäisessä määrin vaikuttaa se, että tietoturvallisuuden arviointilaitoksen lisäpätevyyden hakeminen ja myöntäminen tulisi arviointilaitoslaissa mahdolliseksi ilman FINASin akkreditointia. Mahdollisuus koskisi vain lisäpätevyyksiä ja tietoturvallisuuden arviointilaitoksen hyväksynnän edellytys olisi jatkossakin jokin soveltuva FINASin akkreditoima pätevyys, kuten pätevyys tietoturvallisuuden johtamisjärjestelmän sertifiointiin standardin ISO/IEC 27001 mukaan. Lisäpätevyyksien hyväksyntä Liikenne- ja viestintäviraston päätöksellä ilman FINASin akkreditointia ei vaikuttaisi FINASin tehtäviin tai vastuisiin, sillä näiden lisäpätevyyksien seuranta kuuluisi kokonaisuudessaan Liikenne- ja viestintäviraston ohjaus- ja valvontatoiminnan vastuulle. Arviointilaissa ehdotettuun hajasäteilysuojaus- eli TEMPEST-yritysten hyväksyntään mahdollisesti sisällytettävä akkreditointi voisi tuoda FINASille vain vähäisiä lisätehtäviä ottaen huomioon yritysten pieni lukumäärä.

Arviointilaitoslakiin ehdotettu Liikenne- ja viestintäviraston velvollisuus pyytää lausuntoa sotesääntelyyn perustuvissa lisäpätevyyksissä ei vaikuttaisi soteviranomaisten tehtäviin, vaan selkeyttäisi arviointilaitoslain, asiakastietolain ja toisiolain välistä suhdetta. Samoin Liikenne- ja viestintäviraston oikeus saada arviointilaitoslain valvonnassa välttämättömiä tietoja soteviranomaisilta selkeyttäisi viranomaisten suhdetta ja yhteistyötä, jota viranomaiset tekevät jo ennestään.

Tiedonhallinnan muutokset

Esityksellä selvennetään tiedonhallintayksikön vastuuta tietoaineistojen ja tietojärjestelmien turvallisuudesta. Lisäksi esityksellä vahvistetaan viranomaisten palveluiden yleistä tietoturvallisuuden tasoa ja kriisinkestävyyttä. Tietojärjestelmien ja tietoliikennejärjestelyjen häiriötilanteilla voi olla merkittäviä ja laajamittaisia haitallisia vaikutuksia, joiden toteutumista esityksellä pyritään välttämään. Hyvä tietoturvallisuus ja häiriönsietokyky minimoivat tietovuotojen sekä aineellisten ja aineettomien omaisuuksien menetyksiä ja tietojärjestelmän käytön keskeytymisestä aiheutuvia haittoja. Tietojärjestelmien tietoturvallisuuden ja varautumisen arvioinnin parantuessa haitallisten vaikutusten aiheuttaminen viranomaisten toiminnan kannalta keskeisille palveluille vaikeutuu ja kallistuu.

4.2.2.2 Kansallinen turvallisuus

Kansallista turvallisuutta tarkastellaan tässä viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden ja varautumisen kannalta yleisesti ja erityisesti turvallisuusluokittelun tiedon suojaamisen näkökulmasta.

Tietoturvallisuuden ja varautumisen arviointi parantaa yleisesti tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuutta ja jatkuvuutta, mikä vaikuttaa positiivisesti myös kansalliseen turvallisuuteen. Velvoite turvallisuusluokkiin I ja II luokiteltuja tietoja käsittelevien tietojärjestelmien ja tietoliikennejärjestelyjen arvioinnin hankkimiseen arviointiviranomaiselta parantaa osaltaan kansallista turvallisuutta. Turvallisuusluokkaan III luokiteltua tietoa käsittelevien tietojärjestelmien ja tietoliikennejärjestelyjen osalta arviointien parantava vaikutus kansalliseen turvallisuuteen riippuu osittain siitä, millaisia arviointimenettelyjä viranomaiset riskiarvioinnin perusteella valitsevat.

Puolustushallinnon arviointitehtävän arvioidaan vaikuttavan myönteisesti kansallisen turvallisuuden kehittymiseen, koska Puolustusvoimien tietojärjestelmien ja tietoliikennejärjestelmien

arviointipalvelujen saatavuus kasvaa ja sotilaallisen puolustuksen erityispiirteiden huomiointi arvioinneissa paranee, mikä vuorostaan parantaa järjestelmien tietoturvallisuutta ja varautumista ja nopeuttaa järjestelmien käyttöönottoa. Tietoturvallisuuden arviointilaitosten yritysturvallisuusselvitykset sekä yritysturvallisuusselvitysten edellyttäminen turvallisuuskriittisten tuotteiden valmistajilta edistävät osaltaan kansallista turvallisuutta, koska siten varmistetaan arviointilaitosten ja valmistajien luotettavuus ja turvallisuus.

Kansallisen turvallisuuden kannalta etenkin turvallisuusluokkaan IV luokitellun tiedon käsittelyn tietoturvallisuusjärjestelyjä ja viranomaisen tietojärjestelmien ja tietoliikennejärjestelyjen varautumisen järjestelyjä koskevien tietojen käsittely arviointipalveluja tarjoavissa yrityksissä toimeksiannosta toteutetuissa arvioinneissa voi aiheuttaa riskejä turvallisuusluokkaan IV luokiteltujen tietojen luottamuksellisuuden vaarantumisesta tai päätymisestä pahantahtoisille toimijoille. Riskit voivat liittyä esimerkiksi tietojenkäsittelyn tietoturvallisuuteen, turvallisuusluokiteltujen tietojen kertymiseen palveluntarjoajalle, palveluntarjoajien henkilöstöön, toimitusketjuihin tai ulkomaisiin vaikutusmahdollisuuksiin. Ne voivat vähentää viranomaisten kokemaa luottamusta toistensa järjestelmistä. Siten toimeksiannosta toteutettu arviointi edellyttää huolellista arviointikohteen perusteella toteutettua kansallisten riskien arviointia sekä palveluntarjoajan luotettavuuden ja viranomaisten tietojen asianmukaiseen suojaamisen varmistamista. Täten voidaan saavuttaa taloudellisissa vaikutuksissa ja vaikutuksissa viranomaisiin kuvatut toimeksiannosta toteutettujen arviointien myönteiset vaikutukset ilman kansalliseen turvallisuuteen liittyvien riskien toteutumista.

Esityksellä arvioidaan olevan viranomaisten häiriöttömän toiminnan edistämisen kautta välillisesti myönteisiä vaikutuksia kansalaisten turvallisuudelle. Edistämällä viranomaisten toiminnan ja palveluiden kykyä sietää tietoturvahäiriöitä parannetaan välillisesti kansalaisten turvallisuutta erityisesti silloin, kun toimialassa tai palvelussa kyse on kansalaisten turvallisuuteen vaikuttavista seikoista. Esityksen tavoitteena on vähentää tietoturvahäiriöiden määrää. Näkyvien tietoturvahäiriöiden yleistyminen olisi omiaan vaikuttamaan kansalaisten luottamukseen viranomaisiin ja kansalaisten kokemukseen turvallisuudesta.

4.2.2.3 Tietoyhteiskunta ja tietosuoja

Esityksellä on myönteisiä vaikutuksia tietoyhteiskunnan kehitykseen, sillä se edistää tietoturvallisten palvelujen ja käytänteiden käyttöönottoa sekä tietojärjestelmien ja tietoliikennejärjestelyjen koko elinkaaren aikaisen tietoturvallisuuden paranemista ja yleistä tietoturvatason nousua. Tämä luo kysyntää tietoturvallisuuden ammattilaisille sekä tietoturvallisille tuotteille ja palveluille markkinoilla. Tietoturvatason parantuminen vähentää julkisten palvelujen käytössä esiintyviä häiriöitä ja edistää yleistä luottamusta digitaalisiin palveluihin.

5 Muut toteuttamisvaihtoehdot

5.1 Vaihtoehdot ja niiden vaikutukset

Esitystä valmisteltaessa on arvioitu mallia, jossa Valtion tieto- ja viestintätekniikkakeskus Valtorin yhteyteen perustettaisiin itsenäinen ja riippumaton arviointi- ja hyväksyntäviranomainen, jonka tehtävänä olisi Valtorin palveluiden sekä niihin liittyvien tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden ja varautumisen vaatimustenmukaisuuden arviointi. Mallissa Valtorin arviointitoimintaa voitaisiin käytettävissä olevien resurssien puitteissa hyödyntää laajemminkin yhteisiin tieto- ja viestintäteknisiin palveluihin liitettävien asiakkaiden tietojärjestelmien tietoturvallisuuden tai varautumisen arvioinnissa. Valtorilla olisi maksullinen arviointipalvelu, joka toimisi arviointilaitoksien arviointitoiminnan rinnalla.

Lain valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä (1226/2013) jäljempänä *Tori-laki*, peruslähtökohta kuitenkin on, että Valtori on palvelutuottaja, jolta viranomaiset tilaavat tieto- ja viestintätekniset palvelunsa. Tori-lain esitöissä (HE 150/2013 vp s. 41) on katsottu, että valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestäminen olisi julkinen hallintotehtävä. Palvelujen järjestämiseen liittyvää julkista valtaa käyttäisi valtiovarainministeriö tai muu viranomainen, jolla on kokonaisuuteen liittyviä viranomaistehtäviä. Valtori ei käyttäisi julkista valtaa eikä tekisi hallintopäätöksiä, vaan sen toiminta perustuisi sopimuksiin. Tämän vuoksi Valtorin nykyinen oikeudellinen asema ei mahdollista viranomaistehtävien, kuten arviointitehtävien, hoitamista ilman Valtorin oikeudellisen aseman ja lainsäädännön muutosta.

Esitystä valmisteltaessa on arvioitu myös mallia, jossa arviointilakiin ehdotettavat valtionhallinnon viranomaisia koskevat arviointivelvoitteet säädettäisiin koskemaan myös muita kuin valtiohallinnon viranomaisia. Tämä tukisi esityksen tavoitetta, että viranomaiset hyödyntäisivät kaikkien tietojärjestelmiensä ja tietoliikennejärjestelyjensä tietoturvallisuustoimenpiteiden ja varautumistoimenpiteiden mitoittamisessa tilanteeseen soveltuvaa arviointia tietojärjestelmien tietoturvallisuuden kasvavan merkityksen vuoksi.

Arviointivelvoite olisi kuitenkin aluehallinnolle, hyvinvointialueille ja kunnille uusi lakisääteinen tehtävä, josta aiheutuisi niille kustannuksia. Pääministeri Petteri Orpon hallitusohjelman mukaan hallitus jatkaa normien purkamista nykyisestä kuntien tehtäväkentästä. Kunnille lisäkustannuksia aiheuttavia säädösmuutoksia ei voida pitää hallituksen tavoitteiden mukaisina. Kuntien olosuhteet, talous ja elinkeinorakenne vaihtelevat merkittävästi ympäri maata, jolloin myös niiden edellytykset arvioida tietojärjestelmiä vaihtelevat suuresti. Näin ollen ei voida pitää tarkoituksenmukaisena velvoittaa kuntia tietojärjestelmien arviointiin. Rakenneuudistuksen kohteena olevalle aluehallinnolle tai toimintaansa vasta aloitteleville hyvinvointialueille ei myöskään nähty perustelluksi asettaa mahdollisesti kustannuksia kasvattavia uusia velvoitteita.

Arviointitoiminnan ajantasaistamistyön yhteydessä on myös pohdittu mallia, jossa viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden ja varautumisen arviointimenettelyitä olisivat ainoastaan itsearviointi ja turvallisuusluokitellun tiedon käsittelyn osalta tietoturvallisuuden arviointilaitosten toteuttama arviointi. Tietoturvallisuuden arviointilaitokset ovat investoineet merkittävästi henkilöstön osaamisen kehittämiseen sekä tietoturvallisuuden arviointitoiminnassa tarvittaviin tiloihin, laitteisiin ja prosessien kehittämiseen. Arviointilaitosten osaamisessa korostuu turvallisuusluokitellun tiedon käsittelyn luottamuksellisuuden ja eheyden turvaamisen arviointi. Arviointiviranomaisilla on kuitenkin tietoturvallisuuden arviointilaitoksia vankempi osaaminen turvallisuusluokkia I ja II käsittelevien tietojärjestelmien ja tietoliikennejärjestelyjen toiminnallisista vaatimuksista, toimintaympäristöstä ja turvallisuusjärjestelystä. Turvallisuusluokkaa IV olevia tietoja käsittelevien tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden ja varautumisen arvioinneissa luottamuksellisuuden ja eheyden arvioinnin rinnalla merkittävää on arviointien kustannukset ja saatavuuden varmistaminen sekä tietojen saatavuuden turvaamisen arviointi. Siten turvallisuusluokitellun tiedon käsittelyn arviointien keskittämistä kokonaan tietoturvallisuuden arviointilaitoksille ei voida pitää perusteltuna.

Kaikille viranomaisille asetettavia arviointivelvoitteita valmisteltaessa esillä oli myös vaihtoehto, jossa valtioneuvoston asetuksella voitaisiin säätää viranomaisen velvollisuudesta hakea arviointiviranomaisen tai tietoturvallisuuden arviointilaitoksen arviointi asetuksessa nimetylle tietojärjestelmälleen tai tietoliikennejärjestelylleen, joka on yhteiskunnan turvallisuuden ja varautumisen kannalta merkittävä. Säännöksen tarkoituksena olisi ollut varmistaa, että arviointiviranomainen tai tietoturvallisuuden arviointilaitos toteuttaisi yhteiskunnan turvallisuuden ja varautumisen kannalta merkittävien tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden ja varautumisen arvioinnit, vaikka arvioitavassa järjestelmässä ei käsiteltäisi

turvallisuusluokkiin I, II tai III luokiteltuja tietoja. Kyseessä olisi voinut olla esimerkiksi yhteiskunnan, valtionhallinnon, aluehallinnon tai paikallishallinnon toimivuuden tai yksityisyyden suojan näkökulmasta merkittävä järjestelmä, esimerkiksi väestötietojärjestelmä, kiinteistötietojärjestelmä, vaalijärjestelmä tai turvallisuus- tai varautumisjärjestelyissä käytettävä alue- tai paikallishallinnon järjestelmä. Vaihtoehtoa ei kuitenkaan toteutettu, koska perusteita sille, että muista arviointivelvoitteista säädettäisiin lain tasolla ja tämä velvoite jäisi asetukseen ei ollut. Myöskään ei nähty mahdolliseksi lain tasolla tunnistaa selkeästi tarkempia kriteerejä, joiden perusteella arviointivelvoite voitaisiin asettaa. Arviointilakiin ehdotettavat muutokset eivät kuitenkaan sulje pois sitä mahdollisuutta, että yhteiskunnan varautumisen ja turvallisuuden kannalta merkittävän järjestelmän haltija valitsee hakea arviointiviranomaisen arviointia järjestelmälleen, mikäli se on riskiarvioinnin perusteella tarkoituksenmukaista.

Työryhmätyöskentelyn aikana on ollut mukana valmistelussa ja arviointilaitoslakiin on luonnosvaiheessa ehdotettu säännöstä, jonka perusteella Liikenne- ja viestintäviraston hyväksymillä tietoturvallisuuden arviointilaitoksilla olisi oikeus oman tai alihankkijan henkilöstön luotettavuuden varmistamiseksi hakea turvallisuusselvityslain mukaisia henkilöturvallisuusselvityksiä ja Suojelupoliisi voisi tarpeettomien turvallisuusselvitysten laadinnan estämiseksi antaa arviointeja suorittaville henkilöille henkilöturvallisuusselvitystodistuksen. Tietoturvallisuuden arviointilaitokset pitävät henkilöturvallisuusselvityksiin liittyviä haasteita tällä hetkellä merkittävästi arviointitoimeksiantojen sujuvuuteen vaikuttavana ongelmana. Ehdotuksen tarkoituksena olisi ollut vähentää päällekkäistä kustannuksia aiheuttavaa työtä sekä varmistaa että arviointeja suorittavista henkilöistä haetaan turvallisuusselvitykset kattavasti arviointilaitosten toimesta.

Työryhmätyöskentelyssä on tuotu esille, että turvallisuusselvityslaissa lähtökohtana on, että selvitystä hakee se, jonka suojattavasta edusta on kysymys. Vain taho, jonka etua suojataan, voisi arvioida henkilöturvallisuusselvitysten mahdollisten ilmoitettavien tietojen merkityksen suhteessa tehtävässä suojattavaan etuun. Ehdotus merkitsisi poikkeamista turvallisuusselvityslain keskeisistä lähtökohdista, eikä sitä ole otettu osaksi työryhmän lopullista esitystä. Asiaa ehdotetaan arvioitavaksi turvallisuusselvityslain arvioinnin yhteydessä.

Arviointimenettelyjen sujuvoittamiseksi tarkoitettuja sääntelyn tarkennuksia on valmistelussa käsitelty laajemmin kuin mitä muutosehdotuksiin on sisällytetty. Pohditut sääntelyn tarkennukset koskivat muun muassa valtiovarainministeriön ohjausta ja ohjeistusta koskien viranomaisten pyytämiä ja hankkimia arviointeja, arvioinnissa käytettäviä todentamis- eli tarkastusmenetelmiä, arviointikriteeristöjä, arviointien voimassaoloaikoja, viranomaisten velvollisuuksia tietojärjestelmien poikkeamien havainnoinnissa ja niihin reagoimisessa sekä viranomaisten viestintävelvoitetta toteutetuista arvioinneista julkiselle hallinnolle. Näiden tarkennusten osalta todettiin, että valtiovarainministeriön yleistoimivalta on riittävä ohjauksen ja ohjeistuksen antamiselle. Muiden käsiteltyjen näkökulmien osalta todettiin, että yksityiskohtaisen ja nopeasti muuttuvan sääntelyn välttämiseksi ne soveltuvat paremmin ohjauksella ja ohjeistuksella toteutettaviksi kuin lainsäädäntöön lisättäviksi.

5.2 Ulkomaiden lainsäädäntö ja muut ulkomailla käytetyt keinot

Muiden valtioiden lainsäädännön ja käytäntöjen tarkastelussa on tarpeen erottaa turvallisuusluokitellun tiedon käsittelyn suojaaminen muista tiedon ja toiminnan vaatimuksista tietojärjestelmissä ja tietoliikennejärjestelyissä. Turvallisuusluokitellun tiedon suojaamisen vaatimuksista ja käytännöistä kattavimpina vertailukohtina voi pitää EU:n ja Naton turvallisuusluokitellun tiedon suojaamista koskevia turvallisuusääntöjä. Useissa valtioissa Nato-sääntelyn toimintamalleja sovelletaan myös kansallisen turvallisuusluokitellun tiedon suojaamisessa. Siten Nato-sääntely on merkittävin yhtenevä kansainvälisten ja kansallisten turvallisuusluokiteltujen tietojen käsittelyyn liittyvä arviointisääntely. EU:n turvallisuusluokitellun tiedon arvioinnin sääntely on

Nato-sääntelyn kanssa pääsääntöisesti yhtenevää. Myös Suomessa turvallisuusluokitellun tiedon suojaamisen sääntelyssä turvallisuusluokitteluasetuksessa on pyritty huomioimaan riittävä yhteensopivuus EU:n turvallisuussääntöjen kanssa.

EU:n ja Naton turvallisuussääntöjen pääpiirteet esityksen kannalta ovat velvoitteet arvioida ja hyväksyä kaikki turvallisuusluokiteltua tietoa käsittelevät tietojärjestelmät ja tietoliikennejärjestelyt. Tietoturvallisuusvaatimusten vähimmäistaso on määritelty turvallisuussäännöissä ja niihin kuuluvissa ohjeissa, mutta keskeinen velvoite on tarkastella uhkia ja riskejä järjestelmäkohtaisesti ja määritellä turvallisuustoimenpiteet sen mukaisesti. Viimekätinen vastuu on järjestelmän haltijalla, mutta sen liikkumavaraa riskipäätöksissä kaventaa se, että tiettyihin elementteihin tulee olla arvioinnista vastaavan toimivaltaisen tahon hyväksyntä. Lisäksi tietojärjestelmä- ja tietoliikennejärjestelyn kokonaisuudesta on laadittava toimivaltaisen arviointitahon hyväksyntälausunto, josta ilmenevät jäännösriskit. EU:n ja Naton turvallisuusääntöjen menettelyt, erityisesti Naton turvallisuusääntöjä tarkentavat direktiivit, ohjaavat myös arvioijan ja järjestelmän haltijan yhteistyöhön suunnittelusta alkaen, jolloin poikkeamiin reagoiminen on mahdollista jo suunnittelu- ja toteutusvaiheessa.

EU:n ja Naton turvallisuusluokitellun tiedon suojaamisessa arviointi- ja hyväksyntävelvoitteet koskevat nimenomaisesti myös salausratkaisuja ja tiettyjä muita tietoteknisiä ratkaisuja kuten yhdyskäytäviä silloin, kun tiedon suojaaminen riippuu näistä ratkaisuista. Salausratkaisuihin liittyy myös toisen arvioinnin, niin kutsutun second party evaluation, vaatimus turvallisuusluokasta EU SECRET ja NATO SECRET alkaen sekä jos salausratkaisu halutaan EU:n yhteiseen hyväksyttyjen salausratkaisujen luetteloon (LAPC, List of Approved Products). Toisen arvioinnin Suomen toimivaltaisen viranomaisen eli Liikenne- ja viestintäviraston lisäksi tekisivät EU:n tapauksessa hyväksytty eli AQUA-valtion toimivaltainen viranomainen ja Naton tapauksessa SECAN-virasto.

Naton ja EU:n turvallisuusääntöjen yksityiskohdat turvallisuuskriittisten tuotteiden ja ratkaisujen suhteen ovat jonkin verran erilaiset, ja niihin liittyy myös näköpiirissä olevia muutoksia. Edelleen arviointi- ja hyväksyntävelvoite koskee tietyissä turvallisuusluokissa tiedon suojaamista tahattoman hajasäteilyn (TEMPEST) vaikutuksilta. Turvallisuussääntöjä täydentävissä ohjetason asiakirjoissa määritellään monia yksityiskohtia ja menettelyjä tuotteiden ja ratkaisujen tietoturvallisuusvaatimuksista sekä niiden valmistuksen vaatimuksista. Ohjetason asiakirjoilla luodaan myös menettely TEMPEST-yritysten hyväksyntään (akkreditointiin) ja jatkuvaan ohjaukseen sekä valvontaan. Menettelyn tarkoitus on nimetä yritykset, jotka ovat osoittaneet kyvykkyytensä ja pätevyytensä tuottaa luotettavasti ja laadukkaasti joitain hajasäteilysuojaukseen liittyviä tuotteita tai toimintoja siten, ettei toimivaltaisen TEMPEST-viranomaisen ole tarpeen arvioida niitä ennalta. Turvallisuusäännöt edellyttävät tiukkaa ohjausta ja valvontaa, mutta eivät ota kantaa siihen, kuinka asia kansallisesti toteutetaan oikeudellisesti. TEMPEST-yritysten nimeäminen voi siten perustua kansalliseen sääntelyyn tai kansalliseen hallintosopimukseen. Suomessa molemmat tavat edellyttäisivät sääntelyperustaa.

Viron kansallisen turvallisuusluokitellun tiedon suojaamiseen kohdistuu samansuuntainen akkreditointimenettely kuin esimerkiksi EU:n ja Naton turvallisuusluokiteltuun tietoon. Virossa siis myös vain kansallista turvallisuusluokiteltua tietoa käsittelevät tietojärjestelmät läpikäyvät akkreditointiprosessin. Kansallista turvallisuusluokiteltua tietoa käsittelevien tietojärjestelmien suojaamisessa hyödynnetään samansuuntaisia vaatimuksia ja menettelyjä kuin esimerkiksi Naton turvallisuusluokitellun tiedon suojaamisessa.

Alankomaissa turvallisuusluokitellun tiedon suojaamisen arviointiin hyödynnetään General Security Requirements for Central Government (ABRO)- kehikkoa, joka on hyvin yhtenevä esimerkiksi Suomen Katakrin kanssa. Alankomaissa ABRO:n historia on puolustushallinnossa,

mutta sen käyttö on viime vuosina laajentunut myös muualla Alankomaiden valtionhallintoon ja sen sidosryhmiin turvallisuusluokitellun tiedon suojaamisen arvioinneissa.

Valtion virastojen ja kriittisen infrastruktuurin toimijoiden tietoturvallisuuden säännöllistä tarkastamista suositellaan Tanskassa, Ruotsissa, Virossa, Saksassa ja Alankomaissa, mutta tarkastuksen toteutuskäytäntö vaihtelee ja NIS2-direktiivin täytäntöönpano on voinut vaikuttaa käytäntöihin. Säännöllistä arviointia edellytetään määrävälein Virossa ja Saksassa, kun taas Tanskassa, Ruotsissa ja Alankomaissa määrävälein toteutettuja arviointeja ei edellytetä. Virossa ministeriöt, virastot sekä valtion tietoturvallisuuteen liittyvät rekisterinpitäjät ovat velvollisia suorittamaan arvioinnin suojausluokituksen mukaisesti kahden, kolmen tai neljän vuoden välein. Saksassa on säädetty, että kriittisen infrastruktuurin toimijoiden tulee kahden vuoden välein osoittaa palvelunsa täyttävän tietoturva-asetuksen (IT-SiG) vaatimukset auditointien, tutkimusten tai sertifikaattien avulla. Myös Singaporessa kyberturvallisuuslaki edellyttää kriittisen infrastruktuurin toimijoita suorittamaan tietoturvallisuusauditointia vähintään kerran vuodessa.

Yleisesti ottaen Tanskassa, Ruotsissa, Virossa, Saksassa ja Alankomaissa tunnustetaan ja hyväksytään kansainväliset tietoturvallisuuden alueiden standardit. ISO/IEC 27001 -standardi on tunnustettu tietoturvan hallintajärjestelmien toteuttamisessa ja ISO/IEC 17021-1 -standardi asettaa vaatimuksia tietoturvallisuuden arviointilaitosten akkreditointiprosessiin. Tanskassa on erityisesti säädetty, että kaikkien valtion viranomaisten on noudettava ISO/IEC 27001 -standardia vuodesta 2014 lähtien. Saksassa on kehitetty tietoturvan hallintajärjestelmänä BSI IT-Grundschutz, joka kattaa tekniset ja organisatoriset sekä infrastruktuuriin ja henkilöstöön liittyvät näkökulmat. Viro on ottanut mallia Saksan IT-Grundschutzista ja laatinut oman E-ITS-standardinsa.

Virossa asetus tietojärjestelmien turvatoimenpiteiden järjestämisestä edellyttää, että valtion turvallisuuden hallintajärjestelmän toteutuksen auditoinnissa tarkastajalla tulee olla voimassa olevat sertifikaatit. Tarkastajalla täytyy siis olla paikallisen ISACA:n myöntämä CISA-sertifikaatti (Certified Information Systems Auditor) sekä Yhdistyneen kuningaskunnan kansallisen standardointielimen (British Standards Institution, BSI) myöntämä ISO/IEC 27001 -sertifikaatti tai Saksan kyberturvallisuusviranomaisen (Bundesamt für Sicherheit in der Informationstechnik, BSI) myöntämä ISO/IEC 27001 IT-sertifikaatti.

