HE 85/2026 vp

Hallituksen esitys eduskunnalle laeiksi viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annetun lain, tietoturvallisuuden arviointilaitoksista annetun lain sekä turvallisuusselvityslain 18 ja 48 §:n muuttamisesta

ESITYKSEN PÄÄASIALLINEN SISÄLTÖ

Esityksessä ehdotetaan muutettaviksi viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annettua lakia sekä tietoturvallisuuden arviointilaitoksista annettua lakia. Lisäksi ehdotetaan muutettavaksi turvallisuusselvityslakia, jota koskevat muutosehdotukset ovat teknisiä.

Viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annettuun lakiin ehdotetuilla muutoksilla selkeytettäisiin viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen arviointimenettelyjä sekä parannettaisiin niiden saatavuutta mahdollistamalla nykyistä useammanlaisia arviointimenettelyjä. Myös muille luotettaviksi todetuille yrityksille kuin tietoturvallisuuden arviointilaitoksille säädettäisiin mahdollisuus tarjota tietoturvallisuuden ja varautumisen arviointipalveluja viranomaisille korkeintaan turvallisuusluokan IV tietojen käsittelyn arviointiin saakka. Lakiin lisättäisiin valtionhallinnon viranomaisille velvollisuus arvioida tietojärjestelmänsä ja tietoliikennejärjestelynsä vähintään itsearviointeina. Muidenkin kuin valtionhallinnon viranomaisten olisi mahdollista toteuttaa lain mukaisia arviointeja. Kaikkien viranomaisten tulisi kuitenkin pyytää arviointiviranomaisen arviointia turvallisuusluokan I ja II tietojen käsittelylle. Lisäksi kaikkien viranomaisten tulisi pyytää arviointiviranomaisen arviointia tai hankkia tietoturvallisuuden arviointilaitoksen arviointi turvallisuusluokan III tietojen käsittelylle, jollei viranomainen riskiarvioinnin perusteella päättäisi 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.

Viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annettuun lakiin ehdotetuilla muutoksilla myös 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. Ehdotetuilla muutoksilla tarkennettaisiin ja tehostettaisiin arviointiviranomaisten yhteistyötä, työjakoa ja tiedonsaantioikeuksia sekä mahdollistettaisiin arviointiviranomaista avustava tehtävä.

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

SISÄLLYS

ESITYKSEN PÄÄASIALLINEN SISÄLTÖ 1
PERUSTELUT 4
1 Asian tausta ja valmistelu 4
1.1 Tausta 4
1.2 Valmistelu 4
2 Nykytila ja sen arviointi 5
2.1 Viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arviointi 5
2.2 Salaustuotteiden ja muiden turvallisuuskriittisten ratkaisujen arviointi 12
2.3 Tietoturvallisuuden arviointilaitokset 13
2.4 Euroopan unionin oikeus 15
3 Tavoitteet 17
4 Ehdotukset ja niiden vaikutukset 18
4.1 Keskeiset ehdotukset 18
4.2 Pääasialliset vaikutukset 19
4.2.1 Taloudelliset vaikutukset 19
4.2.1.1 Yritykset 19
4.2.2 Muut ihmisiin kohdistuvat ja yhteiskunnalliset vaikutukset 21
4.2.2.1 Viranomaiset 21
4.2.2.2 Kansallinen turvallisuus 26
4.2.2.3 Tietoyhteiskunta 27
4.2.2.4 Tietosuoja 27
5 Muut toteuttamisvaihtoehdot 28
5.1 Vaihtoehdot ja niiden vaikutukset 28
5.2 Ulkomaiden lainsäädäntö ja muut ulkomailla käytetyt keinot 30
6 Lausuntopalaute 32
6.1 Lausuntokierros 32
6.2 Yleisvaikutelma lausunnoista 32
6.3 Lausunnoista tarkemmin ja pääasialliset muutokset jatkovalmistelussa 33
7 Säännöskohtaiset perustelut 34
7.1 Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista 34
7.2 Laki tietoturvallisuuden arviointilaitoksista 55
7.3 Turvallisuusselvityslaki 62
8 Lakia alemman asteinen sääntely 62
9 Voimaantulo 63
10 Suhde perustuslakiin ja säätämisjärjestys 64
LAKIEHDOTUKSET 71
Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annetun lain muuttamisesta 71
Laki tietoturvallisuuden arviointilaitoksista annetun lain muuttamisesta 79
Laki turvallisuusselvityslain 18 ja 48 § muuttamisesta 84
LIITE 85
RINNAKKAISTEKSTIT 85

Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annetun lain muuttamisesta....85
Laki tietoturvallisuuden arviointilaitoksista annetun lain muuttamisesta 99
Laki turvallisuusselvityslain 18 ja 48 § muuttamisesta 107

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, viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annettu laki (1046/2011) jäljempänä *arviointilaki*, sekä tietoturvallisuuden arviointilaitoksista annettu laki (1045/2011) jäljempänä *arviointilaitoslaki,* on valmisteltu yli 14 vuotta sitten.

Digitalisaation edistyminen ja kehittyvät teknologiat kuten pilvipalvelut, tekoäly ja kvanttilaskenta ovat vaikuttaneet sekä julkisen hallinnon toimintatapoihin että 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 tullut voimaan arviontilain ja arviointilaitoslain voimaantulon jälkeen. Lisäksi tietoturvallisuuden vaatimuksenmukaisuuden arviointia koskeva EU-sääntely on lisääntynyt viime vuosina. Näiden muutosten sekä aikaisemmin tehtyjen selvitysten perusteella on tunnistettu tarve julkisen hallinnon tietoturvallisuuden ja varautumisen arviointia koskevan sääntelyn ajantasaistamiselle ja tehostamiselle.

Suomen 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 (Puolustusministeriön julkaisuja 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, joka valmistui 12.12.2024. Ensimmäisen vaiheen raportista järjestettiin sidosryhmätilaisuus julkiselle hallinnolle ja elinkeinoelämälle 21.11.2024.

Yhteiskunnan uudistamisen ministerityöryhmä käsitteli 7.3.2025 työryhmän ensimmäisen vaiheen raportissa esitettyjä säädösvalmistelukohteita. Tähän perustuen työryhmä valmisteli lainsäädännön muutosehdotukset hallituksen esityksen muotoon. Työryhmän laatima luonnos hallituksen esitykseksi valmistui 23.9.2025. Esitysluonnokseen sisältyviä lainsäädännön muutosehdotuksia käsiteltiin työryhmän julkiselle hallinnolle 9.9.2025 ja yritysten edustajille 11.9.2025 järjestämissä sidosryhmätilaisuuksissa. Sidosryhmätilaisuuksiin osallistui noin 220 julkisen hallinnon ja 30 yritysten edustajaa.

Työryhmän valmisteleman hallituksen esityksen luonnoksen pohjalta valtiovarainministeriössä valmisteltiin virkatyönä osin muokattu hallituksen esityksen luonnos, joka kuitenkin asiasisällöltään noudatti työryhmän tekemiä ehdotuksia. Tämä hallituksen esityksen luonnos oli lausuntokierroksella 27.11.2025 – 23.1.2026. Lausuntoa pyydettiin ministeriöiltä, valtion viranomaisilta, hyvinvointialueilta, kunnilta, tuomioistuimilta, korkeakouluilta, kansalliselta akkreditointielimeltä, tietoturvallisuuden arviointilaitoksilta sekä turvallisuuskriittisiä ratkaisuja valmistavilta toimijoilta.

Esityksen jatkovalmistelu lausuntokierroksen jälkeen on tehty valtiovarainministeriössä. Jatkovalmistelun aikana on tehty yhteistyötä puolustusministeriön, liikenne- ja viestintäministeriön, Puolustusvoimien ja Liikenne- ja viestintäviraston kanssa.

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

2 Nykytila ja sen arviointi

2.1 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.

Tietoturvallisuuden ohella varautumisen merkitys on kasvanut turvallisuusympäristön muutosten vuoksi. Varautuminen on myös lisätty tiedonhallintalain 13 a §:ään, jonka mukaan tiedonhallintayksikön on selvitettävä sen tietoaineistojen käsittelyn, tietojärjestelmien hyödyntämisen sekä niihin perustuvan toiminnan jatkuvuuteen kohdistuvat olennaiset riskit ja varauduttava normaaliolojen ja poikkeusolojen häiriötilanteisiin. Varautumisen arvioinnista ei kuitenkaan säädetä arviointilaissa, eikä sen arviointi ole vakiintunut osa arviointitoimintaa. Varautuminen on kuitenkin tunnistettu osa-alueeksi, jonka arviointia tulisi kehittää ja varautumisen arviointien määrää lisätä.