Vain osasta vertailuvaltiosta löydettiin tietoja julkisen hallinnon tietoturvallisuuden arviointilaitoksista tai niitä koskevista lainsäädännöistä. Esimerkiksi Saksassa viranomaisten tietoturvallisuusarviointia tukevat kyberturvallisuusviranomaisen (BSI) sertifioimat tietoturvapalveluntarjoajat. Tanskassa, Ruotsissa, Virossa, Saksassa ja Alankomaissa valtiontalouden tarkastusviraston yleiseen tehtävään kuuluu valtion viranomaisten tietoturvajärjestelmien tarkastus.

6 Lausuntopalaute

[täydennetään lausuntokierroksen jälkeen]

7 Säännöskohtaiset perustelut

7.1 Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista

1 § *Soveltamisala.* Lain soveltamisalaa laajennettaisiin siten, että lain *1 momenttiin* lisättäisiin varautumisen arviointi sekä turvallisuuskriittisen ratkaisujen tietoturvallisuuden arviointi.

Laissa säädettäisiin jatkossa viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioimisen lisäksi myös viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen varautumisen arvioinnista. Varautumisen arvioinnin lisääminen olisi tarkoituksenmukaista, koska tiedonhallintalakiin on vuonna 2023 lisätty 13 a §, jonka mukaan tiedonhallintayksikön on selvitettävä sen tietoaineistojen käsittelyn, tietojärjestelmien hyödyntämisen sekä niihin perustuvan toiminnan jatkuvuuteen kohdistuvat olennaiset riskit ja varauduttava normaaliolojen ja poikkeusolojen häiriötilanteisiin. Soveltamisalan laajentaminen edistäisi tietojärjestelmien ja tietoliikennejärjestelyjen jatkuvuudenhallintaan ja valmissuunnitteluun vaikuttavien tekijöiden johdonmukaista huomioimista viranomaisissa.

Lisäksi laissa säädettäisiin turvallisuuskriittisten ratkaisujen valmistuksen ja ratkaisujen tietoturvallisuuden arvioinnista. Turvallisuuskriittisiä ratkaisuja olisi tarve arvioida sekä osana viranomaisen tietojärjestelmiä ja tietoliikennejärjestelyjä että tilanteessa, jossa valmistaja hakee itsenäisesti hyväksyntää turvallisuuskriittiselle ratkaisulle viranomaisen turvallisuusluokiteltujen tietojen suojaamiseen. Turvallisuuskriittisistä ratkaisuista säädettäisiin, koska ne ovat tuotteita ja palveluja, joiden luotettavuudella on merkittävä rooli turvallisuusluokitellun tiedon suojaamisessa ja joita valmistajien on mahdollista tarjota osaksi tietojärjestelmiä ja tietoliikennejärjestelyjä.

Pykälään lisättäisiin uusi *2 momentti*, jossa säädettäisiin, että arviointilain säännöksiä sovellettaisiin arviointiviranomaisten menettelyyn myös kansainvälisten tietoturvallisuusvelvoitteiden mukaisissa määrättyjen turvallisuusviranomaisten tehtävissä, ellei kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa, EU:n tai Naton turvallisuussäännöissä tai kahdenvälisissä tietoturvallisuussopimuksissa toisin säädetä. Kahdenväliset tietoturvallisuussopimukset ovat laintasoisia valtiosopimuksia. Siten myös kansainvälisten tietoturvallisuusvelvoitteiden täyttämiseksi tehtävissä arvioinneissa sovellettaisiin arviointilain menettelysäännöksiä hakemuksen vireillepanosta, arviointiperusteiden määrittämisestä ja arviointiraportin, lausunnon tai päätöksen antamisesta ja muutoksenhausta siltä osin, kun menettelystä ei säädetä toisin kansainvälisiä tietoturvallisuusvelvoitteita koskevissa säädöksissä.

Pykälän *3 momentti* vastaisi muuten voimassa olevaa 2 momenttia, mutta toimivaltaisen viranomaisen nimeksi muutettaisiin Liikenne- ja viestintävirasto. Kyse on teknisluonteisesta muutoksesta. Liikenne- ja viestintäministeriön hallinnonalalla tehdyn virastouudistuksen myötä Viestintävirasto lakkasi olemasta 1.1.2019 alkaen, ja uutena viestintähallinnon viranomaisena toimii Liikenne- ja viestintävirasto.

2 § *Määritelmät.* Pykälässä säädetään laissa käytetyistä määritelmistä. Pykälää muutettaisiin siten, että sen 2 ja 3 kohdan määritelmät päivitettäisiin ja pykälään lisättäisiin uudet kohdat 5–10.

Pykälän *2 kohtaa* muutettaisiin siten, että siinä säädettyä tietoliikennejärjestelyn määritelmää täsmennettäisiin. Tietoliikennejärjestely vastaisi voimassa olevaa määritelmää, sillä erotuksella, että määritelmään lisättäisiin tiedonsiirtoverkkoon, tiedonsiirtolaitteisiin, ohjelmistoihin ja muihin tietojenkäsittelyyn sekä niihin liittyviin menettelyihin koostuvat kokonaisjärjestelyt. Muutoksella täsmennettäisiin sitä, että tietojenkäsittelyn järjestelyihin voivat sisältyä tiedonsiirtoverkkojen ja -laitteiden sekä ohjelmistojen ja muun tietojenkäsittelyn lisäksi myös näihin välittömästi liittyvät hallinnolliset, toiminnalliset ja tekniset menettelyt, jotka on kuvattu esimerkiksi organisaation tietoturvallisuusperiaatteissa, -määräyksissä ja -ohjeissa. Tietoliikennejärjestely ja tietojärjestelmä ovat kompleksisia kokonaisuuksia, joiden tarkkarajaista eroa on vaikea määrittää. Tietojärjestelmä ja tietoliikennejärjestely voivat sisältää turvallisuuskriittisiä ratkaisuja.

Pykälän *3 kohtaa* muutettaisiin siten, että viranomaisen määritelmää laajennettaisiin siten, että laissa tarkoitettuja viranomaisia olisivat kaikki viranomaisten toiminnan julkisuudesta annetun lain (621/1999), jäljempänä *julkisuuslaki*, 4 §:n 1 momentissa tarkoitetut viranomaiset. Tämä lisäisi arviointilaissa tarkoitettuihin viranomaisiin lain tai asetuksen taikka julkisuuslain 1, 2 tai 7 kohdassa tarkoitetun viranomaisen päätöksen perusteella tiettyä tehtävää itsenäisesti hoitamaan asetetut lautakunnat, neuvottelukunnat, komiteat, toimikunnat, työryhmät, toimitusmiehet sekä hyvinvointialueen ja hyvinvointiyhtymän, kunnan ja kuntayhtymän tilintarkastajat sekä muut niihin verrattavat toimielimet sekä lain tai asetuksen taikka lain tai asetuksen nojalla annetun säännöksen tai määräyksen perusteella julkista tehtävää hoitavat yhteisöt, laitokset, säätiöt ja yksityiset henkilöt niiden käyttäessä julkista valtaa. Tiedonhallintalaki koskee myös näitä toimijoita ja ne voivat käsitellä tietojärjestelmissä ja tietoliikennejärjestelyissä korkeimpiin turvallisuusluokkiin luokiteltuja tietoja, jolloin niiden tulisi myös noudattaa arviointilain velvoitteita kyseisten järjestelmien arvioinnista.

Pykälään lisättäisiin uusi *5 kohta*, jossa säädettäisiin tietoturvallisuuden määritelmästä. Tietoturvallisuudella tarkoitettaisiin tiedon saatavuuden, eheyden ja luottamuksellisuuden suojaamista hallinnollisilla, toiminnallisilla ja teknisillä toimenpiteillä. Määritelmän hallinnollisia, teknisiä ja muita toimenpiteitä voisivat esimerkiksi olla tiedonhallintalaissa tarkoitetut tietoturvallisuustoimenpiteet.

Tietoturvallisuudella tarkoitetaan yleisesti menettelyjä, joiden avulla turvataan tiedon luottamuksellisuus eli tietosisällön suojaaminen oikeudettomalta käytöltä, tiedon eheys eli muuttumattomuus sekä tiedon saatavuus huomioiden mahdolliset tiedon luottamuksellisuudesta aiheutuvat saatavuuden rajoitukset. Tietoturvallisuus on huomioitava kaikessa tiedon käsittelyssä tiedon koko elinkaaren ajan. Tiedon käsittelyllä tarkoitetaan tiedon tai asiakirjan vastaanottamista, laatimista, tallentamista, katselua, muuttamista, luovuttamista, kopiointia, siirtoa, välittämistä, tuhoamista, säilyttämistä ja arkistointia sekä muuta tietoon tai asiakirjaan kohdistuvaa toimenpidettä.

Tietoturvallisuuden tulisi olla sisäänrakennettua tietojärjestelmissä ja tietoliikennejärjestelyissä. Tietoturvallisuuden toteuttamiseksi käytetään hallinnollisia, toiminnallisia, fyysisiä ja teknisiä menettelyjä. Niitä ovat esimerkiksi hallinnolliset tietoturvallisuusperiaatteet ja tietojen käsittelyyn liittyvät hallinnolliset menettelytapavaatimukset, yritysten ja henkilöiden turvallisuuden selvittäminen, turvallisuussopimukset, tilaturvallisuus, tietotekniset toteutukset ja turvallisuuskontrollit sekä turvallisuuskriittiset ratkaisut.

Pykälään lisättäisiin uusi *6 kohta*, jossa säädettäisiin uudesta varautumisen määritelmästä. Varautumisella tarkoitettaisiin toimia, joilla huolehditaan tietojärjestelmien ja tietoliikennejärjestelyjen toiminnan jatkuminen normaaliolojen häiriötilanteissa sekä valmiuslain mukaisissa poikkeusoloissa. Määritelmän mukaisia varautumistoimia olisivat esimerkiksi organisaatiossa toteutettuun riskiarviointiin perustuva jatkuvuudenhallinta- ja valmiussuunnitelmien valmistelu, ylläpito ja harjoittelu sekä muut häiriötilanteiden ja kriisien ehkäisemiseksi sekä niissä toimimiseksi ja häiriötilanteista ja kriiseistä toipumiseksi tehdyt toimenpiteet kuten hallinnon yhteisesti johdetussa suunnittelussa hyödynnettävät strategia-asiakirjat kuten Yhteiskunnan turvallisuusstrategia ja Kansalliseen riskiarvio. Tiedonhallintayksikön varautumisvelvoitteesta säädetään tiedonhallintalain 13 a § 3 momentissa, jonka mukaan tiedonhallintayksikön on riskiarvioinnin perusteella valmiussuunnitelmin ja häiriötilanteissa tapahtuvan toiminnan etukäteisvalmisteluin sekä muilla toimenpiteillä huolehdittava, että sen tietoaineistojen käsittely, tietojärjestelmien hyödyntäminen ja niihin perustuva toiminta jatkuvat mahdollisimman häiriöttömästi normaaliolojen häiriötilanteissa sekä valmiuslaissa tarkoitetuissa poikkeusoloissa. Valmiuslaissa viranomaisten varautumisvelvollisuudesta poikkeusoloissa säädetään luvussa 3.

Pykälään lisättäisiin uusi *7 kohta*, jossa säädettäisiin tietoturvallisuuden arviointilaitoksen määritelmästä. Tietoturvallisuuden arviointilaitoksella tarkoitettaisiin arviointilaitoslain mukaisesti Liikenne- ja viestintäviraston hyväksymää yritystä, yhteisöä tai viranomaista, joka tarjoaa arviointipalveluita. Määritelmä vastaisi voimassa olevan lain 3 § viittausta arviointilaitoksiin ja arviointilaitoslakiin.

Pykälään lisättäisiin uusi *8 kohta*, jossa säädettäisiin turvallisuusluokan määritelmästä. Turvallisuusluokan määritelmä seuraisi tiedonhallintalain 18 §:ssä säädetystä turvallisuusluokitteluvelvoitteesta. Määritelmällä tarkoitettaisiin tiedonhallintalain asetuksenantovaltuuden nojalla annetun turvallisuusluokitteluasetuksen 3 §:ssä säädettyjä turvallisuusluokkia I, II, III ja IV, jotka ovat olleet voimassa 1.1.2020 alkaen.

Pykälään lisättäisiin uusi *9 kohta*, jossa säädettäisiin turvallisuuskriittisen ratkaisun määritelmästä. Turvallisuuskriittisellä ratkaisulla tarkoitettaisiin salaus-, hajasäteilysuojaus- ja muuta tieto- ja viestintäteknistä ratkaisua, jolla suojataan turvallisuusluokiteltua tietoa tietojärjestelmissä ja tietoliikennejärjestelyissä. Ratkaisulla tarkoitettaisiin tuotetta, palvelua tai toteutusta, jota käytetään tietojärjestelmässä tai tietoliikennejärjestelyssä käsiteltävän tiedon suojaamisessa mukaan lukien tietojen säilyttäminen ja siirtäminen tietoliikenneyhteydellä tietojärjestelmien tai tietoliikennejärjestelmien välillä. Määritelmä olisi teknologiariippumaton. Turvallisuuskriittistä ratkaisua ei tyypillisesti pystytä korvaamaan muilla suojaustoimenpiteillä. Salausratkaisu voi olla esimerkiksi salauslaite tai -ohjelmisto. Hajasäteilysuojaus voidaan toteuttaa esimerkiksi tilaratkaisuilla ja laitteiden suojaamisella. Turvallisuuskriittisiä ratkaisuja ovat myös esimerkiksi yhdyskäytävät.

Pykälään lisättäisiin uusi *10 kohta*, jossa säädettäisiin uudesta turvallisuuskriittisen ratkaisun valmistajan määritelmästä. Turvallisuuskriittisen ratkaisun valmistajalla tarkoitettaisiin yritystä, joka vastaa turvallisuuskriittisestä ratkaisusta koko sen elinkaaren ajan kehittämisestä ylläpitoon. Toisin sanoen yritys vastaa niistä toimenpiteistä, joilla on merkitystä ratkaisun luotettavuudelle turvallisuusluokitellun tiedon suojaamisessa. Turvallisuuskriittinen ratkaisu voi koostua useista erilaisista elementeistä tai komponenteista ja on tyypillistä, että valmistaja hankkii ratkaisuun elementtejä, komponentteja tai toimintoja useilta toimijoilta. Yritys vastaa koko toimitusketjun luotettavuudesta mukaan lukien alihankittujen osien luotettavuudesta.

Yrityksellä tarkoitettaisiin elinkeinotoimintaa harjoittavaa luonnollista henkilöä tai muuta yksikköä, joka yritys- ja yhteisötietolain (244/2001) 3 §:n 1 momentin 1–3 kohdan mukaan on rekisteröitävä yritys- ja yhteisötietojärjestelmään. Kyseessä voisi siis olla 1) elinkeinotoimintaa harjoittava luonnollinen henkilö ja kuolinpesä, 2) avoin yhtiö, kommandiittiyhtiö, osakeyhtiö, osuuskunta, yhdistys, säätiö ja muu yksityisoikeudellinen oikeushenkilö tai 3) valtio ja sen laitos, kunta, kuntayhtymä, seurakunta ja muu uskonnollinen yhdyskunta sekä muu julkisoikeudellinen oikeushenkilö. Sen sijaan lain 3§:n pykälän 4–5 kohtien mukaiset ulkomaisen yhteisön tai säätiön Suomessa oleva sivuliike tai eurooppayhtiö, eurooppaosuuskunta ja eurooppalainen taloudellinen etuyhtymä eivät käytännössä tulisi kysymykseen valmistuksen kotimaisuusedellytysten ja yritysturvallisuusselvityksessä tehtävän ulkomaisen vaikutuksen mahdollisuuden poissulkemisen johdosta.

3 § *Tietoturvallisuuden ja varautumisen arviointi*. Pykälän otsikko muutettaisiin tietoturvallisuuden arviointipalvelujen käyttämisestä tietoturvallisuuden ja varautumisen arvioinniksi. Uudistettu pykälä sisältäisi säännökset arviointimenettelyistä, valtionhallinnon viranomaisia koskevista arviointivelvoitteista sekä kaikkia viranomaisia koskevista velvoitteista hakea arviointiviranomaisen arviointia korkeimpien turvallisuusluokkien tietoja käsitteleville järjestelmilleen. Lisäksi pykälässä säädettäisiin mahdollisuudesta hakea arviointiviranomaisen

hyväksyntää vaatimukset täyttävälle tietojärjestelmälle tai tietoliikennejärjestelylle kansainvälisissä tietoturvallisuustilanteissa.

Pykälän *1 momenttia* muutettaisiin siten, että siinä säädettäisiin viranomaisen käytettävissä olevista arviointimenettelyistä. Arviointimenettelyjä ehdotetaan lisättäväksi nykyisestä siten, että viranomaisen toteuttama itsearviointi ja viranomaisen toimeksiannosta palveluntarjoajan toteuttama arviointi olisivat arviointimenettelyjä voimassa olevan lain mukaisten tietoturvallisuuden arviointilaitoksen toteuttaman arvioinnin ja arviointiviranomaisen toteuttaman arvioinnin lisäksi.

Momentin *1 kohdassa* säädettäisiin viranomaisen toteuttamasta itsearvioinnista yhtenä viranomaisen käytettävissä olevista arviointimenettelyistä. Itsearvioinnilla tarkoitettaisiin viranomaisen itsenäisesti toteuttamaa sen määräämisvallassa olevan tai hankittavaksi suunnitteleman tietojärjestelmän tai tietoliikennejärjestelyn arviointia. Itsearviointi voisi myös olla usean viranomaisen yhdessä toteuttama arviointi tai vertaisarviointi. Itsearviointeja toteuttavan viranomaisen tulisi huolehtia, että sillä on itsearvioinneissa tarvittava osaaminen tietoturvallisuuden ja varautumisen toteuttamisesta.

Valtionhallinnon viranomainen voisi toteuttaa ehdotuksen mukaisen itsearvioinnin ensimmäisen kerran riskiarvioinnin perusteella esimerkiksi tiedonhallintalain 9 § mukaisen tiedonhallinnan muutosta koskevan lausuntomenettelyn yhteydessä.

Momentin *2 kohdassa* säädettäisiin viranomaisen toimeksiannosta palveluntarjoajan toteuttamasta arvioinnista yhtenä arviointimenettelynä. Viranomaisilla ei välttämättä ole osaamista ja resursseja etenkään korkeampiriskisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden ja varautumisen perusteelliseen arviointiin. Siten tietoturvallisuuden ja varautumisen arviointien toteuttamisen mahdollistaminen viranomaisen toimeksiannosta olisi perusteltua. Viranomaisen toimeksiannosta toteutetulla arvioinnilla tarkoitettaisiin muun kuin tietoturvallisuuden arviointilaitoksen tai muun viranomaisen kuin ehdotetun 3 a §:ssä tarkoitetun arviointiviranomaisen toteuttamaa arviointia.

Julkisia ja salassa pidettäviä tietoja käsittelevien, vähäriskisten tietojärjestelmien pääsääntöinen arviointien toteutustapa olisi viranomaisen itsearviointi tai viranomaisen toimeksiannosta toteutettu arviointi. Arviointien toteuttamisesta aiheutuvien kustannusten hillitsemiseksi viranomaisten tulisi mahdollisuuksien mukaan hankkia arviointeja yhdessä.

Momentin *3 ja 4 kohdassa* säädettäisiin arviointimenettelyiksi tietoturvallisuuden arviointilaitoksen toteuttama arviointi sekä arviointiviranomaisen toteuttama arviointi. Nämä arviointimenettelyt vastaisivat voimassa olevan lain 3 §:ssä säädettyjä sallittuja arviointimenettelyjä.

Pykälään lisättäisiin uusi *2 momentti*, jossa valtionhallinnon viranomaiselle säädettäisiin velvollisuus arvioida tietojärjestelmiensä ja tietoliikennejärjestelyjensä tietoturvallisuutta ja varautumista riskiarvioinnin perusteella toteuttaen vähintään itsearviointeja. Arviointimenettelynä olisi käytettävä 1 momentissa säädettyjä menettelyjä.

Valtionhallinnon viranomainen valitsisi riskiarvioinnin perusteella millä menettelyllä julkisia ja salassa pidettäviä tietoja käsittelevien tietojärjestelmien ja tietoliikennejärjestelyjen turvallisuutta ja varautumista arvioidaan, kuka on arvioinnin toteuttaja, mitä vaatimuksia ja kriteerejä arvioinnissa käytetään, ja miten arvioinneista huolehditaan tietojärjestelmän ja tietoliikennejärjestelyn elinkaaren ajan. Tietojärjestelmän tai tietoliikennejärjestelyn eri osiin tai osa-alueisiin voitaisiin valita erilainen arviointimenettely. Arviointimenettelyä valittaessa voitaisiin huomioida arvioinnin taloudellinen ja tehokas toteuttaminen, arvioitavassa tietojärjestelmässä tai

tietoliikennejärjestelyssä käsiteltävien tietojen luottamuksellisuus-, eheys-, saatavuus- ja jatkuvuudenhallintavaatimukset sekä salassapitovaatimukset ja turvallisuusluokat, arvioitavan järjestelmän tarkoituksenmukaiseen tuotantotapaan kohdistuvat vaatimukset ja tekninen laajuus, toteutustapa ja liitynnät muihin järjestelmiin sekä ulkopuolisen erityisosaamisen tarve suhteessa viranomaisen käytettävissä oleviin resursseihin. Arviointimenettelyn valintaa rajoittaisivat kuitenkin 3, 4, 5 ja 6 momentissa säädettäväksi ehdotetut rajoitteet.

Ehdotettua riskiarviointiin perustuvaa velvoitetta ei olisi tarkoitus sitoa ainoastaan tietojärjestelmän ja tietoliikennejärjestelyn käyttöönottoon, vaan arviointeja olisi tarkoituksenmukaista toteuttaa säännöllisesti tietojärjestelmien ja tietoliikennejärjestelyjen elinkaaren ajan. Tiedonhallintalain 13 §:n mukaisesti tiedonhallintayksikön on varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan sekä selvitettävä olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti. Järjestelmien elinkaaren ajan toteutetut arvioinnit lisäisivät viranomaisen tietoja järjestelmien riskeistä. Arvioinnissa tunnistettujen riskien hallinnan kautta on mahdollista vahvistaa tietoturvallisuutta ja varautumista, ja siten koko toimintaympäristön kykyä sietää ja vastustaa tietoturvahäiriöitä ja -loukkauksia sekä muita järjestelmiin haitallisesti vaikuttavia häiriöitä ja palautua niistä.

Muutkin kuin valtiohallinnon viranomaiset, esimerkiksi kunnat, voisivat hyödyntää arviointilain mukaisia tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden ja varautumisen arviointimenettelyjä osana tiedonhallintalain 13§:n mukaista tietojenkäsittelyn riskien selvittämistä ja tietoturvallisuustoimenpiteiden mitoittamista. Tietoturvallisuuden ja varautumisen arviointien toteuttaminen tai hankkiminen tukisi viranomaisten tietojenkäsittelyyn liittyvää riskienhallintaa. Muita kuin valtionhallinnon viranomaisia koskisivat myös ehdotetun pykälän 3–7 momentit.

Pykälään lisättäisiin uusi *3 momentti,* jossa säädettäisiin kaikkien viranomaisen velvollisuudesta varmistua turvallisuusluokkaan I tai II luokiteltuja tietoja käsittelevien tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuudesta ja varautumisesta pyytämällä niille arviointiviranomaisen arviointi. Arviointivelvoite koskisi sekä tietoturvallisuutta että varautumisen arviointia. Arvioinnin uusimisen tarve tulisi punnita riskiarvioin perusteella esimerkiksi muutosten yhteydessä. Velvollisuus koskisi pääsääntöisesti valtionhallinnon viranomaisia, mutta myös muita viranomaisia, jos ne käsittelisivät näiden turvallisuusluokkien tietoa tietojärjestelmissään tai tietoliikennejärjestelyissään. Tietojen käsittelyllä tarkoitettaisiin 2 §:n 5 kohdan perusteluihin kirjatusti myös tietojen säilyttämistä ja arkistointia, joten velvoite koskisi myös viranomaisia, joita ei koske tiedonhallintalain turvallisuusluokitteluvelvoite, mutta jotka säilyttäisivät tai arkistoisivat turvallisuusluokan I tai II tietoja tietojärjestelmissä tai tietoliikennejärjestelyissä.

Pykälään lisättäisiin uusi *4 momentti*, jonka nojalla kaikkien viranomaisten olisi pyydettävä tai hankittava turvallisuusluokkaan III luokiteltuja tietoja käsittelevälle tietojärjestelmälle tai tietoliikennejärjestelylle arviointiviranomaisen tai tietoturvallisuuden arviointilaitoksen arviointi, ellei se ole viranomaisen riskiarvion perusteella tarpeetonta. Arviointivelvoite koskisi sekä tietoturvallisuutta että varautumisen arviointia. Viranomaisen toteuttamassa riskiarviossa tulisi huomioida samat seikat, kuin 2 momentin mukaisessa riskiarviossa. Arvioitavan järjestelmän tekninen laajuus voi vaihdella ja viranomaisella voi itsellään olla tarvittavat resurssit esimerkiksi työaseman arviointiin tai käyttöpisteissä tehtävien muutosten arviointiin. Myös varautumisen toimenpiteiden arviointiin viranomaisella voi itsellään olla hyvät valmiudet ja paras asiantuntemus omaan toimintaansa liittyvien järjestelmien merkityksestä varautumisen kannalta. Jos viranomainen päättää riskiarvion perusteella olla pyytämättä arviointiviranomaisen tai hankittamatta tietoturvallisuuden arviointilaitoksen arviointia, tulisi päätös tehdä viranomaisen sisäisen ratkaisuvallan mukaisesti, mikä usein edellyttää johdon hyväksyntää. Pykälän 3

momentin ehdotuksen tavoin, 4 momentin ehdotus koskisi pääsääntöisesti valtionhallinnon viranomaisia, mutta myös muita viranomaisia, jos ne käsittelisivät näiden turvallisuusluokkien tietoa tietojärjestelmissään tai tietoliikennejärjestelyissään.

Pykälään lisättäisiin uusi *5 momentti*, jossa säädettäisiin, että viranomainen voisi toimeksiannosta hankkia palvelutarjoajalta arvioinnin tietojärjestelmistä ja tietoliikennejärjestelyistä, joissa käsitellään julkisia, salassa pidettäviä tai korkeintaan turvallisuusluokan IV tietoja. Rajoitus koskisi kaikki viranomaisia niiden toteuttaessa tämän lain mukaisia arviointeja. Korkeimpia turvallisuusluokkia käsittelevien tietojärjestelmien ja tietoliikennejärjestelyjen arviointi vaatii syvällistä osaamista ja erityisiä tiloja ja välineitä. Jos palvelutarjoaja tahtoisi erikoistua turvallisuusluokkaa III käsittelevien tietojärjestelmien ja tietoliikennejärjestelyjen arviointiin, se voisi hakeutua tietoturvallisuuden arviointilaitokseksi.