Viranomaisille ei ole voimassa olevassa lainsäädännössä säädetty yleistä tietojärjestelmien ja tietoliikennejärjestelyjen arviointivelvollisuutta. Tiedonhallintalain 13 §:n perusteella vastuu tietoaineistojen ja tietojärjestelmien tietoturvallisuuden varmistamisesta kuuluu tiedonhallintayksikölle, eli viranomaiselle itselleen. 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. Säännöksen tarkoituksena on muodostaa sidos arviointilakiin ja arviointilaitoslakiin, jotta tietojärjestelmien tietoturvallisuuden suunnittelu ja sen arviointia koskeva sääntely muodostaisi selkeän kokonaisuuden (HE 284/2018 vp, s. 93).

Arviointivelvollisuuksia sisältyy 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 julkisen hallinnon turvallisuusverkkotoiminnasta annetussa valtioneuvoston asetuksessa (1109/2015), jäljempänä *turvallisuusverkkoasetus*. Valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä annetun lain (1226/2013), jäljempänä *Tori-laki*, mukaan valtion yhteisten tieto- ja viestintäteknisten palvelujen 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 arviointivelvollisuuksia 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 arviointivelvollisuuksia sisältävät turvallisuussäännöt kansainvälisistä tietoturvallisuusvelvoitteista annetun lain säätämisen yhteydessä sekä Pohjois-Atlantin sopimuksen osapuolten välillä tehdyn sopimuksen voimaansaattamisen yhteydessä (SopS 55–56/2023).

Muuttuneessa turvallisuustilanteessa voisi kuitenkin olla perusteltua, että sektorikohtaisten ja kansainvälisiin tietoturvallisuusvelvoitteisiin liittyvien arviointivelvollisuuksien lisäksi valtionhallinnon viranomaiset toteuttaisivat arviointeja kaikille tietojärjestelmilleen ja tietoliikennejärjestelyilleen. Tällöin olisi tarkasteltava myös arviointimenettelyjä eli sitä, mitkä tahot tekevät arviointeja sekä 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 valtiohallinnon 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.

Käytännössä viranomaiset arvioivat tietojärjestelmiensä ja tietoliikennejärjestelyjensä tietoturvallisuutta myös muilla kuin arviointilain mukaisilla menettelyillä. Tietoturvallisuuden arviointiin liittyvät esimerkiksi tiedonhallintalain 4 a luvussa säädetyt tiedonhallintayksiköiden kyberturvallisuuden hallintavelvollisuudet. Tiedonhallintalain 18 b §:n mukaan tiedonhallintayksikön on tunnistettava, arvioitava ja hallittava kyberriskejä, joita kohdistuu sen toiminnoissa tai palveluntarjonnassa käytettävien viestintäverkkojen ja tietojärjestelmien turvallisuuteen sekä toteutettava tiettyjä mainitun lain 18 c §:ssä säädettyjä kyberturvallisuutta koskevia riskienhallintatoimenpiteitä. Tiedonhallintalain 18 c §:n 1 kohdan mukaan tiedonhallintayksikön on ylläpidettävä kyberturvallisuutta koskevan riskienhallinnan toimintaperiaatteita ja kyberturvallisuuden riskienhallintatoimenpiteiden vaikuttavuuden arviointia. Lain esitöiden mukaan (HE 57/2024 vp, s. 163) arvioinnin voisi tehdä esimerkiksi itsearviointina tai riippumattomia tietoturvapalveluntarjoajia hyödyntäen. Tietoturvallisuuden arviointiin liittyviä toimia toteutetaan myös tiedonhallintalain 9 §:n mukaisessa valtion virastoja ja laitoksia koskevan tiedonhallinnan muutosten lausuntomenettelyssä, jonka osana arvioidaan myös tietojärjestelmien tietoturvallisuusvaatimusten ja –toimenpiteiden muutoksia. Lausuntomenettelyn valmistelun yhteydessä on mahdollista toteuttaa tietojärjestelmän tietoturvallisuuden itsearviointi.

Edellä mainituista syistä olisi tarkoituksenmukaista päivittää arviointilakia kattamaan useampia arviointimenettelyjä.

Arviointilaissa 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. Arviointilaissa säädetyissä arviointimenettelyissä ei myöskään ole huomioitu eri tietojärjestelmien ja tietoliikennejärjestelyjen tietojenkäsittelyn riskejä ja niiden eroja. Lain 8 a §:ssä on säädetty asetuksenantovaltuus, jolla voitaisiin velvoittaa valtionhallinnon viranomainen hankkimaan todistus tietojärjestelmästä tai tietoliikennejärjestelystä, jossa käsitellään turvallisuusluokkaan I tai II kuuluviksi luokiteltuja asiakirjoja. Asetusta ei kuitenkaan ole annettu, eli 8 a §:n mahdollistama riskiarvioon perustuva arviointivelvollisuus on jäänyt käytännössä toteutumatta. Tiedonhallintalain 13 §:ssä säädettyjen tietoaineistojen ja tietojärjestelmien riskiarviointiin perustuvien velvollisuuksien ja turvallisuusluokitteluun sisäänrakennetun riskinäkökulman takia nykytilassa arviointiperusteet määritellään käytännössä riskiarvioinnin perustella ja arviointikriteeristöissä huomioidaan tietoturvallisuusuhkat, joiden toteutumisen todennäköisyys on suuri, ellei niiltä suojauduta riittävillä tietoturvallisuustoimenpiteillä. Edellä kuvatuista syistä on tunnistettu tarve tarkentaa voimassa olevan lainsäädännön arviointimenettelyjen valintaa turvallisuusluokkiin ja riskiarviointiin perustuvaksi.

Tietoturvallisuuden arviointien määrä ja kustannukset

Viranomaisten tietojärjestelmien tietoturvallisuuden arviointien kysyntä ja määrä on viime vuosina kasvanut. Lisääntynyt arviointitarve on aiheuttanut ruuhkautumista arviointitoiminnassa. 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.

Kansainvälisiin tietoturvallisuusvelvoitteisiin liittyvät arviointitarpeet 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. Tietoturvallisuuden arviointilaitosten toteuttamien arviointien määrästä ei ole saatavilla julkisia tietoja.

Valtion tieto- ja viestintätekniikkakeskus Valtorin ja Suomen Erillisverkot Oy:n hankkimien vaatimustenmukaisuuden arviointien määrät ovat arviointilain voimassaolon aikana kasvaneet. Kasvu johtuu palveluiden kehittämistoimista, uusista palveluista sekä EU- ja Nato -tiedon käsittelytarpeesta. Valtion tieto- ja viestintätekniikkakeskus 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 tietoturvallisuuden arviointilaitoksilta hankkimien lakisääteisten tietoturvallisuuden arviointien määrä on ollut lievässä kasvussa vuodesta 2021 lähtien. Kasvu johtuu arviointivelvollisuuden piiriin kuuluvien tietojärjestelmien määrän kasvusta. Tällä hetkellä näitä Lupa- ja valvontaviraston (31.12.2025 asti Valvira) rekisteriin merkittyjä tietojärjestelmiä ja käyttöympäristöjä on 99. Vuonna 2023 rekisteriin merkittiin 27 todistusta tietoturvallisuuden arvioinneista.

Kuntaliiton arvion mukaan kunnissa ei laajamittaisesti toteuteta tietoturvallisuuden arviointilaitosten tai Liikenne- ja viestintäviraston tietoturvallisuuden arviointeja, mutta kattavaa tilannekuvaa ei ole saatavilla. Suurimmissa kaupungeissa toteutetaan riskiarvioinnin perusteella valikoitujen tietojärjestelmien tietoturvallisuuden itsearviointeja, usein yksityisten palveluntarjoajien tukemana. Pienemmissä kunnissa ja kuntayhtymissä tietojärjestelmien tietoturvallisuuden itsearviointeja toteutetaan tapauskohtaisesti.

Arviointien kysynnän ja määrien kasvamisen vuoksi arviointien saatavuutta tulisi parantaa.