Pykälän 5 momentissa säädettäisiin myös, että viranomaisen olisi varmistuttava 1 momentin 2 kohdassa tarkoitettuja arviointipalveluja hankkiessaan palveluntarjoajan luotettavuudesta toimeksiannon edellyttämässä laajuudessa. Säännöksellä pyrittäisiin varmistamaan, että viranomaisen tietojärjestelmiä ja tietoliikennejärjestelmiä voisivat arvioida ainoastaan luotettavat ulkopuoliset toimijat.

Arviointitoimeksiannot, arvioitavat tietojärjestelmät ja tietoliikennejärjestelyt sekä toimeksiannon yhteydessä palveluntarjoajan saamat viranomaisen tiedot voivat vaihdella merkittävästi, joten luotettavuuden varmistamiseen käytettävät riittävät keinot voisivat olla erilaisia. Viranomainen voisi hankintalainsäädännön mahdollistamalla tavalla asettaa tietojen suojaamiseen sekä tarjoajien soveltuvuuteen liittyviä vaatimuksia. Lisäksi viranomainen voisi varmistaa palveluntarjoajan luotettavuutta selvittämällä saatavilla olevia tietoja palveluntarjoajasta, sen vastuuhenkilöistä ja omistajista hyödyntämällä julkisia ja viranomaisten rekisteritietoja sekä luotto- ja yritystietopalveluja. Turvallisuuden varmistamisessa viranomainen voisi hyödyntää hankintojen tietoturvallisuusvaatimusten asettamista koskevia suosituksia, ohjeita, määräyksiä ja työkaluja sekä yhteishankintajärjestelyjä.

Palveluntarjoajan luotettavuuden varmistaminen on tärkeää toimeksiannoissa, joissa palveluntarjoaja käsittelee salassa pidettäviä tietoja, etenkin silloin, jos käsiteltävät tiedot ovat palvelutarjoajan arvioinneille korkeinta mahdollista turvallisuusluokkaa IV. Tällöin arviointipalvelujen hankinnassa ja palveluja koskevissa sopimuksissa olisi otettava huolellisesti huomioon kansalliseen turvallisuuteen liittyvät riskit. Valtionhallinnon viranomaisen tulisi edellytysten täyttyessä ja tarvittaessa teettää turvallisuusselvitykset arviointitehtäviä suorittavista yrityksistä ja henkilöistä, jotka saisivat pääsyn viranomaisen turvallisuusluokiteltuihin tietoihin toimeksiannon aikana. Yritysturvallisuusselvityksen ja henkilöturvallisuusselvityksen laatimisen edellytyksistä säädetään turvallisuusselvityslaissa.

Viranomaisen olisi huolehdittava myös tietojen suojaamisesta. Julkisuuslain 26 §:n 3 momentissa säädetään velvollisuudesta ennakolta varmistua, että tietojen salassapidosta ja suojaamisesta huolehditaan asianmukaisesti. Turvallisuusluokitteluasetuksen 6 §:n 1 momentin mukaisesti valtionhallinnon viranomaisen on ennakolta varmistuttava siitä, että turvallisuusluokitellun asiakirjan suojaamisesta huolehditaan asianmukaisesti, jos se antaa turvallisuusluokitellun asiakirjan muulle kuin valtionhallinnon viranomaiselle.

Lisäksi viranomaisen tulisi huomioida toisten valtioiden kanssa tehdyt tietoturvallisuussopimukset, jotka perustuvat vastavuoroiseen suojaan. Toisen valtion ”RESTRICTED” tietoa voidaan pääsääntöisesti Suomessa käsitellä kansallisissa järjestelmissä, jotka täyttävät turvallisuusluokan IV vaatimukset ja muut kansainvälisen erityissuojattavan tiedon vaatimukset. Sen sijaan EU:n ja Naton turvallisuusluokiteltua tiedon käsittely on sallittua ainoastaan tietojärjestelmissä

ja tietoliikennejärjestelyissä, jotka on akkreditoitu EU:n tai Naton turvallisuussääntöjen mukaisesti.

Viranomaisen tulisi varmistaa tietojen suojaaminen ja tietoturvallisuus hankinnan kaikissa vaiheissa. Palveluntarjoajan kanssa tehtävään sopimukseen tulisi sisällyttää tietoturvallisuutta koskevat sopimusehdot ja vaatimukset. Viranomainen voisi hyödyntää hankintojen tietoturvallisuudesta annettua ohjeistusta kuten Tiedonhallintalautakunnan suositusta tietoturvallisuudesta hankinnoissa (2023:57). Arviointitoimeksiannoissa tulisi erityistä huomiota kiinnittää siihen, missä tietojärjestelmissä ja tiloissa palveluntarjoaja käsittelee viranomaisen salassa pidettäviä tai turvallisuusluokiteltuja tietoja.

Viranomainen voisi käyttää yhteishankintajärjestelyä, johon sisältyisi palveluntarjoajalle asetetut turvallisuusvaatimukset ja turvallisuussopimus. Lain julkisista puolustus- ja turvallisuushankinnoista (1531/2011) tarkoittamissa tilanteissa viranomainen voisi toteuttaa arviointipalvelun hankinnan puolustus- ja turvallisuushankintana.

Pykälään lisättäisiin uusi *6 momentti,* jossa säädettäisiin voimassa olevaan lakiin verraten uutena rajoituksena, että viranomainen voisi hankkia tietoturvallisuuden arviointilaitokselta arvioinnin tietojärjestelmälle ja tietoliikennejärjestelylle, joissa käsitellään julkisia, salassa pidettäviä tai turvallisuusluokkaan IV tai III luokiteltuja tietoja. Rajoitus koskisi kaikkia viranomaisia niiden toteuttaessa tämän lain mukaisia arviointeja. Tietoturvallisuuden arviointilaitoksista ja niiden riippumattomuudesta, luotettavuudesta ja pätevyydestä säädetään arviointilaitoslaissa. Tietoturvallisuuden arviointilaitokset on arvioitu turvallisiksi ja osaaviksi arvioida turvallisuusluokkaa III käsitteleviä tietojärjestelmiä ja tietoliikennejärjestelyitä.

Pykälään lisättäisiin uusi *7 momentti,* jossa säädettäisiin viranomaisen mahdollisuudesta pyytää arviointiviranomaisen hyväksyntää tietojärjestelmälleen tai tietoliikennejärjestelylleen osoittaakseen tietoturvallisuutta koskevien vaatimusten täyttymisen Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain tarkoittamissa tilanteissa tai jos muutoin kansainvälinen yhteistyö sitä edellyttää taikka jos vaatimustenmukaisuuden osoittamisesta erikseen säädetään.

Hyväksynnän tarve ja oikeus hakea hyväksyntää liittyisi kansainvälisistä tietoturvallisuusvelvoitteista tai kansainvälisestä yhteistyöstä johtuvaan tai säädettyyn velvollisuuteen osoittaa tietoturvallisuusvaatimusten täyttyminen riippumattoman arviointielimen toimesta kolmannelle tai kolmansille osapuolille. Hyväksyntään tähtäävä arviointi edellyttäisi, että arviointiprosessia jatketaan, kunnes arvioinnissa havaittujen poikkeamien korjaamisesta on huolehdittu, jolloin arviointiviranomainen laatisi ehdotetun 8 §:n 2 momentin mukaisen hyväksyntäpäätöksen tai -lausunnon siitä, että arvioinnin kohden täyttää arviointiperusteina käytetyt vaatimukset. Riippumattoman arviointiviranomaisen tekemän arvioinnin perusteella annettu hyväksyntäpäätös tai -lausunto vaatimusten täyttymisestä osoittaisi, että arviointiviranomainen on hyväksynyt säädettyjen ja riskiarviointiin perustuvien arviointiperusteiden valinnan ja arviointikohteen teknisen määrittelyn rajauksen. Vaatimusten täyttymisellä ja vaatimusten täyttymisen osoittamisella tarkoitettaisiin, että arviointiviranomainen on todennut arviointiprosessin perusteella, että arvioinnissa havaituista poikkeamista on huolehdittu siten, että arvioinnin pyytäneellä viranomaisella on edellytykset päättää jäännösriskin käsittelystä ilman, että tämä vaarantaa kolmannen osapuolen perustellun luottamuksen järjestelmään.

3 a § *Arviointiviranomaiset.* Lakiin lisättäisiin uusi 3 a §, jossa säädettäisiin arviointiviranomaisista.

Pykälän *1 momentissa* säädettäisiin arviointiviranomaisista, joita olisivat Liikenne- ja viestintävirasto ja Pääesikunnan määrätty turvallisuusviranomainen (DSA Designated Security

Authority). Liikenne- ja viestintävirasto hoitaa arviointitehtäviä jo voimassa olevan lain nojalla, mutta Pääesikunnan määrätylle turvallisuusviranomaiselle tehtävä olisi uusi. Pääesikunnan määrätyn turvallisuusviranomaisen arviointitehtäviä voisi myös hoitaa sen nimeämä Puolustusvoimien palkattuun henkilöstöön kuuluvaa henkilö. Nimetyt henkilöt olisivat tehtäviä hoitaessaan Pääesikunnan määrätyn turvallisuusviranomaisen ohjauksessa ja valvonnassa. Puolustusvoimien arviointitehtävä on tarpeen säätää nimenomaisesti Pääesikunnan määrätylle turvallisuusviranomaiselle toiminnan riippumattomuuden varmistamiseksi. Pääesikunnan määrätyn turvallisuusviranomaisen tehtävistä säädetään laissa kansainvälisistä tietoturvallisuusvelvoitteista.

Pykälän *2 momentissa* säädettäisiin, että arviointiviranomaiselta edellytettäisiin organisatorista ja päätöksenteon riippumattomuutta sille kuuluvien arviointitehtävien hoitamisessa. Arviointiviranomaisen tulisi tuottaa objektiivista arvioinnissa hankkimaansa ja saamaansa selvityksiin perustuvaa tietoa arvioinnin kohteesta. Arviointiviranomaisen tulisi siten olla tehtävissään riippumaton arvioinnin kohteen päätöksenteosta eikä arvioinninkohde saisi voida vaikuttaa arviointiviranomaisen havaintoihin tai päätelmiin. Riippumattomuus voitaisiin varmistaa esimerkiksi viranomaisen työjärjestyksessä.

Riippumattomuuden edellytys koskee myös Pääesikunnan määrätyn turvallisuusviranomaisen nimeämää Puolustusvoimien palkattuun henkilöstöön kuuluvaa henkilöä. Tietoturvallisuuden ja varautumisen arviointitehtäviä eivät siten voisi hoitaa esimerkiksi samat henkilöt, jotka johtavat tai toteuttavat arvioitavan tietojärjestelmän tai tietoliikennejärjestelmän suunnittelua, rakentamista tai ylläpitoa.

Lisäksi pykälän 2 momentissa säädettäisiin, että arviointiviranomaisen on huolehdittava tehtävistään teknisen kehityksen edellyttämällä ammattitaidolla. Arviointiviranomaisen tulisi seurata teknistä kehitystä ja ylläpitää ja kehittää osaamistaan jatkuvasti arvioinnin kohteiden edellyttämällä tavalla.

Pykälän *3 momentissa* säädettäisiin, että arvioinnin tekeminen kuuluu Liikenne- ja viestintäviraston toimivaltaan, ellei arvioinnin tekeminen kuulu Pääesikunnan määrätyn turvallisuusviranomaisen toimivaltaa 4 momentin nojalla. Toimivaltainen arviointiviranomainen olisi siten pääsääntöisesti Liikenne- ja viestintävirasto ja tietoturvallisuuden ja varautumisen arvioinnit olisivat Liikenne- ja viestintäviraston tehtävänä, ellei arviointi kuuluisi 4 momentissa säädetyllä tavalla Pääesikunnan määrätylle turvallisuusviranomaiselle.

Pykälän *4 momentissa* säädettäisiin, että arvioinnin tekeminen kuuluu Pääesikunnan määrätyn turvallisuusviranomaisen toimivaltaan, jos arviointi koskee Puolustusvoimien omia järjestelmiä. Pääesikunnan määrätyn turvallisuusviranomaisen arviointi- ja hyväksyntäviranomaisen toimivalta ja tehtävät olisivat tarkoituksenmukaista rajata Puolustusvoimien omiin tietojärjestelmiin, jotta selkeä tehtävänjako säilyisi Liikenne- ja viestintäviraston kanssa ja vältettäisiin päällekkäisyyksiä. Pääesikunnan määrätty turvallisuusviranomainen toteuttaisi julkisia, salassa pidettäviä ja kaikkien turvallisuusluokkien tietoja käsittelevien omien tietojärjestelmiensä ja tietoliikennejärjestelyjensä tietoturvallisuuden ja varautumisen arviointeja sekä Puolustusvoimien omassa toiminnassa tarvitsemien turvallisuuskriittisten ratkaisujen arviointeja.

4 § *Arviointiviranomaisen tehtävät.* Pykälää ja sen otsikkoa muutettaisiin siten, että Viestintäviraston tehtävien sijaan pykälässä säädettäisiin arviointiviranomaisten tehtävistä.

Pykälän *1 momenttia* muutettaisiin siten, että siinä säädettäisiin tehtävistä, jotka ovat yhteisiä arviointiviranomaisille. Momentin 1 kohta vastaisi nykyistä 1 momentin 1 kohtaa muutettuna siten, että siihen lisättäisiin turvallisuuskriittisten ratkaisujen tietoturvallisuuden arviointi sekä

varautumisen arviointi uutena arviointitehtävänä. Momentin 2 kohdassa säädettäisiin arviointiviranomaisen tehtävästä antaa hyväksyntä vaatimukset täyttävästä tietojärjestelmästä tai tietoliikennejärjestelystä viranomaisen ehdotetun 3 § 7 momentin mukaisesta hakemuksesta. Momentin 3 kohta vastaisi nykyistä 1 momentin 2 kohtaa muutettuna siten, että siinä huomioitaisiin todistuksen sijaan arvioinnin tuloksena annettavat erimuotoiset asiakirjat eli arviointiraportti, hyväksyntäpäätös ja -lausunto.

Pykälän *2 momentissa* säädettäisiin tehtävistä, jotka olisi osoitettu vain Liikenne- ja viestintävirastolle. Momentin *1 kohdan* mukaan viraston tehtävänä olisi käsitellä Suomeen sijoittuneen valmistajien arviointipyynnöt turvallisuuskriittisten ratkaisujen vaatimuksenmukaisuudesta. Tämä olisi Liikenne- ja viestintävirastolle uusi tehtävä, jonka tarkoitus olisi mahdollistaa turvallisuuskriittisten ratkaisujen hyväksyntöjen pyytäminen valmistajille ja edistää suomalaisten tuotteiden tarjontaa ja saatavuutta turvallisuusluokitellun tiedon suojaamisessa.

Liikenne- ja viestintäviraston suorittaman arvioinnin tarkoituksena olisi saada Liikenne ja viestintäviraston hyväksyntä arvioitavan ratkaisun vaatimuksenmukaisuudesta. Hyväksyntä julkaistaisiin ehdotetun 8 c §:n mukaisessa luettelossa. Turvallisuuskriittisen ratkaisun arviointiin olisi sisällytettävä kaikkien sellaisten alihankkijoiden arviointi, joiden toimittamat osat ovat olennaisia ratkaisun luotettavuutta arvioitaessa. Valmistajan tekemän julkiseen hyväksyntään tähtäävän hakemuksen käsittelyssä olisi tarpeen arvioida valmistajan ja sen alihankkijoiden alkuperää, tuotekehitystä ja valmistusta ja itse ratkaisua. Valmistajan ja valmistuksen arviointi olisi tärkeä osa ratkaisun arviointia. Hajasäteily- eli TEMPEST-ratkaisujen valmistajan hyväksynnässä se olisi olennainen osa hyväksynnän sisältöä.

Suomeen sijoittuneella tarkoitettaisiin Suomeen sijoittautunutta yritystä, jonka valmistus on Suomessa ja johon ei liity ulkomaisen vaikutuksen riskiä. Hakemusten käsittelyn rajaamisella Suomeen sijoittuneen valmistajan Suomessa valmistettavaan ratkaisuun olisi tarkoitus rajata Liikenne- ja viestintäviraston julkiseen hyväksyntään tähtäävät arvioinnit sellaiseen kotimaiseen valmistukseen, jonka toteuttamista virasto pystyisi tosiasiassa arvioimaan ja seuraamaan. Sääntelyn tarkoitus olisi osaltaan edistää Suomessa käytäntöä, jota noudatetaan kansainvälisissä tietoturvallisuusvelvoitteissa ja jonka mukaan kukin valtio vastaa toimivaltansa alueella tapahtuvan valmistuksen arvioinnista. Erityisesti salausratkaisujen kohdalla käytännön taustalla olisi tarve varmistua siitä, ettei valmistukseen liity ei-toivottua ulkomaisen vaikutusvallan mahdollisesti aiheuttamia riskejä. Muiden kuin kotimaisten turvallisuuskriittisten ratkaisujen arviointi olisi osa tietojärjestelmien ja tietoliikennejärjestelyjen arviointia siten kuin 1 momentin 1 kohdassa säädettäisiin.

Momentin *2 kohdassa* säädettäisiin Liikenne- ja viestintäviraston neuvontatehtävästä. Liikenne- ja viestintävirasto antaisi tietojärjestelmien, tietoliikennejärjestelyjen ja turvallisuuskriittisten ratkaisujen tietoturvallisuustoimenpiteisiin ja tietoturvallisuuden arviointiin liittyvää neuvontaa. Kyseessä olisi hallintolain 8 §:ssä säädettyä yleistä viranomaisneuvontaa laajempi ja syvällistä tietoturvallisuuden asiantuntemusta edellyttävä neuvontatehtävä, joka liittyisi tietoturvallisuusuhkien tunnistamiseen, tietoturvallisuustoimenpiteisiin, -vaatimuksiin ja -käytäntöihin ja niiden soveltamiseen yleisesti tai tapauskohtaisesti. Tehtävä tukisi esimerkiksi tietojärjestelmien, tietoliikennejärjestelyjen ja turvallisuuskriittisten ratkaisujen kehitysprosesseja, joissa Liikenne- ja viestintävirasto on mukana suunnittelusta lähtien. Arvioinnin ennakointi ja suunnittelu on arvioinnin hakijan ja arviointiviranomaisen vuoropuhelua, jossa selvitetään arvioinnin kohteen turvallisuustavoitteet ja tekniseen toteutukseen liittyvät tiedot sekä arvioinnin kohteen toteutuksen suunnitellut aikataulut.

Liikenne- ja viestintäviraston neuvontatehtävä tukisi myös arviointilaitosten hyödyntämistä viranomaisen tietojärjestelmän tai tietoliikennejärjestelyn arvioinnissa. Liikenne- ja

viestintävirasto voisi antaa neuvontaa tietojärjestelmän ja tietoliikennejärjestelyn suunnitteluvaiheessa, arvioinnin kohdentamisessa ja arviointiperusteiden valinnassa, jolloin arviointilaitoksen arviointitehtävä voitaisiin suunnata tehokkaasti testaamiseen ja todentamiseen.

Momentin *3 kohta* vastaisi voimassa olevan pykälän 1 momentin 3 kohtaa, mutta siihen lisättäisiin tietoturvallisuuden tason selvittämisen lisäksi lain soveltamisalan laajenemisen mukaisesti varautuminen mahdollisten Liikenne- ja viestintäviraston tekemien selvityksen kohteeksi.

Momentin *4 kohdassa* säädettäisiin Liikenne- ja viestintäviraston uudesta tehtävästä ohjata ja valvoa hajasäteilysuojausratkaisuja valmistavan turvallisuuskriittisen ratkaisun valmistajan toimintaa ja antaa tarvittaessa päätös valmistuksen ja ratkaisun vaatimuksista. Tarkoituksena olisi edistää ehdotetun 7 b §:n mukaisesti hyväksytyn TEMPEST-yrityksen toiminnan edellytyksiä. Ohjausmalli olisi yhdenmukainen EU:n ja Naton turvallisuussääntöjen kanssa. Niissä edellytetään toimivaltaiselta viranomaiselta hyväksyttyjen TEMPEST-yritysten jatkuvaa valvontaa ja ohjausta. Ohjaus- ja valvonta loisi yrityksille edellytykset saavuttaa asiakkaiden luottamus toimintaan kansallisesti ja kansainvälisesti. Toiminnan yleiset ehdot tulisi asettaa ehdotetun 8 §:n 3 momentin mukaisessa hajasäteilysuojauksen valmistajaa koskevassa hyväksyntäpäätöksessä. Erilaisten toimenpiteiden ja vaatimusten tulkinnan ohjaus voisi pääsääntöisesti tapahtua neuvonnalla, mutta tarvittaessa Liikenne- ja viestintäviraston tulisi antaa päätös. Toimenpiteet voisivat koskea esimerkiksi jonkin tuotetyypin valmistuksessa edellytettävää tarkistusmittausten otosta.

Pykälän *3 momenttia* muutettaisiin siten, että lakiin lisättäisiin seikkoja, jotka viraston tulisi ottaa huomioon asettaessaan tehtäviään tärkeysjärjestykseen ja tehdessään päätöksen siitä, ottaako virasto haetun arvioinnin tehtäväksi. Virasto voisi myös ottaa haetun arvioinnin tehtäväksi vain osittain. Arvioinnin kohteen teknisestä määrittämisestä säädetään muutoin 7 §:ssä.

Liikenne- ja viestintävirastolla olisi yleinen toimivalta toteuttaa turvallisuusluokiteltuja tietoja käsittelevien tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arviointeja. Viraston tulisi jatkossakin huolehtia ensisijaisesti kansainvälisten tietoturvallisuusvelvoitteiden edellyttämistä arvioinneista. Liikenne ja viestintäviraston tulisi myös huomioida 3 § ehdotettu viranomaisten velvoite hakea turvallisuusluokkiin I ja II luokiteltua tietoa käsittelevien järjestelmien arviointia, ja ottaa tällaiset arvioinnin tehtäväkseen, ellei toimivalta ole Pääesikunnan määrätyllä turvallisuusviranomaisella. Sen lisäksi viraston tulisi priorisoida turvallisuusluokiteltua tietoa käsittelevien tietojärjestelmien ja tietoliikennejärjestelyjen arviointeja ottaen huomioon, onko arviointitehtävän toteuttamiseen saatavilla muita riippumattomia arviointitahoja kuten tietoturvallisuuden arviointilaitosta, jolla olisi pätevyys tehdä turvallisuusluokan III-IV tietoja käsittelevien tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden ja varautumisen arviointeja. Liikenne- ja viestintäviraston tehtävien tärkeysjärjestykseen asettamisessa huomioitaisiin lisäksi suomalaisten turvallisuuskriittisten ratkaisujen tarjonnan edistäminen, hakijoiden yhdenvertainen kohtelu ja vaikutus yhteiskunnan elintärkeiden toimintojen suojaamiseen.

Pykälän *4 momentti* vastaisi muutoin voimassa olevan pykälän 2 momenttia, mutta pyynnön sijaan käytettäisiin termiä hakemus.

4 a § *Arviointiviranomaista avustava tehtävä.* Lakiin lisättäisiin uusi 4 a §, jossa säädettäisiin arviointiviranomaista avustavista tehtävistä.

Pykälän *1 momentissa* arviointiviranomaisille säädettäisiin nykyiseen lakiin nähden uudesta mahdollisuudesta käyttää yksityisiä luonnollisia tai oikeushenkilöitä eli yrityksiä tai yhteisöjä viranomaisarviointien tukena. Arviointiviranomainen ei kuitenkaan voisi siirtää

arviointitehtävää kokonaisuudessaan ulkopuolisen luonnollisen tai oikeushenkilön suoritettavaksi. Uudet viranomaisarviointitehtävät edellyttävät riittäviä henkilöresursseja. Henkilöresurssien hankkiminen yksityisilta markkinoilta tulisi mahdollistaa viranomaisarviointien resurssien varmistamiseksi. Arviointiviranomaisten voi olla vaikeaa saada rekrytoitua riittävästi henkilöstöä arviointitehtäviin, sillä osaavia henkilöresursseja on niukasti.

Arviointiin osallistuvalla ulkopuolisella asiantuntijalla olisi oltava sellainen koulutus ja kokemus, kuin arvioinnin suorittamiseksi on tarpeen. Arviointiviranomainen voisi ulkopuoliselle asiantuntijalle osoitetussa toimeksiannossa määritellä, millaista pätevyyttä asiantuntijalta edellytetään ja mitä arviointikriteeristöä asiantuntijan tulee käyttää. Selvityksen edellytysten täyttyessä ja tarvittaessa kansallisen turvallisuuden tai arvioinnin kohteessa käsiteltävien tietojen turvallisuusluokittelun tai muun yhteiskunnan turvallisuuteen liittyvän syyn sitä edellyttäessä, olisi harkittava turvallisuusselvityslaissa tarkoitetun yritysturvallisuusselvityksen tai henkilöturvallisuusselvityksen edellyttämistä arvioinnin suorittajalta tai siihen osallistuvalta. Yritysturvallisuusselvityksen ja henkilöturvallisuusselvityksen laatimisen edellytyksistä säädetään turvallisuusselvityslaissa.

Ulkopuolisen asiantuntijan käyttämisessä olisi kyse julkisen hallintotehtävän siirtämisestä yksityiselle ja tehtävää suorittavaan asiantuntijaan tulisi soveltaa rikoslain virkavastuuta koskevia säännöksiä. Arvioinnista aiheutuvista kustannuksista vastaisi sama taho kuin arviointiviranomaisen tekemästä arvioinnista. Arviointiviranomaisen tulisi siten sopia ulkopuolisen asiantuntijan käytöstä arvioinnin kustannuksista vastaavan tahon kanssa.

Hallinnon yleislakeja sovelletaan niiden soveltamisalansa mukaisesti julkiseen hallintotehtävään. Siten arviointiviranomaista avustavassa tehtävässä noudatettaisiin, mitä viranomaisten toiminnan julkisuudesta annetussa laissa, sähköisestä asioinnista viranomaistoiminnassa annetussa laissa (13/2003), hallintolaissa (434/2003), kielilaissa (423/2003) ja saamen kielilaissa (1086/2003) säädetään.

Pykälän *2 momentissa* säädettäisiin Teknologian tutkimuskeskus VTT Oy:n (jäljempänä VTT) tehtävästä arvioida turvallisuuskriittisiä ratkaisuja arviointiviranomaisen toimeksiannosta. Tehtävä liittyy kyberturvallisuuden tavoitteisiin, joita on kirjattu Petteri Orpon hallituksen hallitusohjelmaan, valtioneuvoston puolustusselontekoon 2024 ja kyberturvallisuusstrategiaan vuosille 2024–2035. Kyberturvallisuusstrategian mukaan Suomi pyrkii kriittisen salausteknologian osalta omavaraisuuteen. Tämä edellyttää, että kansallisesti kriittisiä salausteknologioita kuten kvantinkestäviä salausratkaisuja kehitetään kotimaassa ja kokonaisvaltaista salausteknologista kyvykkyyttä vahvistetaan muun muassa tuotannon, tutkimuksen, laskennan, takaisinmallinnuksen sekä organisoitumisen osa-alueilla. Kyberturvallisuusstrategian toimeenpanosuunnitelmassa 3.12.2024 on esitetty kansallisen salausteknologian kyvykkyyden kehittämiseksi salausteknologisen laboratorion rakentamista. Samoin valtioneuvoston puolustusselonteossa todetaan, että salausteknologian kyvykkyyksiin liittyvän tutkimuksen, osaamisen kehittämisen, kotimaisen tuotantokyvyn ja eri viranomaisten tehtävien tukemiseksi perustetaan kansallinen salausteknologinen laboratorio.