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, Valtion tieto- ja viestintätekniikkakeskus Valtorista ja ministeriöistä[1]. Suomen Erillisverkot Oy:n vuosittain toteuttamien noin 20 itsearvioinnin vaatima

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

henkilötyömäärä on ollut noin 300 henkilötyöpäivä vuodessa 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 ovat olleet noin 57 000 euroa/arviointi. Viranomaisten hakemien tietoturvallisuuden arviointien hinta on keskimäärin ollut yhteensä 60 000–70 000 euroa/arviointi, joista pääsääntöisesti tietoturvallisuuden arviointilaitoksilta hankitun ulkoisen arvioinnin osuus on ollut keskimäärin 30 000–40 000 euroa. Esimerkiksi liikenne- ja viestintäministeriön hallinnonalalla on vuosittain hankittu noin 220–230 henkilötyöpäivän edestä arviointilain ja arviointilaitoslain mukaisia arviointipalveluja. Hallinnonalan palvelujen hankintakustannusten arvioidaan olevan vuositasolla noin 300 000 euroa. Muilta tietoturvapalveluja tarjoavilta yrityksiltä on hankittu vuosittain noin 720–750 henkilötyöpäivän edestä arviointeihin liittyviä palveluja. Kustannusten arvioidaan olevan vuositasolla noin 650 000 euroa. Liikenne- ja viestintäministeriön hallinnon alalla arviointilakien mukaiset arvioinnit ovat siten olleet henkilötyöpäivinä noin 20 % ja euromääräisesti noin 30 % kaikista tietoturvallisuuden arvioinneista.[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 ja arviointilaissa. Arviointilain 3 §:n mukaan Liikenne- ja viestintävirasto on nykytilassa ainoa viranomainen, joka toteuttaa arviointilain mukaisia viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arviointeja. Liikenne- ja viestintäviraston tehtävien osalta on tunnistettu päivitystarve alla käsiteltyjen tehtävien osalta.

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 (1338/2025).

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 tarvittaessa kansallisen turvallisuusluokkaan I ja II luokiteltuja tietoja käsittelevien tietojärjestelmien arviointiin liittyviä pyyntöjä, joihin ei ole saatavilla tietoturvallisuuden arviointilaitoksen arviointeja.

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 tai

salaustuotteita. Kansallisen turvallisuusluokitellun tiedon osalta arviointitoiminta perustuu tiedonhallintalaissa ja turvallisuusluokitteluasetuksessa säädettyihin tiedonhallintayksikön ja valtionhallinnon viranomaisen velvollisuuksiin huolehtia tietoaineistojen ja tietojärjestelmien tietoturvallisuudesta. 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. Edellä kuvatuista syistä on tunnistettu tarve säätää Puolustusvoimille erillinen viranomaistehtävä tehdä sen omien tietojärjestelmien ja tietoliikennejärjestelyjen arviointeja.

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 viranomaiselle kuuluvan tehtävän hoitamisesta. Arviointiviranomaisten toiminnassa on tunnistettu tarve säätää tiedonvaihdosta ja yhteistyövelvoitteista sekä tehtävien sopimisesta myös arviointilaissa.

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 etenkin tehtävien henkilöresurssitarpeen turvaamiseksi.

Arviointiperusteet ja -kriteerit

Arviointilain 7 §:ssä ja arviointilaitoslain 10 §:ssä säädetään arviointiperusteista, joita Liikenne- ja viestintävirasto tai tietoturvallisuuden arviointilaitos voi käyttää viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arviointiperusteina. Arviointiperusteiden luettelo on samansisältöinen molemmissa laeissa ja ne mahdollistavat laajasti eri säädösten, ohjeiden ja standardien käyttämisen arviointiperusteina. Luetteloa tulisi kuitenkin päivittää.

Voimassa olevan lain mukaan 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. Katakria käytetään lisäksi myös monissa kansallisissa tilanteissa, kuten julkisen hallinnon turvallisuusverkkotoiminnasta annetun lain

(10/2015) jäljempänä *Tuve-laki,* mukaisten palveluiden arvioinneissa sekä yritysturvallisuusselvityksiin liittyvissä arvioinneissa. Arviointikriteerien määrittämisessä hyödynnetään myös tiedonhallintalautakunnan suositusta julkisen hallinnon tietoturvallisuuden arviointikriteeristöstä (Julkri). 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. 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 kumoutunut ja ohjeet ovat vanhentuneet. Asetuksen on korvannut tiedonhallintalaki ja sen perusteella annettu valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019), jäljempänä *turvallisuusluokitteluasetus*. Arviointilaitoslain nojalla tehdyissä arvioinneissa 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.

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

Arviointilaissa ei säädetä millä perusteella tai kenen toimesta arvioinnissa käytettävät arviointiperusteet valitaan. Arviointilaitoslain 10 §:n mukaan arvioinnin kohde valitsee arviointiperusteet, mutta tietoturvallisuuden arviointilaitoksen hyväksytyt pätevyydet vaikuttavat siihen, mitä arviointeja tietoturvallisuuden arviointilaitos voi tehdä. Arviointitoiminnassa on tunnistettu, että arviointiperusteiden valinnassa ja arvioinnin kohteen määrittelyssä tulisi ottaa huomioon tietojärjestelmän tietoturvallisuudelle ja varautumiselle säädetyt vaatimukset ja riskiarvioinnin perusteella valitut vaatimukset. Tämä ei kuitenkaan ilmene voimassa olevasta lainsäädännöstä, joten arviointiperusteiden valinnasta tulisi säätää tarkemmin.

Todistus vaatimusten täyttymisestä

Arviointilain 8 §:n 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 säädettyä mahdollisuutta säätää valtioneuvoston asetuksella valtionhallinnon viranomaisille velvollisuus hankkia todistus turvallisuusluokkaan I tai II luokiteltuja asiakirjoja käsittelevien järjestelmien arvioinneista ei ole käytetty, joten Liikenne- ja viestintäviraston arvioinnin tai todistuksen pyytäminen kansallisen turvallisuusluokitellun tiedon käsittelyssä on vapaaehtoista. Arviointilain 8 §:n mukaisesti pyydetyt Liikenne- ja viestintäviraston antamat todistukset ovat koskeneet kansallisia turvallisuusluokiteltuja tietoja käsitteleviä tietojärjestelmiä. Todistuksia on pyydetty ja annettu erittäin harvoin.

Todistuksen luonteinen päätös tai lausunto voidaan kuitenkin antaa tietoturvallisuusvaatimukset täyttävistä järjestelmistä kansainvälisistä tietoturvallisuusvelvoitteista annetun lain tarkoittamissa tilanteissa. EU:n ja Naton tietoturvallisuusvelvoitteiden mukaisista arvioinneista turvallisuussäännöissä edellytetty hyväksyntälausunto on arviointilain menettelyn valossa todistuksen luonteinen. Liikenne- ja viestintävirasto antaa myös todistuksen luonteisia selvityksiä tietoturvallisuusvaatimukset täyttävistä tietojärjestelmistä turvallisuusselvityslain mukaisten yritysturvallisuusselvitysten yhteydessä suojelupoliisin tai Pääesikunnan pyynnöstä. Lopullisen yritysturvallisuusselvityksen antaa kuitenkin turvallisuusselvityslain mukainen toimintavaltainen viranomainen.

Tietoturvallisuuden 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 kuitenkaan säädetä voimassa olevassa arviointilaissa. Arviointilain voimassa oleva sääntely arvioinnista tuotettavan raportoinnin osalta ei siis vastaa arviointitoiminnassa käytössä olevia käytänteitä, minkä vuoksi on todettu tarve päivittää arvioinnin tuloksen raportointia ja dokumentointia myös lain tasolla.

2.2 Salaustuotteiden ja muiden turvallisuuskriittisten ratkaisujen arviointi

EU:n ja Naton turvallisuussäännöt sisältävät salausratkaisujen ja hajasäteilysuojauksen (TEMPEST) arviointia koskevia velvollisuuksia sekä velvollisuuksia arvioida eräitä muita turvallisuuskriittisiä tuotteita. Myös valtioiden kahden- tai monenvälisissä tietoturvallisuussopimuksissa valtioiden välisten sähköisten tiedonsiirtoyhteyksien 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 4 §:n 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. Salaustuotteiden lisäksi turvallisuuskriittisiä tuotteita ovat muutkin tietojärjestelmien turvallisuuden kannalta keskeiset komponentit, kuten yhdyskäytävätuotteet ja tiedon tuhoamiseen käytettävät ylikirjoitustuotteet.