VTT:lle ehdotettava arviointiviranomaista avustava tehtävä arvioida turvallisuuskriittisiä ratkaisuja on perusteltu, koska yllä mainittu salausteknologian laboratorio tulee VTT:n yhteyteen. VTT:n avustava arviointitehtävä mahdollistaisi pitkäjänteisen yhteistyön arviointiviranomaisten kanssa. VTT ei tekisi arviointia itsenäisesti, vaan arviointiviranomaisen toimeksiannosta ja ohjauksessa. Momentin mukaisessa VTT:n tehtävässä olisi myös kyse julkisesta hallintotehtävästä ja VTT:n työntekijään sovellettaisiin 1 momentissa ulkopuoliselle asiantuntijalle säädettyä vaatimusta koulutuksesta ja kokemuksesta sekä rikosoikeudellista virkavastuuta koskevia säännöksiä.

4 b § *Arviointiviranomaisten tiedonvaihto ja yhteistyö.* Lakiin lisätäisiin uusi 4 b §, jossa säädettäisiin arviointiviranomaisten keskinäisestä yhteistyöstä, tiedonvaihdosta ja joustavasta resurssien käytöstä. Ehdotus on tarpeen arviointiviranomaisten tehokkaan ja tarkoituksenmukaisen toiminnan turvaamiseksi.

Pykälän *1 momentissa* säädettäisiin arviointiviranomaisten yhteistyöstä ja tiedonsaantioikeuksista tehtävien hoitamiseksi. Arviointiviranomaisten olisi annettava toisilleen tehtävien hoitamiseksi välttämättömiä tietoja sen estämättä, mitä salassapitovelvollisuudesta säädetään. Tiedonvaihto olisi olennainen osa yhteistyötä. Yhteistyön ja tiedonvaihdon tarkoituksena olisi edistää yhteistä tilannekuvaa julkisen hallinnon arviointitarpeista, ehkäistä päällekkäistä työtä ja edistää osaamisen jakamista sekä teknisen kehityksen ja tietoturvauhkien huomioimista ja yhdenmukaista vaatimusten tulkintaa arviointitoiminnassa.

Pykälän *2 momentissa* säädettäisiin, että 4 §:n 1 ja 2 momentissa säädettyjen arviointiviranomaisten tehtävien estämättä arviointiviranomaiset voivat sopia tietyn tehtävän tai sen osan hoitamisesta toisen arviointiviranomaisen lukuun, jos järjestely on tarpeen tehtävien hoitamiseksi tarkoituksenmukaisesti, taloudellisesti ja joutuisasti. Tämä edistäisi arviointiresurssien joustavaa käyttöä yhdessä sovittujen priorisointien mukaisesti.

Pykälän *3 momentissa* velvoitettaisiin Liikenne- ja viestintävirasto koordinoimaan arviointiviranomaisten yhteistyötä yhtenäisen soveltamiskäytännön luomiseksi arviointiviranomaisten toiminnassa. Tarkoitus olisi varmistaa, että arviointiviranomaisten yhteistyö ja tiedonvaihto on sujuvaa. Turvallisuuskriittisten ratkaisujen arvioinnin kannalta yhteistyön ja soveltamiskäytännön koordinoinnin tärkeänä tavoitteena olisi valmistajien ja eri viranomaiskäyttäjien tarpeiden kannalta, että ratkaisuihin sovellettavat tietoturvallisuusvaatimukset ja niiden soveltaminen arviointiviranomaisilla eivät eroa toisistaan, mutta myös varmistaa, että Puolustusvoimien erityiset toiminnalliset vaatimukset tulevat tarkoituksenmukaisesti huomioiduiksi.

5 § *Selvitykset valtiovarainministeriön toimeksiannosta.* Pykälää muutettaisiin siten, että toimivaltaisen viranomaisen nimeksi muutettaisiin Liikenne- ja viestintävirasto. Kyse on teknisluonteisesta muutoksesta. Liikenne- ja viestintäministeriön hallinnonalalla tehdyn virastouudistuksen myötä Viestintävirasto lakkasi olemasta 1.1.2019 alkaen, ja uutena viestintähallinnon viranomaisena toimii Liikenne- ja viestintävirasto.

Pykälän *1 momenttiin* lisättäisiin tietoturvallisuuden tason selvittämisen lisäksi lain soveltamisalan laajenemisen mukaisesti varautuminen mahdollisten valtionvarainministeriön Liikenne- ja viestintävirastolta pyytämien selvitysten kohteeksi. Teknisenä muutoksena momenttia päivitettäisiin siten, että valtiovarainministeriö voi pyytää Liikenne- ja viestintävirastolta selvityksiä tietoturvallisuudesta annettujen säännösten toimeenpanosta voimassa olevassa pykälässä säädetyn toimeenpanoon liittyvän selvityksen sijaan.

Pykälän *2 momentissa* Liikenne- ja viestintäviraston arvion sijaan säädettäisiin Liikenne- ja viestintäviraston selvityksestä. Kyse on teknisestä muutoksesta, jotta terminologia saadaan vastamaan 1 momenttia.

6 § *Arviointiviranomaisen tarkastusoikeus, tiedonsaantioikeus ja oikeus päästä tiloihin ja tietojärjestelmiin.* Pykälän otsikkoa muutettaisiin siten, että Viestintävirasto vaihdettaisiin arviointiviranomaiseksi.

Pykälän *1 momenttia* muutettaisiin siten, että tiedonsaanti- ja pääsyoikeudet laajennettaisiin koskemaan arviointiviranomaisia eli Liikenne- ja viestintäviraston lisäksi Pääesikunnan

määrättyä turvallisuusviranomaista. Arviointiviranomaisen toimeksiannosta toimiva asiantuntija korvattaisiin ehdotetun 4 a §:n mukaisella arviointiviranomaista avustavassa tehtävässä toimivalla avustavalla asiantuntijalla. Momenttiin lisättäisiin myös ehdotetussa 4 §:n mukaisessa turvallisuuskriittisten ratkaisujen ja niiden valmistuksen arvioinnissa arviointiviranomaisten tarvitsemat tiedonsaantioikeudet ja pääsyoikeudet. Lisäksi tiedonsaantioikeudet sidottaisiin välttämättömyysperusteeseen voimassa olevassa pykälässä säädetyn tarpeellisuusperusteen sijaan. Tiedonsaantioikeuteen sisältyvien tietojen tulisi siis olla välttämättömiä laissa säädetyn tehtävän suorittamiseksi. Tiedonsaantioikeus sidottaisiin säännöksessä tässä laissa säädettyihin tehtäviin, jotka olisivat ehdotetussa 4 §:ssä ja 5 §:ssä laajemmat kuin voimassa olevassa laissa. Tietojärjestelmien ja tietoliikennejärjestelyn sekä turvallisuuskriittisten tuotteiden arvioinnin ja 5 §:n mukaisen valtiovarainministeriölle laadittavan selvitysten lisäksi laissa säädettäisiin hyväksytyn hajasäteilysuojausratkaisuja tarjoavan yrityksen ohjaus- ja valvontatehtävästä Liikenne- ja viestintävirastolle. Voimassa olevan lain mukaan arviointiviranomaisella on tiedonsaantioikeus sen estämättä mitä tietojen salassapidosta säädetään, mikä muutettaisiin muotoon salassapitosäännösten estämättä ja pykälään lisättäisiin tiedonsaantioikeus myös muiden tiedon luovuttamista koskevien rajoitusten estämättä. Muita tiedon luovuttamista koskevia rajoituksia voivat olla esimerkiksi yrityksen liike- tai ammattisalaisuudet. Tietojen välttämättömyyden arviointi olisi arviointiviranomaisen tehtävä ja sen tulisi pystyä perustelemaan tietojen välttämättömyys pyytäessään niitä viranomaisilta ja yrityksiltä arviointien, selvitysten tai valvonnan suorittamiseksi.

Arviointiviranomaisen oikeutta päästä tiloihin ja tietojärjestelmään tarkennettaisiin siten, että pääsyoikeuksiin lisättäisiin myös tietoliikennejärjestely. Lisäksi 1 momenttiin lisättäisiin tiedonsaantioikeuden kohteena asiakirjat, laitteet ja ohjelmistot. Turvallisuuskriittisten ratkaisujen arvioinnissa voisi olla tarpeen esimerkiksi arvioida ohjelmistoja ja lähdekoodia sekä testata laitteita. Momenttiin lisättäisiin selvyyden vuoksi maininta oikeudesta suorittaa tarvittavia hallinnollisia ja teknisiä arviointitoimenpiteitä. Näitä olisivat erilaiset tekniset tarkastustoimenpiteet, kuten tietojärjestelmään ja tietoliikenteeseen kohdistuvia haavoittuvuusskannauksia ja testejä. Tekninen testaus on välttämätön menettely sekä tietojärjestelmien että turvallisuuskriittisten ratkaisujen tietoturvallisuuden arvioinnissa. Teknisesti testaamalla voidaan todentaa asiakirjojen ja haastattelujen perusteella saatua selvitystä ja havainnoida tietojärjestelmän tai turvallisuuskriittisen ratkaisun kyvykkyyttä erilaisilta tietoturvallisuusuhkilta suojautumisessa. Tekninen testaus voi edellyttää pääsyä tilaan, jossa tietojärjestelmään tai tietoliikennejärjestelyyn kuuluvat laitteet ovat.

Pykälään lisättäisiin uusi *2 momentti*, jossa säädettäisiin Liikenne- ja viestintäviraston tai sitä avustavan asiantuntijan tarkastusoikeudesta hajasäteilysuojausratkaisuja tarjoavan valmistajan valvonnassa. Erotuksena 1 momentissa tarkoitetuissa arvioinneissa ja selvityksissä tehtäviin arviointitoimenpiteisiin tässä olisi kysymys hallintolain 39 §:n mukaisesta tarkastuksesta, jonka tarkoitus olisi selvittää, noudattaako valmistaja tämän lain nojalla annettuja päätöksiä. Liikenne- ja viestintäviraston päätöksissä yksilöidyt vaatimukset perustuisivat 7 §:ssä arviointiperusteiksi säädettyihin säädöksiin, ohjeisiin tai standardeihin, joiden vaatimukset valmistaja haluaa täyttää. Tällaisia voivat olla esimerkiksi Euroopan unionin neuvoston ja Pohjois-Atlantin liiton turvallisuussääntöjen vaatimukset ja kansainväliset standardit. Liikenne- ja viestintävirasto yksilöisi 8 §:n 3 momentin mukaisessa hyväksyntäpäätöksessä ehdot, jotka ovat tarpeen valmistuksen luotettavuuden ylläpidossa ja toiminnan aikana tarvittaessa 4 §:n 2 momentin 4 kohdan mukaisessa valmistuksen toimenpiteiden tai ratkaisun vaatimuksia koskevassa päätöksessä. Tiedonsaantioikeudet ja pääsyoikeudet tarkastuksessa vastaisivat 1 momentissa säädettyä.

Pykälään lisättäisiin uusi *3 momentti*, joka vastaisi voimassa olevan lain 2 momenttia sillä erotuksella, että kotirauhan piirin turvaaminen ulotettaisiin koskemaan myös 2 momenttiin ehdotettua tarkastusta.

7 § *Tietoturvallisuuden ja varautumisen arviointiperusteet*. Pykälän otsikkoa muutettaisiin siten, että siinä huomioitaisiin ehdotettu lain soveltamisalan laajentaminen, jolloin tietoturvallisuuden arviointiperusteiden lisäksi pykälässä säädettäisiin varautumisen arviointiperusteista.

Pykälän *1 momentin* arviointiperusteiden luettelon tarkoituksena olisi mahdollistaa laajasti eri arviointiperusteiden käyttäminen. Momentin *1 kohtaan* lisättäisiin kyberturvallisuus- ja varautumisvaatimukset tietoturvallisuusvaatimusten lisäksi. Viranomaisten toiminalle on asetettu tietoturvallisuusvaatimusten rinnalle myös kyberturvallisuusvaatimuksia, jotka olisi tarkoituksenmukaista huomioida osana tietojärjestelmien ja tietoliikennejärjestelyjen arviointeja.

Tiettyjen viranomaisten, kuten valtiovarainministeriön ja kansallisen turvallisuusviranomaisen ohjeiden mainitsemisen sijaan yleisesti viranomaisen ohjeet säädösten soveltamisesta olisi riittävä ja yleispätevämpi määrittely. Viranomaisten tulisi varmistua ohjeistuksen yhdenmukaisuudesta ja yhtenäisyydestä. Näin ollen nykyinen 1 momentin 2 kohta sisältyisi muutettuun 1 kohtaan.

Momentin *2 kohta* vastaisi nykyistä 3 kohtaa, mutta siihen lisättäisiin Suomen Nato-jäsenyyden myötä Euroopan unionin lisäksi Pohjois-Atlantin liitto säännösten tai ohjeiden mahdollisena antajana. Momentin 1 kohdan tavoin myös 2 kohtaan lisättäisiin tietoturvallisuuden lisäksi kyberturvallisuus ja varautuminen.

Momentin *3 kohta* vastaisi nykyistä 4 kohtaa ja momentin *4 kohta* vastaisi nykyistä 5 kohtaa sillä erotuksella, että molempiin kohtiin lisättäisiin tietoturvallisuutta koskevien säännösten, määräysten tai ohjeiden sekä vaatimusten lisäksi varautumista ja kyberturvallisuutta koskevat säännökset, määräykset tai ohjeet sekä vaatimukset.

Pykälän *2 momenttia* muutettaisiin siten, että siinä säädettäisiin arviointiperusteiden ja arvioinnin kohteen määrittämisessä huomioon otettavista seikoista. Arviointiperusteiden määrittämisellä tarkoitettaisiin säädettyjen ja riskiarvioinnin perusteella valittujen vaatimusten määrittämistä 1 momentissa säädetyistä arviointiperusteiden kokonaisuudesta. Tarkoitus olisi, että arviointiperusteet ja arvioinnin kohde määritettäisiin riskiarvioinnin perusteella arviointikohdekohtaisesti. Arviointiperusteiden valinnan pohjana toimiva riskiarvio edellyttää uhkien tunnistamista. Uhkia ovat yleisesti tunnetut tietoturvauhkat, jotka koskevat tietojärjestelmiä ja tietoliikennejärjestelyjä toimialasta riippumatta. Uhkia ovat myös arvioinnin kohteen erityiset tietoturvauhkat, jotka voivat liittyä esimerkiksi arvioitavan järjestelmän merkitykseen yhteiskunnan turvallisuudelle, kansalliselle turvallisuudelle tai viranomaisen toiminnalle tai arvioinnin kohteen toiminnan kiinnostavuuteen pahantahtoisten toimijoiden kannalta tai yhteisöjen ja kansalaisten palvelujen saatavuudelle tai tiettyyn tekniseen toteutustapaan.

Tietojärjestelmän ja tietoliikennejärjestelyn tietoturvallisuudelle ja varautumiselle säädetyillä vaatimuksilla tarkoitettaisiin esimerkiksi julkisuuslain, tiedonhallintalain ja turvallisuusluokitteluasetuksen säännöksiä. Säädettyjen ja riskiarvioinnin perusteella valittujen arviointiperusteiden määrittämisessä samoin kuin jo tietojärjestelmän ja tietoliikennejärjestelmän suunnittelussa tulisi huomioida arvioinnin kohteessa käsiteltävien tietojen luottamuksellisuus-, eheys-, saatavuus- ja jatkuvuudenhallintavaatimukset sekä tekniseen tuotantotapaan liittyvät vaatimukset. Vaatimusten tunnistamisessa huomioidaan esimerkiksi hallinnollinen, toiminnallinen, fyysinen ja tekninen turvallisuus, jatkuvuudenhallinta ja varautuminen sekä tietosuoja. Vaatimusten tunnistamisella jo suunnitteluvaiheessa vältettäisiin ennakoimattomat vaatimukset ja arvioinnissa voitaisiin keskittyä todentamaan arviointikohteen suunnittelun ja toteuttamisen aikana määritettyjen vaatimusten toteutuminen. Arviointi voi perustua suppeaankin joukkoon vaatimuksiin perustuvia arviointikriteerejä.

Arvioinnin kohteen määrittämisellä tarkoitettaisiin niitä rajauksia, joita arvioinnin suunnittelussa tehdään. Uhkien ja riskien tunnistaminen tukee myös arvioinnin kohteen määrittämistä ja rajaamista tarkoituksenmukaisesti. Arvioinnin kohde voi vaihdella aina yhdestä työasemasta monen toimipisteen verkkoon tai olla esimerkiksi organisaatiossa laajasti käytössä oleva monikansallisen toimittajan pilvipalvelu.

Arvioinnin suunnittelussa olisi tavoitteena varmistua siitä, että tietojärjestelmässä ja tietoliikennejärjestelyssä saavutettaisiin käsiteltäville tiedoille riskeihin nähden riittävä muttei liian korkea tai matala tietoturvallisuuden ja varautumisen taso tai saavutettaisiin asetetut tietoturvallisuuden vaatimukset ja että tasoa tai vaatimuksia ylläpidettäisiin järjestelmän elinkaaren ajan. Tämä edellyttäisi sitä, että arvioinnin kohteen rajaukseen sisällytettäisiin sellaiset tietojärjestelmän tai tietoliikennejärjestelyn osat, jotka oleellisesti vaikuttavat käsiteltävien tietojen tietoturvallisuuteen ja varautumiseen. Esimerkiksi tietojärjestelmän päätelaitteet, käyttöpisteet sekä ylläpitoon käytettävät hallintaratkaisut on usein perusteltua sisällyttää arviointiin. Arvioinnin laajuuden ennakointi edellyttäisi, että arvioinnin kohteesta olisi olemassa riittävä dokumentaatio ja viranomainen tuntisi tietojärjestelmää tai tietoliikennejärjestelyä ja tunnistaisi sen tietoturvallisuuteen ja varautumiseen vaikuttavia tekijöitä sillä tarkkuudella, että pystyttäisiin tunnistamaan tietoturvallisuuteen ja varautumiseen olennaisesti vaikuttavat järjestelmän osat.

Momentissa säädettäisiin myös, että arviointiviranomaiselta pyydettävässä arvioinnissa arviointiperusteiden valinta olisi arviointiviranomaisen vastuulla. Hyvän hallintotavan mukaisesti arviointiviranomaisen tulisi kuulla hakijaa ennen arviointiperusteista päättämistä. Näin varmistettaisiin arviointiviranomaisen asiantuntemuksen hyödyntäminen ja arviointien tarkoituksenmukaisuus arviointia hakevan viranomaisen riskinhallinnan tukena. Tarvittaessa arviointiviranomainen neuvoisi viranomaista arvioinnin suunnitteluvaiheessa tai sen edetessä, kun toteutus tarkentuu tai muuttuu.

Viranomaisen itsearvioinnissa tai viranomaisen 3 a §:n 1 momentin 2 kohdan tarkoittamissa palveluntarjoajille annetussa toimeksiannoissa viranomainen määrittäisi arviointiperusteet, arvioinnin kohteen ja sen kohdentamisen. Arviointiperusteista tietoturvallisuuden arviointilaitoksen ja sen asiakkaan toimeksiantosuhteessa säädetään arviointilaitoslaissa. Arvioinnin kohteen määrittäminen ja kohdentaminen tapahtuisi arvioinnin hakijan ja tietoturvallisuuden arviointilaitoksen välisessä vuorovaikutuksessa.

Pykälään lisättäisiin uusi *3 momentti,* jossa säädettäisiin uudesta turvallisuuskriittisten ratkaisujen ja valmistuksen arviointiperusteiden määrittämisestä. Arviointiviranomainen määrittäisi ratkaisuun ja valmistukseen soveltuvat arviointiperusteet 1 momentin arviointiperusteiden kokonaisuudesta valmistajaa kuultuaan. Arviointiviranomaisen tulisi hyvän hallintotavan mukaisesti kuulla hakijaa ennen arviointiperusteista päättämistä. Arviointiperusteiden määrittäminen voitaisiin parhaiten tehdä arviointiviranomaisen ja valmistajan yhteistyössä. Näin olisi varsinkin sellaisissa arvioinneissa, joissa turvallisuus edellyttää arviointia jo kehitysvaiheessa. Arviointi tukisi tällöin myös valmistajan kehitys- ja suunnittelutyötä.

Arviointiperusteiden määrittämisessä otettaisiin huomioon ratkaisuun tyypillisesti vaikuttavat tietoturvauhkat 2 momentin perusteluissa kuvatulla tavalla. Lisäksi otettaisiin huomioon tavoiteltu turvallisuusluokka, valmistuksen turvallisuus ja valmiudet kansainvälisten tietoturvallisuusvelvoitteiden täyttämiseen. Valmistuksen turvallisuudella tarkoitettaisiin valmistusyritykseen ja toimitusketjuun liittyviä seikkoja ja turvallista tuotekehitystä, suunnittelua, valmistusta, ylläpitoa ja muita toimia. Valmiudella kansainvälisten tietoturvallisuusvelvoitteiden täyttämiseen tarkoitettaisiin sitä, että arvioinnissa tulee mahdollisuuksien mukaan edistää valmistajan mahdollisuuksia saada ratkaisulle myös kansainvälisten tietoturvallisuusvaatimusten mahdollisesti edellyttämä hyväksyntä. Tässä tarkoituksessa voitaisiin hyödyntää suoraan erilaisia

kansainvälisten tietoturvallisuusvaatimusten lähteitä osana arviointiperusteita tai määrittää perusteet siten, että jatkokehitys kansainvälisten tietoturvallisuusvaatimusten täyttämiseksi on mahdollista.

7 a § *Valmistajan arviointiin liittyvät selvitykset.* Lakiin lisättäisiin uusi 7 a §, jossa säädettäisiin turvallisuuskriittisen ratkaisun valmistajan arviointiin liittyvistä menettelyistä.

Pykälän *1 momentissa* säädettäisiin Liikenne- ja viestintävirastolle uusi menettelyyn liittyvä edellytys hakea yritysturvallisuusselvitystä 4 §:n 2 momentin 1 kohdassa tarkoitetun turvallisuuskriittisen ratkaisun arvioinnissa. Lisäksi säädettäisiin, että turvallisuuskriittisen ratkaisun hyväksyntä edellyttää, että valmistajan yritysturvallisuusselvityksessä ei ole ilmennyt mitään, mikä kokonaisharkinnan perusteella vaarantaisi valmistuksen turvallisuuden ja luotettavuuden ottaen huomioon ulkomaisen vaikutuksen riskit.

Pykälän *2 momentissa* säädettäisiin tilanteista, joissa arviointiperusteena käytetään kansainvälistä standardia, jonka mukainen pätevyys on mahdollista akkreditoida vaatimustenmukaisuuden arviointipalvelujen pätevyyden toteamisesta annetussa laissa säädetyn FINASin akkreditointimenettelyn avulla. Menettely ei olisi pakollinen, vaan Liikenne- ja viestintävirasto voisi harkita hyväksynnän perusteet. Hyväksynnän perusteisiin voisi liittyä kansainvälisen erityissuojattavan tiedon käsittelyä tai turvallisuusluokitellun tiedon käsittelyä, mikä voisi vaikuttaa mahdollisuuteen käyttää sujuvasti FINASin akkreditointipalvelua.

Säännös mahdollistaisi myös sen, että yhtenä osana hyväksynnän perusteita voitaisiin huomioida valmistajan mahdollisesti jo aikaisemmin saama akkreditointi. Hajasäteilysuojauksen ratkaisujen valmistajien arvioinnissa hakemus voisi koskea itse valmistajan hyväksyntää TEMPEST-yrityksenä. Hajasäteilysuojaus on kapea tekninen erityisalue, joka koskee korkeimpia turvallisuusluokkia. Arviointiperusteina käytetään ensisijaisesti kansainvälisiä turvallisuusluokitellun tiedon suojaamiseen laadittuja lähteitä. Valmistuksen menettelyjen arvioinnissa voidaan hyödyntää samoja standardeja, joita hyödynnetään muillakin valmistuksen aloilla, kuten ISO/IEC 17025 ja ISO/IEC 9001 mukaiset akkreditoinnit. Tällöin valmistajan pätevyyden standardinmukaisuuden arvioinnissa voitaisiin hyödyntää FINASin akkreditointia. TEMPEST-yrityksen hyväksynnän perusteena huomioitavassa akkreditoinnissa ei olisi välttämätöntä huomioida yksityiskohtaista turvallisuusluokiteltua teknistä substanssitietoa, vaan prosessien tasalaatuisuus ja vertailukelpoisuus. Hajasäteilysuojauksen ratkaisujen valmistajan arviointi ja hyväksyntä tarkoittaisi sitä, että yrityksellä olisi todettu kyvykkyys ylläpitää valmistuksen laatua ja menettelyjä ilman, että arviointiviranomainen arvioi jokaisen tuotteen, laitteen tai muun ratkaisun.

8 § *Arviointiraportin, hyväksyntäpäätöksen ja -lausunnon antaminen.* Pykälän otsikkoa muutettaisiin siten, että todistuksen antamisen sijaan siinä säädettäisiin arviointiraportin ja hyväksyntäpäätöksen tai -lausunnon antamisesta.

Pykälän *1 momenttia* muutettaisiin siten, että siinä säädettäisiin arvioinnista laadittavasta arviointiraportista. Arviointiraportti tulisi laatia kaikista ehdotetun 3 §:n 1 momentin mukaisilla menettelyillä toteutetuista arvioinneista.

Arvioinnin toteuttaja laatisi arvioinnin tuloksista raportin arvioinnin kohteen tietoturvallisuuden ja varautumisen tasosta ja mahdollisista riskeistä. Raportti sisältäisi tiedot arvioinnin kohteesta, käytetyistä arviointiperusteista, arvioinnin laajuudesta ja arvioinnin aikana tehdyistä havainnosta. Arvioinnin laajuudella tarkoitettaisiin esimerkiksi käytettyjä todentamismenetelmiä, arvioinnin syvyyttä kuten teknisessä arvioinnissa käytettyjä penetraatiotestauksia tai koodin tarkistusta sekä arvioinnin kattavuutta ajallisesti ja organisatorisesti. Raportissa voitaisiin todeta

lieviä tai vakaviakin poikkeamia arviointiperusteiden toteutumisessa. Viranomainen tarvitsisi arviointiraporttia päättäessään jäännösriskeistä ja tehdessään tietojärjestelmän tai tietoliikennejärjestelyn käyttöönotto- ja käyttöpäätöksiä.

Arviointiraportilla olisi tarkoitus selkeyttää viranomaisen vastuuta tietojärjestelmiensä ja tietoliikennejärjestelyjensä tietoturvallisuudesta. Arviointiraportin käytöllä parannettaisiin ja yhdenmukaistettaisiin viranomaisen tietoturvallisuus- ja varautumistoimenpiteistä ja tietojärjestelmien ja tietoliikennejärjestelyjen jäännösriskeistä, käyttöönotosta ja käytöstä tekemien päätösten laatua, sillä arviointiraportti lisäisi viranomaisen tietopohjaa toimintaympäristön, tietojärjestelmien ja tietoliikennejärjestelyjen riskeistä.

Pykälän *2 momenttia* muutettaisiin siten, että siinä säädettäisiin arviointiviranomaisen antamasta hyväksyntäpäätöksestä tai -lausunnosta, kun viranomainen on hakenut hyväksyntää ehdotetun 3 § 7 momentin mukaisesti ja arvioitava tietojärjestelmä tai tietoliikennejärjestely täyttää vaatimukset. Hyväksyntä koskisi siis pääasiassa kansainvälisiä tilanteista, joissa viranomaisen liikkumavaraa jäännösriskipäätöksissä on voitu rajoittaa erityissääntelyssä, esimerkiksi kansainvälisissä tietoturvallisuusvelvoitteissa tai muussa toimialakohtaisessa sääntelyssä.

EU:n ja Naton turvallisuusluokitellun tiedon käsittelyyn käytettävät tietojärjestelmät on turvallisuusääntöjen mukaan etukäteen akkreditoitava, ja myös tietyt osa-alueet tai elementit on etukäteen arvioitava ja hyväksyttävä. Päätökseen muotoon ja sisältöön liittyy erilaisia vaatimuksia eri tilanteissa ja ne voivat olla muodoltaan esimerkiksi hyväksyntälausuntoja, väliaikaisia lausuntoja tai päätöksiä hyväksynnästä. Näiden lausuntojen ja päätösten vaikutukset arviointiprosessissa määritellään kansainvälisissä tietoturvallisuusvelvoitteissa. Menettelyt eroavat riippuen siitä, onko kysymyksessä EU:n tai Naton Suomeen toimittama järjestelmä vai kansallisesti toteutettu EU:n tai Naton turvallisuusluokitellun tiedon käsittelyyn tarkoitettu järjestelmä. Kansallisen järjestelmän arvioinnissa hyväksynnästä ja hyväksymislausunnossa ilmenevän jäännösriskin hyväksynnästä vastaa järjestelmän vastuuviranomainen, jonka on otettava huomioon riippumattoman arvioinnin tulos. Kansallisen järjestelmän arvioinnissa hyväksyntälausunto annetaan päätöksellä ja eräissä tilanteissa mahdollinen väliaikainen hyväksyntälausunto välipäätöksellä, jossa todetaan ehdot varsinaisen hyväksyntälausunnon saamiseksi. Toimitetun järjestelmän arvioinnissa puolestaan kansallisesti tehtävä arviointi painottuu tyypillisesti toimitettua tietojärjestelmää ympäröiviin suojauksiin kuten fyysiseen turvallisuuteen, henkilöstöturvallisuuteen sekä käyttöpisteen hajasäteilysuojaukseen, joista laaditaan vaatimuksenmukaisuuslausunto ja hyväksyntälausunnon antaa yleensä jokin EU:n tai Naton toimielin.

Liikenne- ja viestintäviraston hyväksynnän saaman tietoturvallisuuden arviointilaitoksen myöntämästä todistuksesta säädetään arviointilaitoslaissa.

Pykälään lisättäisiin uusi *3 momentti*, jossa säädettäisiin Liikenne- ja viestintäviraston uudesta tehtävästä antaa suomalaisen valmistajan turvallisuuskriittisen ratkaisun arvioinnista tekemään hakemukseen ja hajasäteilysuojausratkaisujen valmistajan tekemään hakemukseen valmistajan hyväksymisestä valituskelpoinen hallintopäätös. Jos turvallisuuskriittinen ratkaisu täyttää arvioinnille määritetyt vaatimukset, päätös olisi ratkaisun hyväksyntäpäätös. Arviointi ja päätös tehtäisiin aina suhteessa turvallisuusluokkaan ja hyväksyntä olisi pääsääntöisesti määräaikainen, sillä teknologian kehittyminen ja uhkaympäristön kehitys edellyttävät ratkaisujen teknistä kehittämistä ja arviointia aika ajoin. Ratkaisujen käyttö turvallisuusluokitellun tiedon suojaamisessa edellyttää tyypillisesti tietynlaisia valintoja tai määrittelyjä ratkaisun hyödyntämisessä tai sen käyttöympäristöltä. Tällaiset ehdot voitaisiin merkitä päätökseen tai esimerkiksi sen liitteenä annettavaan käyttöohjeeseen eli käyttöpolitiikkaan. Jos vaatimukset eivät täyttyisi, valmistaja voisi hyödyntää saamaansa arviointiraporttia ja päätöstä ratkaisun kehittämisessä ja tarjoamisessa.

Hajasäteilysuojaratkaisun eli TEMPEST-laitteiden valmistajaa koskevaan hyväksyntäpäätökseen tulisi asettaa toiminnan yleiset ehdot. Hyväksyntä olisi pääsääntöisesti määräaikainen.

8 a § *Viranomaisen velvollisuus hankkia todistus.* Pykälä ehdotetaan kumottavaksi, sillä viranomaisten arviointivelvoitteista ehdotetaan säädettävän 3 §:ssä.

8 b § *Turvallisuusselvitysrekisteriin merkittävät tiedot ja merkinnän poistaminen*. Pykälä ehdotetaan kumottavaksi, sillä turvallisuusrekisteriä on käytetty vain vähäisessä määrin pykälässä säädetyssä tarkoituksessa.

8 c § *Hyväksyttyjen turvallisuuskriittisten ratkaisujen ja valmistajien luettelo.* Lakiin lisättäisiin uusi 8 c §, jossa säädettäisiin Liikenne- ja viestintävirastolle uusi tehtävä ylläpitää ja julkaista hyväksyttyjen turvallisuuskriittisten ratkaisujen ja valmistajien luetteloa.

Pykälässä säädettäisiin, että hyväksyttyään turvallisuuskriittisen ratkaisun 4 §:n 2 momentin 1 kohdassa säädetyn tehtävän mukaisesti ja annettuaan 8 §:n mukaan hyväksyvän päätöksen turvallisuuskriittisen ratkaisun vaatimustenmukaisuudesta Liikenne- ja viestintävirasto julkaisisi tiedon ratkaisusta ja sen valmistajasta julkisessa luettelossa. Jos vaatimustenmukaisuudesta annetussa päätöksessä todettaisiin, että arvioitu turvallisuuskriittinen ratkaisu ei täytä määritettyjä vaatimuksia, tietoa päätöksestä ei julkaistaisi. Luettelon tarkoituksena olisi tarjota turvallisuuskriittisiä ratkaisuja tarvitseville viranomaisille ja yrityksille tietoja tarjonnasta. Menettely vastaisi EU:n ja Naton turvallisuusluokitellun tiedon suojaamiseen liittyviä luetteloita.

Lisäksi pykälässä säädettäisiin vähimmäistiedoista, jotka soveltuvin osin tulisi ilmetä luettelosta ratkaisusta tai valmistajasta riippuen. Luettelosta tulisi ilmetä ratkaisun nimi ja tarvittaessa versio, jota hyväksyntä koskee, sekä turvallisuusluokka, jonka mukaisen tiedon suojaamiseen ratkaisu on todettu riittäväksi. Luetteloon merkittäisiin tieto kansallisen turvallisuusluokan perusteella ja tarvittaessa EU:n tai Naton turvallisuusluokan perusteella tehdystä arvioinnista. Luettelosta tulisi ilmetä tieto valmistajasta. Jos hyväksyntä koskisi TEMPEST-laitteiden valmistajaa, tieto valmistajasta ja hyväksynnän alueesta voisi olla riittävä, eikä ratkaisuja, tuotteita tai versioita välttämättä olisi tarpeellista yksilöidä. Tiedot voimassaolosta, muutoksista tai lakkaamisesta ovat tärkeitä ratkaisujen hankinnan suunnittelussa. Muutos voisi koskea esimerkiksi turvallisuusluokan nostamista tai alentamista tai versiomuutosta. Voimassaolo voisi lakata valmistajan aloitteesta, jos voimassaolon jatkoa ei pyydetä. Voimassaolo voisi lakata myös Liikenne- ja viestintäviraston 10 §:n mukaisesti tekemällä päätöksellä, jos ratkaisu tai valmistaja ei enää täytä hyväksynnän edellytyksiä.

9 § *Tietoturvallisuuden ylläpito ja seuranta*. Pykälää muutettaisiin siten, että nykyinen todistuksen saaneen sitoumus ylläpitää tietoturvallisuuden tasoa, korvattaisiin päätöksen tai lausunnon saaneen velvollisuudella ylläpitää tietoturvallisuus päätöksen tai lausunnon mukaisena. Tietoturvallisuutta koskeva muutosilmoitus tulisi tehdä päätöksen tai lausunnon myöntäneelle arviointiviranomaiselle. Muutosilmoituksen kynnystä laskettaisiin tietoturvallisuustasoon vaikuttavista muutoksista sellaisiin muutoksiin, joilla voi olla vaikutusta päätöksen tai lausunnon mukaisiin vaatimuksiin.

Arviointiviranomaisen tiedonsaantioikeuksista sekä oikeudesta päästä tiloihin ja järjestelmiin säädettäisiin kattavasti 6 §:ssä, jolloin pääsyoikeuksista ei tarvitsisi enää säätää erikseen tässä pykälässä.

10 § *Hyväksyntäpäätöksen kumoaminen tai -lausunnon peruuttaminen.* Pykälä ja sen otsikko muutettaisiin vastaamaan ehdotetun 8 § muutosta siten, että todistuksen peruuttamisen sijaan

pykälässä säädettäisiin hyväksyntäpäätöksen tai -lausunnon perumisesta. Lisäksi Viestintävirasto korvattaisiin arviointiviranomaisella.

11 § *Muutoksenhaku.* Pykälää ehdotetaan muutettavaksi siten, että Viestintävirasto korvattaisiin arviointiviranomaisella ja viittaus kumottuun hallintolainkäyttölakiin (586/2966) korvattaisiin viittauksella voimassa olevaan lakiin oikeudenkäynnistä hallintoasioissa (808/2019).

12 § *Maksut.* Pykälän sanamuotoa ja viittausta valtion maksuperustelakiin (150/1992) päivitettäisiin, Viestintävirasto korvattaisiin arviointiviranomaisella ja viittaus todistukseen viittauksella ehdotetun 8 §:n mukaiseen arviointiraporttiin, lausuntoon tai päätökseen. Lisäksi arviointiviranomaisen antama neuvonta lisättäisiin maksullisiin palveluihin.

7.2 Laki tietoturvallisuuden arviointilaitoksista

1 § *Lain tarkoitus.* Pykälää muutettaisiin siten, että lain tarkoituksena olisi myös säätää menettelystä, jonka avulla viranomaiset voivat hankkia riippumattoman tietoturvallisuuden ja varautumisen arvioinnin. Pykälään ehdotettava muutos olisi yhdenmukainen arviointilakiin ehdotettavan 3 a §:n kanssa, jossa säädettäisiin, että hyväksytyn tietoturvallisuuden arviointilaitoksen toteuttama arviointi on yksi viranomaisen tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden ja varautumisen arviointimenettelyistä. Pykälään ehdottava muutos olisi myös luonteeltaan nykytilaa selkeyttävä, sillä viranomaiset ovat voineet jo voimassa olevan säännöksen nojalla hankkia tietoturvallisuuden arviointeja hyväksytyiltä tietoturvallisuuden arviointilaitoksilta.

2 § *Lain soveltamisala.* Lain soveltamisalaa täsmennettäisiin ja pykälän *1 momenttiin* lisättäisiin maininta siitä, että lakia sovelletaan Suomeen sijoittautuneisiin toimijoihin. Laissa säädetyn tietoturvallisuuden arviointilaitosten hyväksyntä- ja valvontamenettelyn keskeinen tarkoitus on varmistaa luotettava ja laadukas arviointi viranomaisille ja niiden palveluntarjoajille. Tietoturvallisuuden arviointilaitosten valvonnan, sekä luotettavuuden riittävän arvioinnin mahdollistamiseksi arviointilaitoksen tulisi olla Suomen lainkäytön piirissä ja näin ollen Suomeen rekisteröitynyt ja sijoittautunut oikeushenkilö. Luotettavuuden varmistaminen on keskeistä, sillä laitokset pääsevät toimeksiantojen aikana asiakkaiden luottamuksellista, salassa pidettävää ja turvallisuusluokiteltua tietoa käsitteleviin tietojärjestelmiin, saavat tietoja niihin liittyvistä asiakirjoista ja turvajärjestelyistä sekä mahdollisista heikkouksista, puutteista ja haavoittuvuuksista järjestelmissä sekä tietoliikennejärjestelyissä.

Pykälän 1 momenttiin myös lisättäisiin yhdenmukaisesti arviointilakiin ehdotetun kanssa, että arviointilaitosten tehtävänä olisi jatkossa toimeksiannosta arvioida tietoturvallisuuden lisäksi myös tietojärjestelmän tai tietoliikennejärjestelyn varautumisen tasoa. Lisäksi pykälän 1 momentissa huomioitaisiin liikenne- ja viestintäministeriön hallinnonalalla tehty virastouudistus, jonka myötä Viestintävirasto lakkasi olemasta 1.1.2019 alkaen, ja uutena viestintähallinnon viranomaisena toimii Liikenne- ja viestintävirasto.

Pykälän *2 momentti* muutettaisiin vastaamaan arviointilakiin ehdotettavia muutoksia. Pykälän viittaus muualla säädettävistä Viestintäviraston tehtävistä päivitettäisiin arviointiviranomaisen muualla säädettäviin tehtäviin ja tietoturvallisuuden arvioinnin lisäksi momentissa huomioitaisiin varautumisen arviointi. Lisäksi momentin viittaus yhteisöturvallisuusselvitykseen muutettaisiin vastaamaan selvityksen nykyistä nimitystä yritysturvallisuusselvitys.

3 § *Arviointilaitoksen hyväksymistä koskeva hakemus*. Pykälän *1 momenttia* muutettaisiin siten, että hyväksytty tietoturvallisuuden arviointilaitos voisi hakea hyväksyntää arvioinnin pätevyysaluetta varten Liikenne- ja viestintävirastolta. Arviointilaitokselle hyväksytyt pätevyysalueet rajaavat mitä tietoturvallisuuden ja varautumisen arviointiperusteita arviointilaitos voi käyttää arviointitehtävissään. Arviointilaitoksen tulee hakemuksen yhteydessä ilmoittaa mille pätevyysalueelle se hakee hyväksyntää. Hyväksytty tietoturvallisuuden arviointilaitos voi myöhemmin laajentaa toimintakenttäänsä ja hakea hyväksyntää lisäpätevyysalueille. Mahdollisuus hakea hyväksyntää uudelle pätevyysalueelle koskisi hyväksyttyjen tietoturvallisuuden arviointilaitosten hakemuksia lisäpätevyyksistä, jotka liittyvät arviointilaitoslain 10 §:ssä säädettyjen arviointiperusteiden mukaisiin pätevyysalueisiin, joita laitoksella ei vielä ole. Ehdotetun 5 §:n 3 momentin mukaan lisäpätevyyksien osalta ei jatkossa aina edellytettäisi FINASin akkreditointia. Sen sijaan tietoturvallisuuden arviointilaitokseksi hyväksyminen edellyttäisi jatkossakin FINASin akkreditointia jollekin tietoturvallisuuden tai varautumisen pätevyysalueelle.

Pykälän *1 momentissa* Viestintävirasto muutettaisiin Liikenne- ja viestintävirastoksi.

4 § *Hakemuksen käsittely*. Pykälän *1 momenttiin* lisättäisiin uutena arviointilaitoksen luotettavuuden selvitysmenettelynä yritysturvallisuusselvitys. Yritysturvallisuusselvitys mahdollistaisi arviointilaitoksen omistuspohjan selvittämisen ja seurannan sekä vastuuhenkilöiden turvallisuusselvitykset ja nuhteettomuusseurannan. Yritysturvallisuusselvitys kattaisi myös arviointilaitoksen toimitilat ja tietojärjestelmät, jolloin niiden turvallisuutta ei tarvitsisi tarkastaa erikseen. Liikenne- ja viestintäviraston olisi haettava yritysturvallisuusselvitystä silloin, kun arviointilaitos hakee pätevyyttä, joka koskee turvallisuusluokitellun tiedon käsittelyn arviointia. Tällainen pätevyys on arviointilaitoslain soveltamisalalla esimerkiksi kansallisen turvallisuusviranomaisen ohjeena antaman Katakri-auditointityökalun käyttäminen arviointiperusteena. Liikenne- ja viestintäviraston toimiessa selvityksen hakijana sen tietoon tulisivat suojelupoliisin tekemät mahdolliset havainnot, joiden merkitystä virasto voisi arvioida arviointilaitoshyväksynnän kannalta. Ehdotus on perusteltu, sillä suojelupoliisi voi käyttää hyväkseen tarkkaan säädeltyä ja vakiomuotoista prosessia arviointilaitoksen luotettavuuden selvittämiseksi.

Niissä tilanteissa, joissa arviointilaitos hakee pätevyyttä, joka koskee muun kuin turvallisuusluokitellun tiedon käsittelyä, voitaisiin edelleen käyttää lain nykyistä selvitysmenettelyä, jossa suojelupoliisille varataan tilaisuus lausua arviointilaitoksen vastuuhenkilöistä ja toimitiloista. Lisäksi 1 momenttiin lisättäisiin sana selvitys, jotta se kattaisi myös yritysturvallisuusselvitykset.

Yritysturvallisuusselvitysten tekeminen sellaisten arviointilaitosten hyväksynnässä, jotka hakevat pätevyyttä turvallisuusluokitellun tiedon suojaamisen arviointiin, tehostaisi ja selkeyttäisi arviointilaitoksen luotettavuuden selvittämistä ja seurantaa. Hyväksyntämenettely selkeytyisi Liikenne- ja viestintäviraston ja suojelupoliisin sekä arviointilaitoshyväksyntää hakevan yrityksen kannalta. Yritysturvallisuusselvitystodistus olisi omiaan lisäämään viranomaisasiakkaiden luottamusta arviointilaitoksiin.

Pykälän *2 momentissa* säädettyä viraston mahdollisuutta antaa toimeksiannosta suoritettavia tehtäviä ulkopuoliselle asiantuntijalle muutettaisiin siten, että se koskisi vain avustavia tehtäviä. Kyse olisi samankaltaisesta ulkopuoliselle asiantuntijalle annettavasta avustavasta arviointitehtävästä, josta säädettäisiin arviointilain 4 a §:ssä. Pykälän sisältöä täsmennettäisiin myös siten, että siinä tarkoitetut lausunnot hankittaisiin viranomaisilta. Liikenne- ja viestintävirasto voisi pyytää lausuntoja suojelupoliisin lisäksi esimerkiksi viranomaiselta, jolla on ohjaus- ja valvontatoimivalta haettuna pätevyysperusteena olevan sääntelyn osalta. Tällainen viranomainen olisi esimerkiksi Terveyden ja hyvinvoinnin laitos, kun kyse on sen antamien määräysten mukainen asiakastietojen käsittelyn arviointi, joka on säädetty hyväksytyn tietoturvallisuuden

arviointilaitoksen tehtäväksi laissa sosiaali- ja terveydenhuollon asiakastietojen käsittelystä (703/2023). Lisäksi 2 momenttiin lisättäisiin avustavaa tehtävää koskeva rikosoikeudellinen virkavastuu ja viittaus vahingonkorvauslakiin (412/1972).

5 § *Arviointilaitoksen hyväksyminen.* Pykälän *1 momentin 4 kohtaan* lisättäisiin tietoturvallisuuden arviointilaitoksen hyväksymisen edellytykseksi se, että laitoksen yritysturvallisuusselvityksestä ei ole ilmennyt mitään estettä, mikä kokonaisharkinnan perusteella vaarantaisi yrityksen tai vastuuhenkilöiden luotettavuuden tai sitoumustenhoitokyvyn arviointitehtävässä. Lisäksi 1 momentin 4 kohtaan lisättäisiin edellytys siitä, että laitoksella on luotettavaksi arvioitu ja valvottu menetelmä, jolla henkilökunnan luotettavuus varmistetaan. Arviointilaitoksella tulisi olla prosessit ja ohjeistus henkilöstöturvallisuudesta huolehtimiseksi. Henkilöstöturvallisuudella tarkoitetaan menettelyjä, joilla varmistetaan henkilöiden tietoturvavastuut ja velvollisuudet, tietoturvaosaaminen ja taustatarkastukset sekä avainhenkilöriskien hallinta. Lisäksi nämä menettelyt kattavat väärinkäytösten estämistä, kuten vaarallisten työyhdistelmien tunnistamista ja välttämistä, työtehtäväkiertoa, sekä työsuhteen tai sopimuksen päättymisen. Arviointilaitoksen hakiessa pätevyyttä, joka koskee turvallisuusluokitellun tiedon käsittelyn arviointia, olisi luotettavuuden arviointi tehtävä ehdotetun 4 §:n mukaisesti hakemalla yritysturvallisuusselvitys. Osana yritysturvallisuusselvitystä varmistetaan myös laitoksen toimitilojen ja tietojenkäsittelyn turvallisuus. Niissä tilanteissa kun, kun yritysturvallisuusselvitystä ei tehdä, tulee Liikenne- ja viestintäviraston muilla tavoin varmistua edellytysten täyttymisestä.

Pykälään lisättäisiin uusi *3 momentti*, jonka mukaan Liikenne- ja viestintävirasto voisi sen estämättä, mitä pykälän 2 momentissa säädetään, päättää hyväksytyn tietoturvallisuuden arviointilaitoksen uuden pätevyysalueen hyväksynnästä kuultuaan hyväksymisen kannalta keskeisiä viranomaisia. Voimassa olevan pykälän 2 momentin mukaan arviointilaitoksen riippumattomuus ja pätevyys osoitetaan vaatimustenmukaisuuden arviointipalvelujen pätevyyden toteamisesta annetussa laissa (920/2005) säädetyn menettelyn avulla eli kansallisen akkreditointiyksikön FINASin tekemällä akkreditoinnilla. Uuden momentin tarkoituksena olisi mahdollistaa lisäpätevyyksien hyväksyntä arviointilaitoksen hakemuksesta Liikenne- ja viestintäviraston päätöksellä sen sijaan, että FINAS vastaisi pätevyyden edellytysten selvittämisestä akkreditoinnilla. FINAS ei siten vastaisi myöskään näiden lisäpätevyyksien tai niiden ajantasaisuuden seurannasta, vaan se olisi kokonaisuudessaan Liikenne- ja viestintäviraston ohjaus- ja valvontatoiminnan vastuulla. Tietoturvallisuuden arviointilaitosten (lisä)pätevyystarpeet liittyvät usein viranomaisten tietojärjestelmien turvallisuusratkaisuihin ja niitä koskeviin säädöksiin ja säädösten soveltamista koskeviin viranomaisohjeisiin ja -menettelyihin, joilla on liityntä myös kansalliseen turvallisuuteen. Näiden pätevyystarpeiden erityisasiantuntemusta on lähinnä kapealla joukolla toimivaltaisia viranomaistoimijoita kuten Liikenne- ja viestintävirastolla tai tietyillä sosiaali- ja terveydenhuollon tietojärjestelmien vaatimuksenmukaisuudesta vastaavilla viranomaisilla. FINASin akkreditointiprosessi perustuu kansainvälisiin akkreditointistandardeihin, jotka soveltuvat erityyppisten markkinatoimijoiden tasalaatuisen ja vertailukelpoisen arvioinnin pätevyyksiin, mutta eivät tue kansallisen tietoturvallisuussääntelyn edellä kuvattuja erityispiirteitä. Hyväksytyksi tietoturvallisuuden arviointilaitokseksi hyväksyminen ja aseman säilyttäminen edellyttäisi jatkossakin voimassa olevaa FINASin akkreditointia jollekin riittävän yleiskäyttöiselle tietoturvallisuuden pätevyysalueelle, sillä akkreditointimenettely varmistaa osaltaan arviointilaitoksen kyvyn noudattaa johdonmukaisesti tasalaatuisuuden ja vertailukelpoisuuden turvaavia toimintaprosesseja. Siten jatkossakin olisi perusteltua edellyttää tietoturvallisuuden arviointilaitoksen hyväksynnässä esimerkiksi maailmanlaajuisesti yleisesti käytetyn tietoturvallisuuden ISO/IEC 27000 -standardisarjan pätevyyden akkreditointia. Akkreditointimenettelyä ei siis kuitenkaan välttämättä edellytettäisi, kun jo aiemmin hyväksytty arviointilaitos hakee jotakin lain 10 §:ssä säädetyn arviointiperusteen mukaista uutta pätevyysaluetta. Myös EU-sääntelyssä on tunnistettu toimivaltaisen viranomaisen tekemä pätevyyden hyväksyntä akkreditointiyksikön akkreditoinnin sijasta, esimerkiksi kyberkestävyyssäädöksen (EU) 2024/2847

(nk. CRA) 42 artiklassa säädetään tällaisesta vaihtoehdosta. Liikenne- ja viestintäviraston olisi kuultava lisäpätevyyden hyväksyntämenettelyn harkinnassa ja pätevyyden selvittämisessä pätevyyden hyväksymisen kannalta keskeisiä viranomaisia, joita olisivat tapauskohtaisesti esimerkiksi FINAS mahdollisesti soveltuvien standardien osalta ja ne viranomaiset, joiden viranomaistehtäviin haettu pätevyysperuste liittyy. Liikenne- ja viestintäviraston olisi kuulemisella ja muilla tarvittavilla selvityksillä varmistettava lisäpätevyys, ja että 1 momentin 1–3 kohtien vaatimusten täyttyminen ei lisäpätevyyden osalta vaarannu. Liikenne- ja viestintäviraston on hyvän hallinnon tasapuolisuusvaatimuksen mukaisesti varmistettava hakijoiden yhdenmukainen kohtelu. Siten tietyn lisäpätevyysalueen myöntämisen perusteiden ja -menettelyn tulisi olla samanlaiset kaikille hakijoille. Uudella menettelyllä halutaan myös keventää ja joustavoittaa uusien pätevyysalueiden hyväksyntäprosessia sekä vähentää arviointilaitoksille niistä aiheutuvia kustannuksia ja hallinnollista taakkaa.

Pykälän nykyinen 3 momentti siirrettäisiin 4 momentiksi ja 4 momentti 5 momentiksi. Pykälän 4 momenttiin tehtaisiin myös tekninen muutos, jossa Viestintävirasto päivitetään Liikenne- ja viestintävirastoksi.