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 turvallisuuskriittisten tai muidenkaan tuotteiden valmistajien pyynnöstä, eivätkä turvallisuuskriittisiä ratkaisuja tarjoavat yritykset tai valmistajat voi itsenäisesti tehdä arviointilain mukaisia arviointipyyntöjä. Voimassa olevassa lainsäädännössä ei siten säädetä 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 turvallisuuskriittisten ratkaisujen arviointeja suomalaisten valmistajien tuotteille ja laatii näistä arvioinneista lausuntoja. Arvioinnit tehdään valmistajan pyynnöstä, mutta taustalla on oltava jonkin viranomaisen tarve tuotteelle. Valmistajien arviointipyyntöjen käsittely edellyttää sopimuksen tekemistä Liikenne- ja viestintäviraston ja valmistajan välillä. Sopimusmalli perustuu Liikenne- ja viestintävirastosta annetun lain (935/2018) 3 §:ssä säädettyyn Kyberturvallisuuskeskuksen sopimusvaltuuteen, jonka perusteella Kyberturvallisuuskeskus voi tehdä sille säädettyihin tehtäviin perustuvia suoritteita sopimusperusteisesti. Sopimusperusteisesti Liikenne- ja viestintävirasto tekee arviointeja vain suomalaisten valmistajien Suomessa valmistamille tuotteille. Arviointien tarkoituksena on varmistua turvallisuuskriittisen ratkaisun luotettavuudesta siinä määrin, että Liikenne- ja viestintävirasto voi julkaista tiedon arvioidusta tuotteesta. Viraston verkkosivuilla ylläpidetyllä listalla on tällä hetkellä kymmenkunta arvioitua salaustuotetta ja viitisen muuta arvioitua tuotetta. Uusia arviointeja tai tuotepäivitysten arviointeja on yleensä samanaikaisesti käynnissä alle kymmenen.

Salaustuotteiden ja muiden turvallisuuskriittisten ratkaisujen arviointiin liittyviä viranomaistehtäviä tulisi tarkentaa ja valmistajille tulisi säätää mahdollisuus hakea arviointia ja hyväksyntää turvallisuuskriittisille ratkaisuille ja niiden valmistukselle.

2.3 Tietoturvallisuuden arviointilaitokset

Arviointilaitoslaissa säädetään 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.

Arviointilaitoslaissa ei säädetä siitä, mitkä tahot voivat hankkia arviointeja tietoturvallisuuden arviointilaitoksilta. Siten ei ole estettä sille, että viranomainen hankkii arvioinnin tietoturvallisuuden arviointilaitokselta ja arviointilain 3 §:n mukaan valtionhallinnon viranomaisen yhtenä arviointimenettelyvaihtoehtona onkin tietoturvallisuuden arviointilaitoksen suorittama arviointi.

Arviointilaitoslain 3 §:n mukaan tietoturvallisuuden arviointilaitos voi hakea Liikenne- ja viestintäviraston hyväksyntää. Hyväksynnän edellytyksistä ja hakemuksen käsittelystä säädetään lain 4 ja 5 §:ssä. 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.

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. Vastaavaa menettelyä voitaisiin hyödyntää, jotta tietoturvallisuuden arviointilaitokset voisivat joustavammin hankkia lisäpätevyyksiä arviointien saatavuuden parantamiseksi.

Pätevyyden akkreditoinnin lisäksi arviointilaitoksen hyväksyntä edellyttää arviointilaitoslain 5 §:n 1 momentin 4 ja 5 kohdan 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 tietoturvallisuuden arviointilaitoksen vastuuhenkilöiden luotettavuudesta ja sen toimitilojen turvallisuudesta. Suojelupoliisi tekee vastuuhenkilöistä henkilöturvallisuusselvityksen Liikenne- ja viestintäviraston hakemuksesta.

Tietoturvallisuuden arviointilaitokseksi pääsy ja laitoksen pätevyyksien hyväksyntä on koettu hankalaksi ja se on voinut kestää kauan. Voimassa olevan arviointilaitoslain menettelyissä yrityksen luotettavuuden varmistamisessa ei hyödynnetä turvallisuusselvityslain yritysturvallisuusselvityksen menettelyjä kuin osittain. Laissa ei myöskään säädetä tietoturvallisuuden arviointilaitoksen henkilökunnan luotettavuudesta. Sääntelyä olisi tarkoituksenmukaista tarkentaa edellä mainittujen seikkojen osalta.