6 § *Arviointilaitoksen hyväksymisen peruuttaminen.* Pykälää muutettaisiin siten, että Liikenne- ja viestintäviraston olisi mahdollista peruuttaa koko arviointilaitoshyväksynnän lisäksi yksittäinen arviointilaitokselle hyväksytty pätevyysalue. Arviointilaitoksen laiminlyönnit ja puutteet sen toiminnassa voivat liittyä arviointilaitoksena toimimiseen yleisemmin tai vain jonkin pätevyysalueen arviointeihin, jonka vuoksi hyväksynnän peruuttaminen tulisi voida rajata tarvittaessa vain osaan arviointilaitoksen toiminnasta, esimerkiksi yksittäisen hyväksytyn pätevyysalueen osalta. Pätevyysalueen hyväksynnän peruuttaminen mahdollistaisi toimintaan puuttumisen vain niiltä osin kuin se on tarpeen. Yksittäisen pätevyysalueen peruuttaminen tarkoittaisi sitä, että arviointilaitos voisi jatkaa arviointitoimintaansa niiden pätevyysalueiden osalta, joissa ei ole havaittu ongelmia tai puutteita. Pätevyysalueen hyväksynnän peruuttamisesta päättäisi Liikenne- ja viestintävirasto.

7 § *Liikenne- ja viestintäviraston tiedonsaanti- ja tarkastusoikeus.* Pykälän otsikkoa muutettaisiin siten, että Viestintävirasto muutettaisiin Liikenne- ja viestintävirastoksi ja otsikkoon lisättäisiin maininta Liikenne- ja viestintäviraston tiedonsaantioikeudesta.

Pykälän *1 momenttia* muutettaisiin siten, että pykälässä säädetty tarkastusoikeus koskisi Liikenne- ja viestintäviraston lisäksi, sen toimeksiannosta toimivan asiantuntijan sijaan, sitä avustavaa asiantuntijaa. Muutos vastaisi 4 §:n 2 momenttiin ehdotettavaa mahdollisuutta antaa vain avustavia tehtäviä ulkopuoliselle asiantuntijalle. Avustavassa tehtävässä toimivaa ulkopuolista asiantuntijaa voitaisiin käyttää arviointilaitoksen toimitiloja ja menetelmiä koskevassa tarkastuksessa.

Pykälään lisättäisiin uusi *2 momentti*, jossa säädettäisiin Liikenne- ja viestintäviraston tiedonsaantioikeuksista, joista on aiemmin säädetty voimassa olevan lain 8 §:n 2 momentissa. Liikenne- ja viestintäviraston toimivaltuuksia täydennettäisiin siten, että Liikenne- ja viestintävirastolla olisi jatkossa mahdollisuus saada salassapitosäännösten estämättä pyynnöstä tietoja, jotka ovat välttämättömiä sen valvomiseksi, että arviointilaitos täyttää toimintaansa koskevat vaatimukset. Tiedonsaantioikeus koskisi suojelupoliisilta, kansalliselta akkreditointiyksiköltä tai pätevyysalueen arviointiperustetta ohjaavalta tai valvovalta viranomaiselta, arviointilaitokselta tai sen asiakkaalta saatavia tietoja, jotka voivat olla salassa pidettäviä esimerkiksi liikesalaisuutena tai arviointilaitoksen asiakkaana olevien viranomaisten turvallisuusjärjestelyjä tai varautumista koskevina tietoina.

8 § *Arviointilaitoksen ilmoitusvelvollisuus.* Pykälän otsikosta poistettaisiin maininta arviointilaitoksen tiedonantovelvollisuudesta.

Pykälän *1 momenttiin* tehtäisiin tekninen muutos, jossa Viestintävirasto muutettaisiin Liikenne- ja viestintävirastoksi.

Pykälän *2 momentti* Liikenne- ja viestintäviraston tiedonsaantioikeudesta siirrettäisiin lain 7 §:n 2 momenttiin.

3 luvun otsikkoa ehdotetaan muutettavan ja siihen lisättäisiin varautuminen. Jatkossa luvun otsikko olisi Tietoturvallisuuden ja varautumisen arviointi.

9 § *Arviointilaitoksen tehtävät***.** Pykälän *1 momenttiin* lisättäisiin arviointilakiin ehdotettujen muutosten mukaisesti varautumisen arviointitehtävä. Pykälän 1 momentin 1 kohtaa muutettaisiin lisäksi siten, että toimitilat olisi tarkastettava niissä tilanteissa, kun se on tarpeen. Ehdotonta vaatimusta toimitilojen tarkastamisesta joka arvioinnin yhteydessä ei olisi. Arvioinnin pyytäjällä voi olla selvitys toimitilojen turvallisuudesta entuudestaan arviointilaitokselta tai viranomaiselta. Arvioinnin pyytäjällä voi olla myös jokin muu syy olla pyytämättä toimitilojen arviointia. Jatkossa erilaisten pilviteknologioiden ja muiden tietoverkkojen kautta tarjottavien palveluiden käytön oletetaan lisääntyvän entisestään, eikä käytännössä kaikissa tilanteissa ole mahdollista tarkastaa toimitilojen turvallisuutta samassa laajuudessa. On kuitenkin tärkeää, että arviointilaitokset huolehtivat, että mahdolliset rajaukset tarkastusten kattavuudessa käyvät selvästi ilmi arviointiraportista tai todistuksesta.

Pykälään lisättäisiin uusi *3 momentti*, jonka mukaan arviointilaitoksen olisi laadittava arviointiraportti. Arviointiraportti olisi laadittava kaikista arviointilaitoksen suorittamista arvioinneista ja siitä tulisi käydä ilmi käytetyt arviointiperusteet, arvioinnin laajuus eli esimerkiksi tekniset rajaukset tai todentamismenettelyihin liittyvät tiedot sekä tiedot havainnoista. Arviointiraporttiin voisi sisältyä myös arviointilaitoksen analyysi riskeistä, joita havaittuihin poikkeamiin voi liittyä. Ehdotettu muutos vastaisi arviointilakiin ehdotettua muutosta, mutta arviointilaitosten toimintaa koskevat menettelyvaatimukset säädettäisiin tältäkin osin arviointilaitoslaissa.

Pykälään lisättäisiin uusi *4 momentti*, joka vastaisi voimassa olevan pykälän 3 momenttia. Momenttia muutettaisiin siten, että hyväksytty tietoturvallisuuden arviointilaitos voisi jatkossa antaa todistuksen pyynnöstä tai jos niin erikseen säädetään. Hyväksytyn tietoturvallisuuden arviointilaitoksen antamaa todistusta koskevaa erityissääntelyä sisältyy esimerkiksi sosiaali- ja terveydenhuollon alan sääntelyyn. Jos todistusta koskevaa erityissääntelyä ei ole, arvioinnin pyytäjä voisi päättää, pyytääkö arviointiraportin lisäksi todistuksen. Todistuksen pyytäminen voi olla tarpeen esimerkiksi silloin, kun arvioinnin pyytäjällä on tarve osoittaa toimintansa tietoturvallisuus jollekin ulkopuoliselle. Pykälän 4 momenttia muutettaisiin myös siten, että arvioitavan kohteen toimitiloihin ja toimintaan viitattaisiin jatkossa ilmauksella arvioitava kohde. Muutoksen tarkoituksena olisi saattaa todistuksen antamisen edellytykset vastaamaan pykälän 1 momenttiin ehdotettavaa muutosta. Lisäksi pykälän 4 momentissa säädettyä listaa todistuksen sisällöstä täydennettäisiin ja todistukseen olisi jatkossa merkittävä sen voimassaoloaika. Todistuksen voimassaoloajan perusteella todistukseen luottava kolmas osapuoli voi arvioida, kuinka kauan arvioinnissa saatuun tietoon voi luottaa.

9 a § *Alihankinta.* Lakiin lisättäisiin uusi 9 a §, jossa säädettäisiin alihankintaa koskevista reunaehdoista. Pykälä selkeyttäisi hyväksytyn tietoturvallisuuden arviointilaitoksen toiminnan edellytyksiä, parantaisi sääntelyn ennakoitavuutta ja vähentäisi siten toiminnan suunnitteluun liittyviä tulkintakysymyksiä sekä edistäisi asiakkaiden luottamusta laitosten toimintaan.

Pykälän *1 momentissa* säädettäisiin siitä, että hyväksytty tietoturvallisuuden arviointilaitos voisi teettää arviointiin liittyvän tehtävän toisella konserniin kuuluvalla yhtiöllä tai muun alihankintana vain, jos konserniyhtiö tai muu alihankkija täyttää soveltuvilta osin tietoturvallisuuden arviointilaitoksen hyväksymisen edellytykset. Alihankintana pidettäisiin samaan konserniin kuuluvan tytär-, sisar- tai emoyhtiön käyttämistä tai muuta alihankkijaa. Lisäksi 1 momentissa säädettäisiin, että alihankinnasta tulisi antaa selvitys Liikenne- ja viestintävirastolle, jonka perusteella virasto arvioisi, täyttyvätkö alihankinnan edellytykset.

Alihankintana voitaisiin teettää vain sellaisia toimia, joissa hyväksytyllä arviointilaitoksella itsellään on pätevyys toimia ja sen tulee pystyä kontrolloimaan alihankkijan toimia kaikissa vaiheissa. Arviointilaitoksella säilyisi toimistaan kokonaisvastuu tilanteissa, joissa käytetään ulkopuolisia tahoja joissakin tehtävissä.

Pykälän *2 momentissa* säädettäisiin alihankinnan edellytyksistä turvallisuusluokitellun tiedon käsittelyn arviointiin liittyvien tehtävien osalta. Ehdotuksen mukaan tehtävien teettäminen alihankintana tai tytäryhtiöllä olisi mahdollista vain, jos siitä on sovittu erikseen asiakkaan kanssa. Sopimis- ja informointivelvollisuus alihankinnasta turvallisuusluokitellun tiedon käsittelyn arvioinnissa lisäisi arviointilaitoksen toiminnan läpinäkyvyyttä asiakasviranomaisille ja yrityksille.

10 § *Tietoturvallisuuden ja varautumisen arviointiperusteet.* Pykälän otsikkoon lisättäisiin varautuminen ehdotetun soveltamisalan muutoksen mukaisesti. Pykälässä säädettyjä tietoturvallisuuden ja varautumisen arviointiperusteita muutettaisiin siten, että ne ovat yhdenmukaiset arviointilain 7 §:ään ehdotettavien muutosten kanssa.

Pykälän *1 momentin* johtolauseeseen lisättäisiin maininta siitä, että arvioinnin kohteen valinnan eli pyynnön lisäksi käytettäviin arviointiperusteisiin vaikuttaa se, mitkä arviointiperusteet arviointilaitokselle on hyväksytty pätevyysalueina.

Momentin *1 kohtaa* muutettaisiin siten, että arviointiperusteena voitaisiin käyttää lailla tai asetuksella säädettyjä viranomaisten toimintaa koskevia tietoturvallisuus-, kyberturvallisuus- ja varautumisvaatimuksia ja viranomaisten ohjeita niiden soveltamisesta.

Vastaavasti kuin arviointilaitoslain osalta on ehdotettu, tiettyjen viranomaisen, kuten valtiovaranministeriön ja kansallisen turvallisuusviranomaisen ohjeiden mainitsemisen sijaan yleisesti viranomaisen ohjeet säädösten soveltamisesta oli riittävä ja yleispätevämpi määrittely. Näin ollen nykyinen 1 momentin 2 kohta sisältyisi muutettuun 1 kohtaan.

Momentin *2 kohta* vastaisi nykyistä 3 kohtaa, mutta siihen lisättäisiin Suomen Nato-jäsenyyden myötä Euroopan unionin lisäksi Pohjois-Atlantin liitto säännösten tai ohjeiden mahdollisena antajana. Momentin 1 kohdan tavoin myös 2 kohtaan lisättäisiin tietoturvallisuuden lisäksi kyberturvallisuus ja varautuminen. Vaikka arviointiperusteina säädetään kansainvälisistä lähteistä, mahdollisuuteen saada kansainvälisiin tietoturvallisuusvelvoitteisiin liittyviä pätevyyksiä turvallisuusluokitellun tiedon käsittelyn arviointiin vaikuttaa kansainvälisiä tietoturvallisuusvelvoitteita koskeva sääntely.

Momentin *3 kohta* vastaisi nykyistä 4 kohtaa ja momentin 4 kohta vastaisi nykyistä 5 kohtaa sillä erotuksella, että molempiin kohtiin lisättäisiin tietoturvallisuutta koskevien säännösten määräysten tai ohjeiden sekä vaatimusten lisäksi varautumista ja kyberturvallisuutta koskevat säännökset, määräykset tai ohjeet sekä vaatimukset.

11 § *Maksut.* Pykälän sanamuotoa ja viittausta valtion maksuperustelakiin (150/1992) päivitettäisiin vastaavasti kuin mitä arviointilakiin ehdotetaan. Lisäksi pykälää muutettaisiin siten, että Liikenne- ja viestintävirastolla olisi mahdollisuus periä tietoturvallisuuden arviointilaitoksen valvontaa koskevan asian käsittelystä maksu. Muutos vastaisi osittain nykytilaa ja se olisi yhtenevä Liikenne- ja viestintäviraston sähköiseen viestintään liittyvistä suoritteista perittävistä maksuista annetun asetuksen (1190/2023) 5 §:n kanssa, jonka mukaan Liikenne- ja viestintävirasto voi periä maksun jälkikäteisvalvontaan liittyvästä olennaisesta suoritteesta, tietoturvallisuuden arviointilaitosten hyväksyntään liittyvien toimenpiteiden lisäksi. Lisäksi pykälään tehtäisiin tekninen muutos, jossa Viestintävirasto muutettaisiin Liikenne- ja viestintävirastoksi.

12 § *Muutoksenhaku.* Pykälästä poistettaisiin viittaus kumottuun hallintolainkäyttölakiin (586/1996) ja lisättäisiin viittaus oikeudenkäynnistä hallintoasioissa annettuun lakiin (808/2019).

13 § *Virkavastuuta ja hyvää hallintoa koskevien säännösten soveltaminen.* Pykälän otsikkoa täydennettäisiin, ja siihen lisättäisiin maininta virkavastuuta koskevien säännösten soveltamisesta.

Pykälän *1 momentin* listaa sovellettavista hallinnon yleislaeista täydennettäisiin, ja momenttiin lisättäisiin viittaus saamen kielilakiin (1086/2003), tietosuojalakiin (1050/2019) sekä sähköisestä asioinnista viranomaistoiminnassa annettuun lakiin (13/2003). Voimassa olevan lain ja sen perustelujen mukaisesti (HE 45/2011 vp) hallinnon yleislakien soveltamista ei ole sidottu julkisen hallintotehtävän hoitamiseen, vaan niitä sovelletaan kaikkiin arviointilain mukaisten hyväksytyn tietoturvallisuuden arviointilaitosten tehtävien hoitamiseen.

Pykälään lisättäisiin uusi *2 momentti*, jossa säädettäisiin arviointilaitosten vastuuhenkilöiden ja henkilökunnan rikosoikeudellisesta virkavastuusta. Vastuuhenkilöiden ja henkilökunnan rikosoikeudellinen vastuu perustuisi siihen, että hyväksytyn tietoturvallisuuden arviointilaitoksen toiminta katsottaisiin julkiseksi hallintotehtäväksi. Lisäksi 2 momenttiin lisättäisiin viittaus vahingonkorvauslakiin.

7.3 Turvallisuusselvityslaki

18 § *Turvallisuusvaatimusten toteuttaminen yleisenä edellytyksenä*. Pykälän *2 momenttia* ehdotetaan muutettavaksi siten, että sen viittaus arviointilain mukaiseen todistukseen muutettaisiin arviointilain 8 §:n ehdotuksen mukaisesti arviointilain mukaiseen päätökseen tai lausuntoon.

48 § *Turvallisuusselvitysrekisteri, rekisterin käyttötarkoitus ja tietojen tallettaminen rekisteriin*. Pykälää ehdotetaan muutettavaksi siten, että sen 4 momentin 1 kohta kumotaan. Muutos on tarpeen, koska arviointilain 8 b § ehdotetaan kumottavaksi.

8 Lakia alemman asteinen sääntely

Esityksellä kumottaisiin voimassa olevan arviointilain 8 a §, jossa säädetään mahdollisuudesta säätää valtioneuvoston asetuksella velvollisuudesta hankkia todistus valtionhallinnon viranomaisen määräysvallassa olevasta tietojärjestelmästä tai tietoliikennejärjestelystä, jossa käsitellään turvallisuusluokkaan I tai II kuuluviksi luokiteltuja asiakirjoja. Tätä asetuksenantovaltuutta ei ole käytetty sen voimassaoloaikana.

9 Voimaantulo

Ehdotetaan, että lait tulevat voimaan x.x.2026.

Arviointilakia koskevat muutokset sisältäisivät siirtymäsäännöksiä, koska lain voimaantullessa kaikilla viranomaisilla ei ole valmiuksia tai mahdollisuuksia välittömästi soveltaa uutta lakia ja noudattaa sen säännöksiä. Viranomaisilla on käytössä huomattava määrä eri aikoina käyttöönotettuja tietojärjestelmiä ja tietoliikennejärjestelyitä, joiden tietoturvallisuuden arviointimenettelyjen saattamisen velvoitteiden mukaisiksi arvioidaan vievän useita vuosia järjestelmien kompleksisuuden vuoksi. Lisäksi vaadittavien arviointien saatavuudesta on epävarmuutta nykyisten taloudellisten ja arviointiresurssien niukkuuden vuoksi.

Arviointilakiin ehdotetaan siirtymäaikaa siten, että 3 §:n velvoitteita koskisi viiden vuoden siirtymäaika, jonka aikana viranomaisen olisi saatettava tietojärjestelmiensä ja tietoliikennejärjestelyjensä tietoturvallisuuden ja varautumisen arviointi vastaamaan 3§:ssä ehdotettua. Viranomaisen olisi kuitenkin pyydettävä arviointi tietojärjestelmälleen tai tietoliikennejärjestelylleen, jossa käsitellään turvallisuusluokkaan I tai II luokiteltuja tietoja 3 §:n 3 momentin ehdotetun mukaisesti kahden vuoden kuluessa lain voimaantulosta, ja pyydettävä tai hankittava arviointi tietojärjestelmälleen tai tietoliikennejärjestelylleen, jossa käsitellään turvallisuusluokkaan III luokiteltuja tietoja 3 §:n 4 momentissa ehdotetun mukaisesti kolmen vuoden kuluessa lain voimaantulosta.

Tietoturvallisuuden vaatimustenmukaisuudesta annetun todistuksen, joka on annettu voimassa olevan arviointilain mukaan, katsottaisiin vastaavan 8 §:ssä ehdotettua vaatimustenmukaisuudesta annettua päätöstä ja olevan voimassa todistukseen merkityn ajan. Siten jos tietojärjestelmästä tai tietoliikennejärjestelystä olisi voimassa oleva tietoturvallisuuden vaatimustenmukaisuutta osoittava todistus, järjestelmää ei tarvitsisi arvioida uudelleen tämän lain voimaan tullessa. Järjestelmän tietoturvallisuuden ylläpito olisi toteutettava 9 §:ssä ehdotetun mukaisesti

10 Suhde perustuslakiin ja säätämisjärjestys

Esitys sisältää perustuslain kannalta merkityksellisiä ehdotuksia suhteessa perustuslain 10 §:ssä turvattuun yksityiselämän, henkilötietojen ja luottamuksellisen viestinnän suojaan, perustuslain 15 §:ssä turvattuun omaisuudensuojaan, perustuslain 18 §:ssä turvattuun elinkeinovapauteen, sekä perustuslain 124 §:ssä hallintotehtävän antamisesta muulle kuin viranomaiselle säädettyyn.

Julkinen hallintotehtävä

Esityksessä ehdotetaan säädettäväksi arviointitoiminnassa avaustavasta tehtävästä arviointilain 4 a §:ssä ja Liikenne- ja viestintäviranomaisen tietoturvallisuuden arviointilaitosten hakemusten käsittelyissä avaustavasta tehtävästä arviointilaitoslain 4 §:n 2 momentissa. Ehdotukset ovat merkityksellisiä perustuslain 124 §:ssä kannalta, minkä mukaan julkinen hallintotehtävä voidaan antaa muulle kuin viranomaiselle vain lailla tai lain nojalla, jos se on tarpeen tehtävän tarkoituksenmukaiseksi hoitamiseksi eikä vaaranna perusoikeuksia, oikeusturvaa tai muita hyvän hallinnon vaatimuksia. Merkittävää julkisen vallan käyttöä sisältäviä tehtäviä voidaan kuitenkin antaa vain viranomaiselle. Arviointilain mukaisten arviointiviranomaisten tekemien arviointien lähtökohtana kuitenkin olisi, että ne itse suorittavat arvioinnin. Arviointia ei myöskään voisi siirtää ehdotetun 4 a §:n nojalla kokonaisuudessaan ulkopuolisen asiantuntijan suoritettavaksi, vaan vastuu arvioinnin toteuttamisesta säilyisi arviointiviranomaisella myös silloin, kun se olisi päättänyt käyttää apuna ulkopuolista asiantuntijaa. Sama koskisi myös arviointilaitoslain 4 §:n 2 momentin ehdotusta, jossa lähtökohtana olisi Liikenne- ja viestintäviraston vastuu hakemusten käsittelystä.

Perustuslakivaliokunta on lausuntokäytännössään todennut, että viranomaistehtävä voi olla tarkoituksenmukaista suorittaa viranomaisen siihen valtuuttaman asiantuntijan toimesta, kun tehtävän suorittamiseen liittyy ammatillisia ja teknisiä erityispiirteitä (PeVL 40/2002 vp, s.3, PeVL 44/2016 vp, s.5). Tarpeellisuusvaatimus voi täyttyä esimerkiksi silloin, kun tehtävän tekeminen edellyttää osaamista tai resursseja, joita viranomaisella ei ole (PeVL 29/2013 vp, s.2/I). Ehdotetun arviointilain 4 a §:n mukaan ulkopuolisen asiantuntijan käyttäminen olisi mahdollista, jos se on arvioinnin laadun, käytettävissä olevien voimavarojen tai arviointiin liittyvien teknisten syiden vuoksi tarpeellista. Ehdotetun arviointilain 4 a §:n 2 momentin mukaisesti arviointitehtäviä ulkoistettaisiin Teknologian tutkimuskeskus VTT Oy:lle käytännössä silloin, kun arviointi vaatisi sellaista teknistä erityisosaamista ja -resursseja, joihin arviointiviranomaisen ei ole mahdollista tai tarkoituksenmukaista resursoida.

Perustuslakivaliokunta on katsonut, että perusoikeuksien, oikeusturvan ja hyvän hallinnon vaatimusten turvaamisesta voidaan huolehtia asianomaisten henkilöiden pätevyyden ja sopivuuden avulla (PeVL 5/2006 vp, s. 8/I, PeVL 67/2002 vp, s. 5/I ja PeVL 2/2002 vp, s. 2/II). Ehdotetussa arviointilain 4 a §:n mukaan ulkopuolisella asiantuntijalla olisi oltava tehtävään tarvittava koulutus.

Perusoikeuksien, oikeusturvan ja hyvän hallinnon osalta perustuslakivaliokunta on lisäksi katsonut, että tarkastuksessa noudatetaan hallinnon yleislakeja ja että asioita käsitellään virkavastuulla (PeVL 20/2006 vp, s. 2, PeVL 46/2002 vp, s. 10, PeVL 33/2004 vp, s. 7/II, PeVL 11/2006 vp, s. 3). Ehdotettujen arviointilain 4 a §:n ja arviointilaitoslain 4 §:n 2 momentin mukaan ulkopuoliseen asiantuntijaan ja Teknologian tutkimuskeskus VTT Oy:n työntekijään sovellettaisiin rikosoikeudellista virkavastuuta koskevia säännöksiä heidän hoitaessaan kyseisten pykälien mukaisia tehtäviä. Lakiin ei enää nykyisin ole välttämätöntä sisällyttää perustuslain 124 §:ään perustuvaa viittausta hallinnon yleislakeihin, mikäli ehdotuksesta käy selvästi ilmi, että hallinnon yleislakeja sovelletaan perustuslain 124 §:ssä tarkoitettuun toimintaan (PeVL 20/2006 vp, s.2) Hallinnon yleislakeja sovelletaan silloin, kun kyse on julkisuuslain 4 §:n 2 momentin mukaisesta toimijasta. Arviointilaitoslain 13 §:n viittausta hallinnon yleislakeihin ehdotetaan kuitenkin säilytettävän ja täydennettävän siten, että listasta tulee kattava. Tämä siitä syystä, että voimassa olevan arviointilaitoslain esitöiden mukaan hallinnon yleislakien soveltamista ei ole sidottu julkisen hallintotehtävien hoitamiseen, vaan niitä sovelletaan kaikkien arviointilaitoslain mukaisien tehtävien hoitamisessa.

Elinkeinovapaus

Esitys sisältää ehdotuksia, jotka ovat merkityksellisiä perustuslain 18 §:n 1 momentissa säädetyn elinkeinovapauksen näkökulmasta. Elinkeinovapaudella turvataan jokaiselle oikeus lain mukaan hankkia toimeentulonsa valitsemallaan työllä, ammatilla tai elinkeinolla. Säädös mahdollistaa elinkeinovapauden rajoittamisen, mutta edellyttää, että rajoittaminen toteutetaan lain tasolla. Sääntelyn tulee täyttää myös muut perusoikeutta rajoittavalta lailta vaadittavat yleiset edellytykset. Elinkeinovapauden rajoitusten tulee olla täsmällisiä ja tarkkarajaisia, minkä lisäksi rajoittamisen laajuuden ja edellytysten pitää ilmetä laista. (PeVL 16/2003 vp s. 2)

Arviointilain 3 a §:ssä säädettäisiin uudistetuista arviointimenettelyistä, joihin lisättäisiin arviointimenettelyiksi viranomaisen toteuttama itsearviointi ja viranomaisen toimeksiannosta palveluntarjoajan toteuttama arviointi voimassa olevan lain mukaisten arviointimenettelyiden, eli tietoturvallisuuden arviointilaitoksen ja arviointiviranomaisen tekemän arvioinnin lisäksi. Esityksen tarkoituksena on parantaa arviointien sujuvuutta ja saatavuutta avaamalla arviointitoiminta tietyiltä osin myös yksityisille palveluntarjoajille. Viranomaisen toimeksiannosta toimivan palveluntarjoajan kannalta sääntely on merkityksellinen myös perustuslain 18 §:n 1 momentissa säädetyn elinkeinovapauden näkökulmasta. Arviointilain ehdotettu muutos

mahdollistaisi uutta liiketoimintaa arviointipalveluita tarjoaville yrityksille. Toisaalta palveluntarjoajien toteuttamat arvioinnit rajattaisiin tietojärjestelmiin, joissa käsitellään julkisia, salassa pidettäviä ja korkeintaan turvallisuusluokkaan IV luokiteltuja tietoja. Rajoitus perustuisi siihen, että turvallisuusluokitellun tiedon käsittelyyn liittyvät korkeammat tiedon suojaamisvaatimukset, rajatummat käyttöoikeudet sekä suuremmat riskit, jos tieto oikeudettomasti paljastauisi. Palveluntarjoajien on lisäksi mahdollista hakea tietoturvallisuuden arviointilaitoksiksi, jos ne haluaisivat arvioida turvallisuusluokkaan III luokiteltuja tietoja käsitteleviä tietojärjestelmiä ja tietoliikennejärjestelyjä.

Esitykseen sisältyy myös ehdotus tietoturvallisuuden arviointilaitosten arviointitoiminnan rajaamisesta tietojärjestelmiin ja tietoliikennejärjestelyihin, joissa käsitellään korkeintaan turvallisuusluokkaan III luokiteltuja tietoja. Kyseessä on voimassa olevan menettelyn säätäminen lakiin, sillä tietoturvallisuuden arviointilaitoksille ei ole myönnetty turvallisuusluokkaa III korkeampaan turvallisuusluokkaan luokiteltuja tietoja sisältävien tietojärjestelmien arviointipätevyyttä. Tätä perustellaan turvallisuusluokkiin I ja II luokiteltuja tietoja käsittelevien tietojärjestelmien ja tietoliikennejärjestelyjen erityisen suurella ja merkittävällä riskitasolla sekä sillä erityisellä osaamisella, joka arviointiviranomaisella on turvallisuusluokkiin I ja II luokiteltuja tietoja käsittelevien tietojärjestelmien ja tietoliikennejärjestelyjen toiminnallisista vaatimuksista, toimintaympäristöstä ja turvallisuusjärjestelystä.

Tietoturvallisuuden arviointilaitosten hyväksymismenettelyn suhdetta perustuslain vaatimuksiin on kuvattu voimassa olevan arviointilaitoslain esitöissä (HE 45/2011 vp s. 13). Nyt ehdotettavassa arviointilaitoslain muutoksessa arviointilaitoslain 3 §:ään lisättäisiin mahdollisuus hakea hyväksyntä toiminnan lisäksi yksittäiselle pätevyysalueelle. Ehdotuksen on tarkoitus laajentaa arviointilaitosten toimintamahdollisuuksia. Arviointilaitoslain 4 §:ään ehdotetaan lisättäväksi yritysturvallisuusselvityksen teettäminen osaksi arviointilaitoksen hyväksyntäprosessia, kun kyseessä on turvallisuusluokitellun tiedon käsittelyn arvioinnin pätevyysalue. Ehdotettujen muutosten ei kuitenkaan arvioida vaikuttavan voimassa olevan arviointilaitoslain säätämisen yhteydessä esitettyyn elinkeinovapauteen liittyvään perustuslailliseen arvioon, koska arviointilaitosten hyväksymisprosessi pysyisi samana edellä esitettyjä lisäyksiä lukuun ottamatta.

Ehdotettu arviointilain 4 § loisi turvallisuuskriittisten ratkaisujen valmistajalle mahdollisuuden hakea Suomessa valmistetun turvallisuuskriittisen ratkaisun tietoturvallisuuden vaatimuksenmukaisuutta koskevaa arviointia. Laissa ei kuitenkaan säädettäisi vaatimuksenmukaisuuden arviointia markkinoille pääsyn edellytykseksi. Päätöksen peruuttaminen saattaisi kuitenkin edellä sanotusta huolimatta käytännössä vaikuttaa turvallisuuskriittisen ratkaisujen valmistajan toimintaan. Siksi päätöksen peruuttaminen voi olla merkityksellistä perustuslain 18 §:ssä turvatun elinkeinovapauden kannalta, vaikka ehdotuksessa ei ole kyse elinkeinotoimintaan vaadittavasta luvasta. Perustuslakivaliokunta on elinkeinotoiminnan sääntelyn yhteydessä vakiintuneesti pitänyt elinkeinotoimintaan vaadittavan luvan peruuttamista yksilön oikeusasemaan puuttuvana viranomaistoimena vaikutuksiltaan jyrkempänä kuin haetun luvan epäämistä. Sen vuoksi valiokunta on katsonut sääntelyn oikeasuhtaisuuden kannalta välttämättömäksi sitoa luvan peruuttamismahdollisuus vakaviin tai olennaisiin rikkomuksiin tai laiminlyönteihin sekä siihen, että luvanhaltijalle mahdollisesti annetut huomautukset tai varoitukset eivät ole johtaneet toiminnassa esiintyneiden puutteiden korjaamiseen (PeVL 20/2006 vp, s. 3/I). Vaikka turvallisuuskriittisen ratkaisun arviointi ei olisikaan edellytys elinkeinotoiminnan harjoittamiseksi, arviointilain 10 §:ään sisältyy ehdotus, että ennen päätöksen mahdollista perumista, päätöksen saanutta kuultaisiin ja tälle varattaisiin tilaisuus korjata puute.

Esityksen edellä kuvatut elinkeinovapauden kannalta merkitykselliset, ja sitä mahdollisesti rajoittavat ehdotukset säädettäisiin kaikki lain tasolla siten, että niiden edellytykset ilmensivät laista.

Tiedonsaantioikeudet

Perustuslakivaliokunta on käytännössään katsonut, että salassapitosäännösten edelle menevässä tietojensaantioikeudessa on viime kädessä kysymys siitä, että tietoihin oikeutettu viranomainen omine tarpeineen syrjäyttää ne perusteet ja intressit, joita tietoja hallussaan pitävään viranomaiseen kohdistuvalla salassapitovelvollisuudella suojataan. Perustuslakivaliokunta on lisäksi tietojen saamista ja luovuttamista koskevaa sääntelyä perustuslain 10 §:n 1 momentissa säädetyn yksityiselämän ja henkilötietojen suojan kannalta arvioidessaan kiinnittänyt huomiota muun muassa siihen, mihin ja ketä koskeviin tietoihin tiedonsaantioikeus ulottuu ja miten tietojensaantioikeus sidotaan tietojen välttämättömyyteen. Tällöin tietojensaanti- ja luovuttamismahdollisuus on voinut liittyä jonkin tarkoituksen kannalta ”tarpeellisiin tietoihin”, jos tarkoitetut tietosisällöt on pyritty luettelemaan laissa tyhjentävästi. Jos taas tietosisältöjä ei ole samalla tavoin luetteloitu, sääntelyyn on pitänyt sisällyttää vaatimus ”tietojen välttämättömyydestä” jonkin tarkoituksen kannalta (mm. PeVL 10/2014 vp, s. 6/II, PeVL 19/2012 vp, s. 3—4 ja PeVL 62/2010 vp, s. 4/I).

Esitykseen sisältyy ehdotus arviointilain 4 b §:n mukaisten arviointiviranomaisten, eli Liikenne- ja viestintäviraston ja Puolustusvoimien Pääesikunnan määrätyn turvallisuusviranomaisen välisestä yhteistyöstä ja arviointi- ja koordinointitehtävien hoitamiseksi välttämättömien tietojen tiedonsaantioikeudesta sen estämättä, mitä salassapitovelvollisuudesta säädetään. Arviointilaitoslain 7 §:ään ehdotetaan lisättävän Liikenne- ja viestintävirastolle tiedonsaantioikeudet suojelupoliisilta, kansalliselta akkreditointiyksiköltä tai pätevyysalueen arviointiperustetta valvovalta viranomaiselta, arviointilaitokselta tai sen asiakkaalta salassapitosäännösten estämättä niistä tiedoista, jotka ovat välttämättömiä sen valvomiseksi, että laitos täyttää toimintaansa koskevat vaatimukset. Molemmissa tilanteissa edellytyksenä olisi tiedon välttämättömyys viranomaiselle säädettyjen tehtävien hoitamista varten. Välttämättömyys edellyttäisi, että tarkoitusta, jota varten näitä tietoja pyydettäisiin, ei olisi saavutettavissa ilman esimerkiksi tieto- ja viestintäjärjestelmien turvajärjestelyjä, onnettomuuksiin tai poikkeusoloihin varautumista koskevia tietoja taikka tietoja, joihin liittyy yksityisiä liike- tai ammattisalaisuuksia.

Lisäksi esitykseen sisältyy arviointilain 6 §:n muutos, jossa listausta arviointiviranomaisen tiedonsaantioikeuden kohteista ehdotetaan tarkennettavaksi. Lisäksi tiedonsaantioikeudet ja pääsy tietojärjestelmään, tietoliikennejärjestelyyn ja tiloihin ehdotetaan sidottavan tarpeellisuuskriteerin sijasta välttämättömyyskriteeriin tehtävien suorittamiseksi. Näin suojattaisiin paremmin niitä intressejä, joita tietoja ja järjestelmiä hallussaan pitävään viranomaiseen ja yritykseen kohdistuvalla salassapitovelvollisuudella suojataan.

Kotirauha

Arviointilain 6 §:n 1 momentin oikeutta päästä tiloihin, joissa tietojärjestelmään, tietoliikennejärjestelyyn tai turvallisuuskriittisen ratkaisun tietoja käsitellään, laajennettaisiin siten, että kaikilla lain mukaisilla arviointiviranomaisilla olisi pykälän mukainen tarkastusoikeus. Lisäksi 6 § toiseen momenttiin lisättäisiin oikeus tehdä tarkastus hajasäteilysuojaratkaisun valmistajan ja sen alihankkijan tiloihin. Säännökset ovat merkityksellinen perustuslain 10 §:n 1 momentissa säädetyn kotirauhan näkökulmasta. Voimassa olevan arviointilain säätämisen yhteydessä 6 § tarkastusoikeutta on arvioitu perustuslain näkökulmasta ja todettu, että tarkastusta ei ole tarkoitus eikä tarpeen ulottaa kotirauhan piiriin kuuluviin tiloihin. Selvyyden vuoksi ja kotirauhaa koskevien perustuslain säännösten huomioon ottamiseksi säännöksessä nimenomaisesti rajattu tällaiset tilat tarkastusoikeuden ulkopuolelle (mm. PeVL 2/2002 vp, PeVL 18/2006 vp). Tätä rajausta ei ole tarkoitus 6 §:n 1 momentin tarkastusoikeuden osalta muuttaa tämän esityksen yhteydessä, ja se on tarkoitus ulottaa myös koskemaan esitettyä 6 §:n 2 momentin mukaista tarkastusoikeutta.

Omaisuudensuoja

Arviointilain 6 §:ssä säädettäisiin arviointiviranomaisen mahdollisuudesta suorittaa arvioinnin kannalta tarvittavia tarkastustoimenpiteitä. Ehdotus on merkityksellinen perustuslain 15 §:n 1 momentissa turvatun omaisuuden suojan näkökulmasta. Omaisuudensuoja sisältää paitsi omistajalle lähtökohtaisesti kuuluvan vallan hallita, käyttää ja hyödyntää omaisuuttaan haluamallaan tavalla myös vallan määrätä siitä (PeVL 41/2006 vp, s. 2, PeVL 49/2005 vp, s. 2, PeVL 15/2005 vp, s. 2). Perustuslakivaliokunnan käytännön mukaan omistajan oikeuksia voidaan rajoittaa lailla, kunhan sääntely täyttää perusoikeuksien yleiset rajoitusedellytykset.

Tarkastustoimenpiteiden tekeminen ja siihen kuuluva tekninen testaus on välttämätön menettely tietojärjestelmien, tietoliikennejärjestelyjen ja turvallisuuskriittisten ratkaisujen tietoturvallisuuden arvioinnissa. Teknisesti testaamalla voidaan todentaa asiakirjojen perusteella saatua selvitystä ja havainnoida tietojärjestelmän tai turvallisuuskriittisen ratkaisun kyvykkyyttä erilaisilta tietoturvallisuusuhkilta suojautumisessa.

Ehdotuksen arvioidaan olevan perusoikeuksien yleisten rajoitusedellytysten kannalta täsmällisiä ja tarkkarajaisia sekä riittävän oikeasuhtaisia suhteessa niihin tavoitteisiin, joita esityksen taustalla on. Tarkastustoimenpiteiden suorittaminen on sidottu tarpeellisuusvaatimukseen, siitä säädetään laintasoisesti eikä sillä puututa omaisuudensuojan ydinalueelle.

Hallituksen käsityksen mukaan lakiehdotukset voidaan edellä todetun perusteella käsitellä tavallisen lain säätämisjärjestyksessä.

Ponsi

Edellä esitetyn perusteella annetaan eduskunnan hyväksyttäviksi seuraavat lakiehdotukset:

1.

Laki

viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti

kumotaan viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annetun lain (1406/2011) 8 a ja 8 b §, sellaisina kuin ne ovat laissa 728/2014,

muutetaan 1–8 ja 9–12 §, sellaisena kuin niistä 1 § on osaksi laissa 728/2014, sekä

lisätään lakiin uusi 3 a, 4 a, 4 b, 7 a ja 8 c § seuraavasti:

1 §

Lain soveltamisala

Tässä laissa säädetään viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden ja varautumisen arvioinnista. Lisäksi tässä laissa säädetään turvallisuuskriittisten ratkaisujen ja niiden valmistuksen arvioinnista.

Tätä lakia sovelletaan tietoturvallisuuden arviointiin, jollei kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa (588/2004) toisin säädetä tai sen mukaisesta kansainvälisestä tietoturvallisuusvelvoitteesta muuta johdu.

Liikenne- ja viestintäviraston tehtävistä yritysturvallisuusselvitystä laadittaessa säädetään turvallisuusselvityslaissa (726/2014).

2 §

Määritelmät

Tässä laissa tarkoitetaan:

1) *tietojärjestelmällä* tietojenkäsittelylaitteista, ohjelmistoista ja muusta tietojenkäsittelystä koostuvaa kokonaisjärjestelyä;

2) *tietoliikennejärjestelyllä* tiedonsiirtoverkosta, tiedonsiirtolaitteista, ohjelmistoista ja muusta tietojenkäsittelystä sekä niihin liittyvistä menettelyistä koostuvaa kokonaisjärjestelyä;

3) *viranomaisella* viranomaisten toiminnan julkisuudesta annetun lain (621/1999) 4 §:n 1 momentissa tarkoitettuja viranomaisia;

4) *valtionhallinnon viranomaisella* valtion hallintoviranomaisia ja muita valtion virastoja ja laitoksia sekä tuomioistuimia ja muita lainkäyttöviranomaisia;

5) *tietoturvallisuudella* tiedon saatavuuden, eheyden ja luottamuksellisuuden suojaamista hallinnollisilla, toiminnallisilla ja teknisillä toimenpiteillä;

6) *varautumisella* toimia, joilla huolehditaan, että tietojärjestelmien ja tietoliikennejärjestelyjen hyödyntäminen ja niihin perustuva toiminta jatkuvat mahdollisimman häiriöttömästi normaaliolojen häiriötilanteissa sekä valmiuslaissa (1552/2011) tarkoitetuissa poikkeusoloissa;

7) *tietoturvallisuuden arviointilaitoksella* tietoturvallisuuden arviointilaitoksista annetussa laissa (1405/2011) tarkoitettua yritystä, yhteisöä tai viranomaista, jonka Liikenne- ja viestintävirasto on hyväksynyt;
8) *turvallisuusluokalla*, julkisen hallinnon tiedonhallinnasta annetun lain (906/2019) 18 §:n 4 momentin nojalla säädetyn valtioneuvoston asetuksen mukaisia turvallisuusluokkia
9) *turvallisuuskriittisellä ratkaisulla* salaus-, hajasäteilysuojaus- ja muuta tieto- ja viestintäteknistä ratkaisua, jolla suojataan turvallisuusluokiteltua tietoa tietojärjestelmissä ja tietoliikennejärjestelyissä;
10) *turvallisuuskriittisen ratkaisun valmistajalla* yritystä, joka vastaa turvallisuuskriittisen ratkaisun kehittämisestä, suunnittelusta, valmistamisesta, kokoamisesta ja ylläpidosta.

3 §

Tietoturvallisuuden ja varautumisen arviointi

Tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden ja varautumisen arviointimenettelyjä ovat:
1) viranomaisen toteuttama itsearviointi;
2) viranomaisen toimeksiannosta palveluntarjoajan toteuttama arviointi;
3) tietoturvallisuuden arviointilaitoksen toteuttama arviointi; sekä
4) arviointiviranomaisen toteuttama arviointi.

Valtionhallinnon viranomaisen on arvioitava tietojärjestelmiensä ja tietoliikennejärjestelyjensä tietoturvallisuutta ja varautumista käyttäen 1 momentin mukaisia menettelyjä. Valtionhallinnon viranomaisen on valittava arviointimenettely tietojärjestelmän tai tietoliikennejärjestelyn riskiarvioinnin perusteella ja toteutettava vähintään tietojärjestelmiensä ja tietoliikennejärjestelyjensä itsearviointeja.

Sen lisäksi, mitä 2 momentissa säädetään, viranomaisen on pyydettävä arviointiviranomaisen arviointi tietojärjestelmälleen tai tietoliikennejärjestelylleen, jossa käsitellään turvallisuusluokkaan I tai II luokiteltuja tietoja.

Sen lisäksi, mitä 2 momentissa säädetään, viranomaisen on pyydettävä arviointiviranomaisen tai hankittava tietoturvallisuuden arviointilaitoksen arviointi tietojärjestelmälleen tai tietoliikennejärjestelylleen, jossa käsitellään turvallisuusluokkaan III luokiteltuja tietoja, ellei se päätä arvioinnin pyytämisen tai hankkimisen olevan tietojärjestelmän tai tietoliikennejärjestelyn riskiarvioinnin perusteella tarpeetonta.

Viranomainen voi hankkia toimeksiannosta 1 momentin 2 kohdan mukaisesti toimivalta palveluntarjoajalta arvioinnin tietojärjestelmälle ja tietoliikennejärjestelylle, jossa käsitellään julkisia, salassa pidettäviä ja korkeintaan turvallisuusluokkaan IV luokiteltuja tietoja. Viranomaisen on ennakolta arviointipalveluja hankkiessaan varmistuttava palveluntarjoajan luotettavuudesta toimeksiannon edellyttämässä laajuudessa.

Viranomainen voi hankkia tietoturvallisuuden arviointilaitokselta arvioinnin tietojärjestelmälle tai tietoliikennejärjestelylle, jossa käsitellään korkeintaan turvallisuusluokkaan III luokiteltuja tietoja.

Viranomainen voi pyytää arviointiviranomaisen hyväksyntää tietojärjestelmälleen tai tietoliikennejärjestelylleen osoittaakseen tietoturvallisuutta koskevien vaatimusten täyttymisen

Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain tarkoittamissa tilanteissa tai jos muutoin kansainvälinen yhteistyö sitä edellyttää taikka jos vaatimustenmukaisuuden osoittamisesta erikseen säädetään.

3 a §

Arviointiviranomaiset

Arviointiviranomaisia ovat Liikenne- ja viestintävirasto ja Pääesikunnan määrätty turvallisuusviranomainen. Pääesikunnan määrätyn turvallisuusviranomaisen arviointitehtäviä voi myös hoitaa sen nimeämä sekä ohjauksessa ja valvonnassa toimiva Puolustusvoimien palkattuun henkilöstöön kuuluva henkilö.

Arviointiviranomaisen on organisaatioltaan ja päätöksenteoltaan oltava riippumaton sille kuuluvien arviointitehtävien hoitamisessa. Lisäksi arviointiviranomaisen on huolehdittava tehtävistään teknisen kehityksen edellyttämällä ammattitaidolla.

Arvioinnin tekeminen kuuluu Liikenne- ja viestintäviraston toimivaltaan, jollei arvioinnin tekeminen kuulu Pääesikunnan määrätyn turvallisuusviranomaisen toimivaltaan 4 momentin nojalla.

Arvioinnin tekeminen kuuluu Pääesikunnan määrätyn turvallisuusviranomaisen toimivaltaan, jos arviointi koskee Puolustusvoimien tietojärjestelmien tai tietoliikennejärjestelyjen taikka niihin kuuluvien turvallisuuskriittisten ratkaisujen tietoturvallisuuden ja varautumisen tasoa tai vaatimuksenmukaisuutta.

4 §

Arviointiviranomaisen tehtävät

Arviointiviranomaisen tehtävänä on viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden edistämiseksi ja varmistamiseksi:

1) arvioida viranomaisen pyynnöstä tietojärjestelmän tai tietoliikennejärjestelyn taikka niihin kuuluvan turvallisuuskriittisen ratkaisun tietoturvallisuutta ja varautumista;

2) antaa 3 §:n 7 momentin mukaisesta viranomaisen pyynnöstä hyväksyntä tietojärjestelmälle tai tietoliikennejärjestelylle, joka täyttää tietoturvallisuusvaatimukset; ja

3) antaa arvioinnista arviointiraportti ja tarvittaessa hyväksyntäpäätös tai -lausunto 8 §:ssä säädetyllä tavalla.

Sen lisäksi mitä 1 momentissa säädetään, Liikenne- ja viestintäviraston tehtävänä on:

1) arvioida Suomeen sijoittautuneen turvallisuuskriittisten ratkaisujen valmistajan hakemuksesta Suomessa valmistetun turvallisuuskriittisen ratkaisun tietoturvallisuuden vaatimuksenmukaisuutta;

2) antaa tietojärjestelmien, tietoliikennejärjestelyjen ja turvallisuuskriittisten ratkaisujen tietoturvallisuustoimenpiteisiin ja tietoturvallisuuden arviointiin liittyvää neuvontaa;

3) tehdä valtiovarainministeriön pyynnöstä selvityksiä valtionhallinnon viranomaisen määräämisvallassa olevien tietojärjestelmien tai tietoliikennejärjestelyjen yleisestä tietoturvallisuuden ja varautumisen tasosta; ja

4) ohjata ja valvoa hajasäteilysuojausratkaisuja valmistavan turvallisuuskriittisen ratkaisun valmistajan toimintaa ja antaa tarvittaessa päätös valmistuksen toimenpiteiden tai ratkaisun vaatimuksista.

Liikenne- ja viestintävirasto asettaa tässä laissa sille tarkoitetut arviointiviranomaisen tehtävät tärkeysjärjestykseen ja päättää arvioinnin tekemisestä käytettävissään olevien voimavarojen mukaisesti ottaen huomioon kansainvälisten tietoturvallisuusvelvoitteiden noudattaminen, tämän lain 3 §:ssä säädetyt arviointimenettelyvelvoitteet, tiedon turvallisuusluokka ja muun riippumattoman arvioinnin saatavuus, suomalaisten turvallisuuskriittisten ratkaisujen tarjonnan edistäminen, arvioinnin pyytäjien ja hakijoiden yhdenvertainen kohtelu sekä pyydettyjen toimenpiteiden yleinen merkitys viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden yleiseen parantamiseen taikka yhteiskunnan elintärkeiden toimintojen suojaamiseen.

Edellä 1 momentin 1 ja 2 kohdassa tarkoitetun pyynnön Liikenne- ja viestintävirastolle voi tehdä viranomainen tai sen toimeksiannosta myös se, joka tekee viranomaisen lukuun hankintoja taikka tuottaa tietojenkäsittely- tai tietoliikennepalveluja taikka hoitaa niiden järjestämiseen liittyviä palvelutehtäviä.

4 a §

Arviointiviranomaista avustava tehtävä

Jos se on arvioinnin laadun, käytettävissä olevien voimavarojen tai arviointiin liittyvien teknisten syiden vuoksi tarpeellista, arviointiviranomainen voi käyttää arvioinnissa apuna ulkopuolista asiantuntijaa. Asiantuntijalla on oltava sellainen koulutus ja kokemus kuin tehtävässä on tarpeen. Ulkopuoliseen asiantuntijaan sovelletaan rikosoikeudellista virkavastuuta koskevia säännöksiä hänen hoitaessaan tämän pykälän mukaisia tehtäviä. Vahingonkorvausvastuusta säädetään vahingonkorvauslaissa (412/1974).

Teknologian tutkimuskeskus VTT Oy:n tehtävänä on arvioida turvallisuuskriittisiä ratkaisuja arviointiviranomaisen toimeksiannosta. Teknologian tutkimuskeskus VTT Oy:n työntekijään sovelletaan mitä 1 momentissa säädetään.

4 b §

Arviointiviranomaisten tiedonvaihto ja yhteistyö

Arviointiviranomaisten on toimittava yhteistyössä tämän lain mukaisten tehtävien hoitamiseksi ja annettava toisilleen tässä tarkoituksessa välttämättömät tiedot sen estämättä, mitä salassapitovelvollisuudesta säädetään.

Sen estämättä, mitä 4 §:n 1 momentissa ja 2 momentissa säädetään, arviointiviranomaiset voivat sopia tietyn tämän lain mukaisen tehtävän tai sen osan hoitamisesta toisen arviointiviranomaisen lukuun, jos järjestely on tarpeen tehtävien hoitamiseksi tarkoituksenmukaisesti, taloudellisesti ja joutuisasti.

Liikenne- ja viestintäviraston on koordinoitava arviointiviranomaisten yhteistyötä yhtenäisen soveltamiskäytännön luomiseksi.

5 §

Selvitykset valtiovarainministeriön toimeksiannosta

Valtiovarainministeriö voi pyytää valtionhallinnon tietoturvallisuudesta annettujen säännösten toimeenpanon seuraamiseksi sekä niiden kehittämiseksi Liikenne- ja viestintävirastoa laatimaan selvityksiä valtionhallinnon viranomaisten tietojärjestelmien tai tietoliikennejärjestelyjen yleisestä tietoturvallisuuden ja varautumisen tasosta. Selvityksen piiriin tulevat tietojärjestelmät voidaan määritellä tietojärjestelmien käyttötarkoituksen, niihin talletettavien tietojen laadun tai muun vastaavan yleisen tekijän mukaan.

Liikenne- ja viestintävirasto voi salassapitosäännösten estämättä sisällyttää valtiovarainministeriölle antamaansa selvitykseen sellaisia tietoja, jotka ovat välttämättömiä arvioinnin tarkoituksen toteuttamiseksi.

6 §

Arviointiviranomaisen tarkastusoikeus, tiedonsaantioikeus ja oikeus päästä tiloihin ja tietojärjestelmiin

Arviointiviranomaisella ja sitä avustavalla asiantuntijalla on oikeus salassapitosäännösten tai muiden tiedon luovuttamista koskevien rajoitusten estämättä saada käyttöönsä tämän lain mukaisten tehtäviensä suorittamiseksi välttämättömät tietojärjestelmää, tietoliikennejärjestelyä tai turvallisuuskriittistä ratkaisua ja sen valmistusta koskevat tiedot, asiakirjat, laitteet ja ohjelmistot sekä oikeus siinä laajuudessa kuin se on välttämätöntä tehtävien suorittamiseksi päästä tietojärjestelmään, tietoliikennejärjestelyyn tai tiloihin, joissa arviointikohteeseen kuuluvia tietoja käsitellään, sekä suorittaa tarvittavia hallinnollisia ja teknisiä arviointitoimenpiteitä.

Liikenne- ja viestintävirastolla tai sitä avustavalla asiantuntijalla on oikeus tehdä hajasäteilysuojausratkaisun valmistajan ja sen alihankkijan tiloissa tarkastus sen selvittämiseksi, noudattaako se tämän lain nojalla annettuja päätöksiä. Liikenne- ja viestintäviraston oikeuteen päästä tiloihin ja saada tutkittavakseen välttämättömät tiedot sekä suorittaa arviointitoimenpiteitä sovelletaan, mitä 1 momentissa säädetään. Tarkastuksesta säädetään hallintolain (434/2003) 39 §:ssä.

Edellä 1 ja 2 momentissa tarkoitettua tarkastusta ei saa suorittaa pysyväisluonteiseen asumiseen käytetyissä tiloissa.

7 §

Tietoturvallisuuden ja varautumisen arviointiperusteet

Tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden ja varautumisen arviointiperusteina voidaan käyttää:

1) lailla tai asetuksella säädettyjä viranomaisten toimintaa koskevia tietoturvallisuus-, kyberturvallisuus- tai varautumisvaatimuksia ja viranomaisten ohjeita niiden soveltamisesta;

2) kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa tarkoitetun kansallisen turvallisuusviranomaisen antamia kansainvälisten tietoturvallisuusvelvoitteiden toteuttamista koskevia ohjeita;
3) Euroopan unionin, Pohjois-Atlantin liiton tai muun kansainvälisen toimielimen antamia tietoturvallisuutta, kyberturvallisuutta tai varautumista koskevia säännöksiä ja ohjeita;
4) julkaistuja ja yleisesti tai alueellisesti sovellettuja tietototurvallisuutta, kyberturvallisuutta tai varautumista koskevia säännöksiä, määräyksiä tai ohjeita;
5) vahvistettuun standardiin sisältyviä tietoturvallisuutta, kyberturvallisuutta tai varautumista koskevia vaatimuksia.

Arviointiperusteiden ja arvioinnin kohteen määrittämisessä tulee ottaa huomioon tietojärjestelmän ja tietoliikennejärjestelyn tietoturvallisuudelle ja varautumiselle säädetyt ja riskiarvioinnin perusteella valitut vaatimukset. Arviointiviranomainen päättää sen toteuttamien arviointien arviointiperusteista arvioinnin pyytäjää kuultuaan.

Arviointiviranomainen asettaa turvallisuuskriittisen ratkaisun valmistajaa kuultuaan turvallisuuskriittisten ratkaisujen arviointiperusteet. Sen lisäksi mitä 1 ja 2 momentissa säädetään, arviointiperusteiden määrittelyssä tulee ottaa huomioon turvallisuusluokka, valmistuksen turvallisuus sekä valmiudet kansainvälisten tietoturvallisuusvelvoitteiden täyttämiseen.

7 a §

Turvallisuuskriittisen ratkaisun valmistajan arviointiin liittyvät selvitykset

Liikenne- ja viestintäviraston tulee 4 §:n 2 momentin 1 kohdassa tarkoitetun turvallisuuskriittisen ratkaisun arvioinnissa hakea yritysturvallisuusselvitystä. Turvallisuuskriittisen ratkaisun hyväksyntä edellyttää, että valmistajan yritysturvallisuusselvityksessä ei ole ilmennyt mitään, mikä kokonaisharkinnan perusteella vaarantaisi valmistuksen turvallisuuden ja luotettavuuden ottaen huomioon ulkomaisen vaikutuksen riskit.

Jos turvallisuuskriittisen ratkaisun valmistuksen arviointiperusteiden osana käytetään vahvistettua kansainvälistä standardia, standardinmukaisuus voidaan osoittaa vaatimustenmukaisuuden arviointipalvelujen pätevyyden toteamisesta annetussa laissa (920/2005) säädetyn menettelyn avulla.

8 §

Arviointiraportin, hyväksyntäpäätöksen ja -lausunnon antaminen

Tietojärjestelmän ja tietoliikennejärjestelyn tietoturvallisuuden ja varautumisen arvioinnista on laadittava arviointiraportti, johon merkitään tiedot arvioinnin kohteesta, käytetyistä arviointiperusteista, arvioinnin laajuudesta ja havainnoista.

Sen lisäksi, mitä 1 momentissa säädetään, arviointiviranomainen antaa 3 §:n 7 momentin mukaisesta pyynnöstä hyväksyntäpäätöksen tai -lausunnon vaatimukset täyttävästä tietojärjestelmästä tai tietoliikennejärjestelystä. Päätökseen tai lausuntoon on merkittävä tiedot arviointiperusteista, arvioinnin laajuudesta, arvioinnin tuloksista ja jäännösriskistä sekä tarvittaessa voimassaoloajasta.

Sen lisäksi, mitä 1 momentissa säädetään, Liikenne- ja viestintäviraston on annettava 4 §:n 2 momentin 1 kohdassa tarkoitettuun hakemukseen turvallisuuskriittisen ratkaisun ja valmistuksen arvioinnista päätös, josta ilmenee arvioinnin tulos ja voimassaolo. Hyväksyntäpäätökseen voidaan sisällyttää sellaisia rajoituksia ja ehtoja, jotka ovat tarpeen ratkaisun turvallisessa käytössä. Hajasäteilysuojausratkaisuja valmistavan turvallisuuskriittisen ratkaisun valmistajaa koskevaan hyväksyntäpäätökseen voidaan sisällyttää ehtoja, jotka ovat tarpeen valmistuksen luotettavuuden ylläpidossa.

8 c §

Hyväksyttyjen turvallisuuskriittisten ratkaisujen ja valmistajien luettelo

Liikenne- ja viestintävirasto ylläpitää julkista luetteloa 8 §:n 3 momentin mukaisesti hyväksynnän saaneista turvallisuuskriittisistä ratkaisuista ja turvallisuuskriittisten ratkaisujen valmistajista. Luettelosta tulee käydä ilmi soveltuvin osin tiedot ratkaisun nimestä ja tarvittaessa versiosta, turvallisuusluokasta, valmistajasta, hyväksynnän voimassaolosta, muutoksesta tai lakkaamisesta sekä turvallisen käytön ehtojen asettamisesta.

9 §

Tietoturvallisuuden ylläpito ja seuranta

Sen, jolle on annettu 8 §:ssä tarkoitettu päätös tai lausunto, on ylläpidettävä tietoturvallisuus lausunnon tai päätöksen mukaisena. Päätöksen tai lausunnon saaneen on ilmoitettava arviointiviranomaiselle sellaisista muutoksista, joilla voi olla vaikutusta päätöksen tai lausunnon mukaisiin vaatimuksiin.

10 §

Hyväksyntäpäätöksen tai -lausunnon peruuttaminen

Arviointiviranomainen voi peruuttaa 8 §:ssä tarkoitetun lausunnon tai päätöksen kokonaan tai osittain, jos arvioinnin kohteena ollut tietojärjestelmä, tietoliikennejärjestely tai turvallisuuskriittinen ratkaisu taikka turvallisuuskriittisen ratkaisun valmistaja ei enää täytä niitä vaatimuksia, jotka ovat olleet edellytyksenä päätöksen tai lausunnon antamiselle.

Arviointiviranomaisen on ennen 1 momentissa tarkoitetun ratkaisun tekemistä kuultava päätöksen tai lausunnon saanutta sekä varattava tälle tilaisuus korjata puute.

Arviointiviranomainen voi 1 momentissa tarkoitetussa päätöksessään määrätä, että päätöstä on noudatettava muutoksenhausta huolimatta, jollei muutoksenhakuviranomainen toisin määrää.

11 §

Muutoksenhaku

Muutoksenhausta arviointiviranomaisen tämän lain nojalla tekemään päätökseen säädetään oikeudenkäynnistä hallintoasioissa annetussa laissa (808/2019).

12 §

Maksut

Arviointiviranomaisen arvioinnista, arviointiraportin, lausunnon tai päätöksen antamisesta, neuvonnasta ja selvityksestä peritään asian vireille saattajalta maksu noudattaen, mitä valtion maksuperustelaissa (150/1992) säädetään.

Tämä laki tulee voimaan x päivänä -kuuta 2026.

Viranomaisen on saatettava tietojärjestelmiensä ja tietoliikennejärjestelyjensä tietoturvallisuuden ja varautumisen arviointi vastaamaan 3§:ssä säädettyä viiden vuoden kuluessa tämän lain voimaatulosta.

Viranomaisen on kuitenkin pyydettävä arviointi tietojärjestelmälleen tai tietoliikennejärjestelylleen, jossa käsitellään turvallisuusluokkaan I tai II luokiteltuja tietoja 3 §:n 3 momentin mukaisesti kahden vuoden kuluessa lain voimaantulosta, ja pyydettävä tai hankittava arviointi tietojärjestelmälleen tai tietoliikennejärjestelylleen, jossa käsitellään turvallisuusluokkaan III luokiteltuja tietoja 3 §:n 4 momentin mukaisesti kolmen vuoden kuluessa lain voimaantulosta.

2.

Laki

tietoturvallisuuden arviointilaitoksista annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan tietoturvallisuuden arviointilaitoksista annetun lain (1405/2011) 1 luku, 3 §:n 1 momentti, 4 §, 5 §:n 1 ja 3–5 momentti, 6–8 §, 3 luvun otsikko, 9–13 § ja 13 a §, sellaisena kuin niistä on 4 § osaksi laissa 727/2014 ja 13 a § laissa 727/2014, sekä

lisätään 3 lukuun uusi 9 a §:

1 Luku

Yleiset säännökset

1 §

Lain tarkoitus

Tässä laissa säädetään menettelystä, jonka avulla viranomaiset voivat hankkia riippumattoman tietoturvallisuuden tai varautumisen arvioinnin ja yritykset voivat osoittaa luotettavasti ulkopuolisille, että niiden toiminnassa on toteutettu määrätty tietoturvallisuuden taso.

2 §

Lain soveltamisala

Tätä lakia sovelletaan Suomeen sijoittautuneisiin elinkeinonharjoittajiin ja palvelutehtäviä julkishallinnolle tarjoaviin yksiköihin, jotka toimeksiannosta arvioivat tietoturvallisuustason taikka tietojärjestelmän tai tietoliikennejärjestelyn varautumisen tasoa (*tietoturvallisuuden arviointilaitos*) ja jotka haluavat toiminnalleen Liikenne- ja viestintäviraston hyväksynnän. Lisäksi tätä lakia sovelletaan hyväksymismenettelyyn.

Arviointiviranomaisten tehtävistä viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden ja varautumisen arvioinnissa sekä yritysturvallisuusselvitysten laadinnassa säädetään erikseen.

2 Luku

Arviointilaitoksen hyväksyminen ja valvonta

3 §

Arviointilaitoksen hyväksymistä koskeva hakemus

Tietoturvallisuuden arviointilaitos voi hakea Liikenne- ja viestintäviraston hyväksyntää toimintaansa ja arvioinnin pätevyysaluetta varten.

— —

4 §

Hakemuksen käsittely

Liikenne- ja viestintäviraston on ennen tietoturvallisuuden arviointilaitoksen hyväksymistä varattava suojelupoliisille tilaisuus lausua arviointilaitoksen vastuuhenkilöiden luotettavuudesta ja sen toimitilojen turvallisuudesta. Jos hakemus koskee turvallisuusluokitellun tiedon käsittelyn arvioinnin pätevyysaluetta, Liikenne- ja viestintäviraston tulee yrityksen ja sen vastuuhenkilöiden luotettavuuden ja sitoumustenhoitokyvyn varmistamiseksi hakea yrityksestä yritysturvallisuusselvitys. Suojelupoliisi noudattaa lausuntoa tai selvitystä laatiessaan, mitä turvallisuusselvityslaissa (726/2014) säädetään. (19.9.2014/727)

Liikenne- ja viestintävirasto voi hakemusta käsiteltäessä hankkia lausuntoja viranomaisilta sekä antaa hakemuksen ja siinä esitettyjen tietojen arvioimiseksi avustavia tehtäviä ulkopuolisille asiantuntijoille. Ulkopuoliseen asiantuntijaan sovelletaan rikosoikeudellista virkavastuuta koskevia säännöksiä hänen hoitaessaan tämän pykälän mukaisia tehtäviä. Vahingonkorvausvastuusta säädetään vahingonkorvauslaissa (412/1974).

5 §

Arviointilaitoksen hyväksyminen

Tietoturvallisuuden arviointilaitoksen hyväksymisen edellytyksenä on, että:

— —

4) laitoksen yritysturvallisuusselvityksessä ei ole ilmennyt mitään estettä, mikä kokonaisharkinnan perusteella vaarantaisi yrityksen tai vastuuhenkilöiden luotettavuuden tai sitoumustenhoitokyvyn arviointitehtävässä tai laitoksen vastuuhenkilöiden luotettavuus on varmistettu, ja laitoksella on luotettavaksi arvioitu ja valvottu menetelmä, jonka avulla laitoksen toimitilojen ja tietojenkäsittelyn turvallisuus ja henkilökunnan luotettavuus varmistetaan;

— —

Sen estämättä mitä 2 momentissa säädetään, hyväksytyn arviointilaitoksen hakiessa hyväksyntää uudelle pätevyysalueelle voi Liikenne- ja viestintävirasto päättää vaatimusten täyttymisestä kuultuaan pätevyyden hyväksymisen kannalta keskeisiä viranomaisia.

Liikenne- ja viestintävirasto hyväksyy saamiensa ja laatimiensa selvitysten sekä suorittamiensa tarkastusten perusteella vaatimukset täyttävän laitoksen hyväksytyksi tietoturvallisuuden arviointilaitokseksi. Tällainen laitos voi markkinoinnissaan ja muussa viestinnässään käyttää Liikenne- ja viestintäviraston hyväksymistä koskevaa ilmaisua edellyttäen, ettei

hyväksymisen voimassaoloa koskeva määräaika ole päättynyt tai Liikenne- ja viestintävirasto ole päättänyt peruuttaa hyväksynnän.

Arviointilaitos voidaan hyväksyä määräajaksi, jos siihen on erityinen syy. Hyväksymistä koskevaan päätökseen voidaan sisällyttää arviointilaitoksen pätevyysaluetta, valvontaa sekä sellaisia toimintaa koskevia rajoituksia ja ehtoja, jotka ovat tarpeen arviointilaitoksen tehtävien asianmukaisen hoidon varmistamiseksi.

6 §

Arviointilaitoksen hyväksymisen peruuttaminen

Jos hyväksytty tietoturvallisuuden arviointilaitos toimii olennaisesti tai jatkuvasti säännösten vastaisesti taikka jos se ei enää täytä hyväksymiselle asetettuja vaatimuksia, Liikenne- ja viestintäviraston on kehotettava arviointilaitosta korjaamaan puute määräajassa. Jos puutetta ei korjata määräajassa, Liikenne- ja viestintävirasto voi peruuttaa arviointilaitoksen tai pätevyysalueen hyväksymisen.

Liikenne- ja viestintävirasto voi päätöksessään määrätä, että päätöstä on noudatettava muutoksenhausta huolimatta, jollei muutoksenhakuviranomainen toisin määrää.

7 §

Liikenne- ja viestintäviraston tiedonsaanti ja tarkastusoikeus

Liikenne- ja viestintävirastolla ja sitä avustavalla asiantuntijalla on oikeus tarkastaa hyväksyntää hakeneen tai hyväksytyn tietoturvallisuuden arviointilaitoksen tilat sekä sen käytössä olevat menetelmät. Tarkastusta ei saa suorittaa pysyväisluonteiseen asumiseen käytetyissä tiloissa.

Liikenne- ja viestintävirastolla on sen estämättä, mitä tietojen salassapidosta säädetään, oikeus saada pyynnöstä suojelupoliisilta, kansalliselta akkreditointiyksiköltä tai pätevyysalueen arviointiperustetta ohjaavalta tai valvovalta viranomaiselta, arviointilaitokselta tai sen asiakkaalta ne tiedot, jotka ovat välttämättömiä sen valvomiseksi, että laitos täyttää toimintaansa koskevat vaatimukset.

8 §

Arviointilaitoksen ilmoitusvelvollisuus

Hyväksytyn tietoturvallisuuden arviointilaitoksen on ilmoitettava Liikenne- ja viestintävirastolle sellaisesta toimintaansa koskevasta muutoksesta, jolla on merkitystä laitosta koskevien velvoitteiden kannalta.

3 Luku

Tietoturvallisuuden ja varautumisen arviointi

9 §

Arviointilaitoksen tehtävät

Hyväksytyn tietoturvallisuuden arviointilaitoksen on saamaansa tietoturvallisuuden ja varautumisen arviointitehtävää suorittaessaan noudatettava huolellisuutta ja pidettävä huolta siitä, että arvioinnin aikana:

1) tarkastetaan tarvittaessa arvioinnin kohteen toimitilat;

2) selvitetään, onko arvioinnin kohteen toiminnassa asianmukaisella tavalla toteutettu 10 §:ssä tarkoitetut tietoturvallisuutta tai varautumista koskevat vaatimukset, jotka on otettu selvityksen perustaksi (tietoturvallisuuden ja varautumisen arviointiperusteet).

Arviointi voidaan tehdä myös osittaisena.

Hyväksytyn tietoturvallisuuden arviointilaitoksen on laadittava arviointiraportti, johon merkitään tiedot käytetyistä arviointiperusteista, arvioinnin laajuudesta ja havainnoista.

Hyväksytty tietoturvallisuuden arviointilaitos voi pyynnöstä, tai jos niin erikseen säädetään antaa selvitysten ja tarkastuksen perusteella todistuksen, jos arvioitava kohde on selvityksen perustana olleiden arviointiperusteiden mukainen. Todistuksessa tulee yksilöidä arvioinnissa käytetyt tietoturvallisuuden ja varautumisen arviointiperusteet ja arvioinnin laajuus sekä voimassaoloaika.

9 a §

Alihankinta

Hyväksytty tietoturvallisuuden arviointilaitos voi teettää arviointiin liittyvän tehtävän toisella konserniin kuuluvalla yhtiöllä tai muuna alihankintana vain, jos konserniyhtiö tai muu alihankkija täyttää tietoturvallisuuden arviointilaitoksen hyväksymisen edellytykset soveltuvin osin ja alihankinnasta on annettu selvitys Liikenne- ja viestintävirastolle ja Liikenne- ja viestintävirasto on todennut edellytysten täyttymisen.

Hyväksytty tietoturvallisuuden arviointilaitos voi teettää alihankintana tai tytäryhtiöllä turvallisuusluokitellun tiedon käsittelyn arviointiin liittyviä tehtäviä ainoastaan, jos siitä on sovittu asiakkaan kanssa.

10 §

Tietoturvallisuuden ja varautumisen arviointiperusteet

Tietoturvallisuuden ja varautumisen arviointiperusteina voidaan tässä laissa tarkoitetussa arvioinnissa käyttää arvioinnin kohteen valinnan ja arviointilaitoksen hyväksytyn pätevyysalueen mukaan:

1) lailla tai asetuksella säädettyjä viranomaisten toimintaa koskevia tietoturvallisuus-, kyberturvallisuus- ja varautumisvaatimuksia ja viranomaisten ohjeita niiden soveltamisesta;

2) Euroopan unionin, Pohjois-Atlantin liiton tai muun kansainvälisen toimielimen antamia tietoturvallisuutta, kyberturvallisuutta tai varautumista koskevia säännöksiä ja ohjeita;
3) julkaistuja ja yleisesti tai alueellisesti sovellettuja tietoturvallisuutta, kyberturvallisuutta tai varautumista koskevia säännöksiä, määräyksiä tai ohjeita;
4) vahvistettuun standardiin sisältyviä tietoturvallisuutta, kyberturvallisuutta tai varautumista koskevia vaatimuksia.

4 Luku

Erinäiset säännökset

11 §

Maksut

Tietoturvallisuuden arviointilaitoksen hyväksymistä ja valvontaa koskevan asian käsittelystä Liikenne- ja viestintävirastossa peritään maksu noudattaen, mitä valtion maksuperustelaissa (150/1992) säädetään.

12 §

Muutoksenhaku

Muutoksenhausta Liikenne- ja viestintäviraston tämän lain nojalla tekemään päätökseen säädetään oikeudenkäynnistä hallintoasioissa annetussa laissa (808/2019).

13 §

Virkavastuuta ja hyvää hallintoa koskevien säännösten soveltaminen

Hyväksytyn tietoturvallisuuden arviointilaitoksen on tässä laissa tarkoitettuja tehtäviä hoitaessaan noudatettava hallintolakia (434/2003), viranomaisten toiminnan julkisuudesta annettua lakia (621/1999), kielilakia (423/2003), saamen kielilakia (1086/2003), tietosuojalakia (1050/2018) sekä sähköisestä asioinnista viranomaistoiminnassa annettua lakia (13/2003).

Arviointilaitosten vastuuhenkilöihin ja henkilökuntaan sovelletaan rikosoikeudellista virkavastuuta koskevia säännöksiä heidän suorittaessaan tässä laissa tarkoitettuja tehtäviä. Vahingonkorvausvastuusta säädetään vahingonkorvauslaissa (412/1974).

13 a §

Turvallisuusselvitysrekisteriin merkittävät tiedot

Liikenne- ja viestintävirasto merkitsee turvallisuusselvityslaissa tarkoitettuun turvallisuusselvitysrekisteriin tiedot hyväksytyistä arviointilaitoksista samoin kuin arviointilaitokselle annettuun todistukseen merkityt tiedot. Hyväksynnän peruuttamisesta on tehtävä välittömästi merkintä rekisteriin.

Hyväksytty arviointilaitos voi ilmoittaa Liikenne- ja viestintävirastolle turvallisuusselvitysrekisteriin merkitsemistä ja siitä edelleen luovuttamista varten tiedot arvioimastaan kohteesta ja sille annetun todistuksen sisällöstä, jollei arvioinnin kohde ole sitä kieltänyt. Arvioinnin kohteelle on ennen ilmoituksen tekemistä annettava tieto tietojenkäsittelyn tarkoituksesta ja sitä koskevasta sääntelystä.

_____

Tämä laki tulee voimaan x päivänä -kuuta 2026.

_____

3.

Laki

turvallisuusselvityslain 18 ja 48 § muuttamisesta

Eduskunnan päätöksen mukaisesti

kumotaan turvallisuusselvityslain (726/2014) 48 § 4 momentin 1 kohta sellaisena kuin se on laissa 347/2020

muutetaan 18 § 2 momentti seuraavasti:

18 §

Turvallisuusvaatimusten toteuttaminen yleisenä edellytyksenä

— —

Edellä 1 momentissa tarkoitettu vaatimuksen täyttyminen voidaan osoittaa tietoturvallisuuden arviointilaitoksista annetussa laissa (1405/2011) tarkoitetun hyväksytyn arviointilaitoksen antamalla todistuksella, viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annetun lain (1406/2011) mukaisesti annetulla päätöksellä tai lausunnolla, turvallisuussuunnitelmalla tai muulla turvallisuusselvityksen tekemisestä päättävän toimivaltaisen viranomaisen hyväksymällä tavalla.

— —

_____

Tämä laki tulee voimaan päivänä kuuta 20 .

_____

Helsingissä x.x.20xx

Pääministeri

Etunimi Sukunimi

..ministeri Etunimi Sukunimi

Liite

Työryhmän ja sihteeristön jäsenet

Tietojärjestelmien vaatimustenmukaisuuden arvioinnin ajantasaistamisen ja tehostamisen työryhmän jäsenet 1.1.25-23.9.25:

- tietohallintoneuvos Tuija Kuusisto, valtiovarainministeriö, puheenjohtaja
- neuvotteleva virkamies Mika Kuronen, valtiovarainministeriö, varapuheenjohtaja
- neuvotteleva virkamies Marika Kalliotie, valtiovarainministeriö
- neuvotteleva virkamies Niko Mäkilä, valtiovarainministeriö
- johtava asiantuntija Jan Seuri, valtioneuvoston kanslia, varajäsen toimialajohtaja Max Hamberg
- tietoturvatarkastaja Mika Pullinen, ulkoministeriö
- lakimies Ville Salmi, ulkoministeriö, Kansallinen turvallisuusviranomainen
- johtava asiantuntija Kimmo Janhunen, oikeusministeriö
- turvallisuuspäällikkö Kari Santalahti, sisäministeriö, varajäsen johtava asiantuntija Ismo Parviainen
- neuvotteleva virkamies Jukka-Pekka Virtanen, puolustusministeriö
- johtava tietohallintoasiantuntija Mika Tuikkanen, maa- ja metsätalousministeriö, varajäsen erityisasiantuntija Hanna Majurinen, 2. varajäsen erityisasiantuntija Ari Mannonen
- valtion kyberturvallisuusjohtaja Rauli Paananen, liikenne- ja viestintäministeriö, Valtion kyberturvallisuusjohtajan toimisto, varajäsen erityisasiantuntija Jukka Seppälä
- hallitusneuvos Mari Starck, yksikön johtaja Lars Dolk 27.3.25 saakka ja 27.2.-31.7.25 ylitarkastaja Nea Nordman, liikenne- ja viestintäministeriö
- erityisasiantuntija Teemupekka Virtanen, sosiaali- ja terveysministeriö
- johtava asiantuntija Tanja Karvonen, työ- ja elinkeinoministeriö, varajäsen erityisasiantuntija Kimmo Kuusela
- IT-erityisasiantuntija Lauri Karppinen, Tietosuojavaltuutetun toimisto
- johtava asiantuntija Jyrki Siivola, Valtion tieto- ja viestintätekniikkakeskus Valtori, varajäsen yksikönpäällikkö Sonja Marjamäki-Ruuskanen ja ryhmäpäällikkö Mika Raappana
- riskienhallintapäällikkö Pekka Ristimäki ja 27.2.25 alkaen erityisasiantuntija Hanna Heikkinen, Digi- ja väestötietovirasto
- osastopäällikkö Johanna Erkkilä ja johtava asiantuntija Anne Lohtander, Liikenne- ja viestintävirasto
- osastoinsinööri Tuomas Munnukka, Puolustusvoimat, varajäsen everstiluutnantti Kimmo Tarvainen
- erityisasiantuntija Hanna Menna, Hyvinvointialueyhtiö Hyvil Oy, varajäsen erityisasiantuntija Marjo Orava
- erityisasiantuntija Martti Setälä, Kuntaliitto
- 31.3.25 saakka hankeassistentti Katariina Rantala, valtiovarainministeriö

- 01.4.25-06.7.25 hankeassistentti Jonna Sailaranta, valtiovarainministeriö
- 11.8.25 alkaen assistenttiharjoittelija Faini El Agoz, valtiovarainministeriö

Tietojärjestelmien vaatimustenmukaisuuden arvioinnin ajantasaistamisen ja tehostamisen työryhmän sihteeristön jäsenet 1.1.25-23.9.25:

- tietohallintoneuvos Tuija Kuusisto, valtiovarainministeriö, puheenjohtaja
- neuvotteleva virkamies Mika Kuronen, valtiovarainministeriö, varapuheenjohtaja
- neuvotteleva virkamies Niko Mäkilä, valtiovarainministeriö
- neuvotteleva virkamies Marika Kalliotie, valtiovarainministeriö
- hallitusneuvos Mari Starck, yksikön johtaja Lars Dolk 27.3.25 saakka ja 27.2.25-31.7.25 ylitarkastaja Nea Nordman, liikenne- ja viestintäministeriö
- hallitussihteeri Tuomas Hyvärinen, puolustusministeriö
- erityisasiantuntija Anna-Minna Lukkala, sisäministeriö
- lakimies Jussi Rissanen ja johtava asiantuntija Anne Lohtander, Liikenne- ja viestintävirasto
- tekninen tietoturvajohtaja Pasi Koljonen ja 27.3.25 alkaen sotilaslakimies Katriina Härmä, Puolustusvoimat
- johtava asiantuntija Jyrki Siivola, Valtion tieto- ja viestintätekniikkakeskus Valtori, 1.1.25-27.2.25, varajäsen yksikönpäällikkö Sonja Marjamäki-Ruuskanen, 1.1.25-27.2.25
- erityisasiantuntija Hanna Heikkinen, Digi- ja väestötietovirasto, 1.1.25-27.2.25