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 ns. Katakri-pätevyys eli pätevyys tehdä turvallisuusluokkaan IV ja III luokitellun tiedon käsittelyn arviointeja kansallisen turvallisuusauditointikriteeristön (Katakri) mukaisesti. Kolmannen arviointilaitoksen Katakri 2020 -pätevyyden akkreditointi ja hyväksyntä on tehty alkuvuonna 2025.Viranomaisten pitkäkestoisten hankintasopimusten takia kolmannen tarjoajan vaikutuksia arviointien tarjontaan ja hintoihin ei vielä ollut mahdollista todeta.

Arviointeja hankkivien viranomaisten näkemyksen ja kokemuksen mukaan tietoturvallisuuden arviointilaitoksilla on ollut niin runsaasti kysyntää arvioinneille, että ne eivät ole pystyneet tarjoamaan arviointipalveluja kysyntää vastaavasti. Valtion tieto- ja viestintätekniikkakeskus 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 tietoturvallisuuden 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 ovat selvityksen perustana olleiden arviointiperusteiden mukaisia. 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, eli hallinnon yleislakien soveltamisesta tietoturvallisuuden arviointilaitosten toiminnassa. Voimassa olevan lain esitöiden mukaan tulkintaongelmien välttämiseksi mainittujen säädösten soveltamista ei olisi sidottu julkisen hallintotehtävän hoitamiseen, vaan säädöksiä sovellettaisiin kaikkiin arviointilaitoslain mukaisten tehtävien hoitamiseen (HE 45/2011 vp s. 10). Käytännössä tulkinta kuitenkin on ollut, että kaikki arviointilaitoslain mukaiset tehtävät ovat julkisia hallintotehtäviä. Pykälässä ei siitä huolimatta säädetä tietoturvallisuuden arviointilaitosten henkilöstön rikosoikeudellisesta virkavastuusta. Tämän osalta on tunnistettu tarve päivittää lakia, sillä perustuslakivaliokunnan käytännön mukaan julkisen hallintotehtävän ulkoistaminen virkamieskoneiston ulkopuolelle edellyttää nimenomaista virkarikosvastuun perustavaa laintasoista säännöstä (esim. PeVL 93/2022 vp, s. 4, PeVL 15/2019 vp, s. 4). Arviointilaitoslaissa ei myöskään säädetä arviointiin liittyvien tehtävien alihankintana teettämisen reunaehdoista, minkä osalta lakia tulisi tarkentaa.

Arviointilaitoslaissa, asiakastietolaissa tai toisiolaissa ei säädetä ohjaus- tai valvontatoimivallan jakautumisesta Liikenne- ja viestintäviraston ja sosiaali- ja terveysalan viranomaisten, Terveyden ja hyvinvoinnin laitoksen (THL), Lupa- ja valvontaviraston (31.12.2025 asti Valvira), Sosiaali- ja terveysalan tietolupaviranomaisen (Findata) ja Kansaneläkelaitoksen (Kela) välillä, kun tietoturvallisuuden 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 tietoturvallisuuden arviointilaitoksilta ne tiedot, jotka ovat tarpeen sen valvomiseksi, että laitos täyttää toimintaansa koskevat vaatimukset. Tiedonsaantioikeus ei koske salassa pidettäviä tietoja eikä muilta viranomaisilta tai tietoturvallisuuden arviointilaitoksen arvioinnin kohteilta pyydettäviä tietoja, jotka olisivat välttämättömiä sen valvomiseksi, että laitos täyttää toimintaansa koskevat vaatimukset. Valvonnan tiedonsaantioikeuksia tulisi tarkentaa.

2.4 Euroopan unionin oikeus

Tieto- ja viestintäjärjestelmien tieto- ja kyberturvallisuuden vaatimustenmukaisuuden arviointia koskeva Euroopan unionin sääntely on viime vuosina lisääntynyt. Euroopan unionin sääntely koskee pääsääntöisesti palveluiden ja tuotteiden sertifiointia niiden tullessa markkinoille. 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.

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) 1 artiklan 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 Cyber Resilience Act: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 asetuksessa (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), säädetään tekoälyjärjestelmistä 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. NIS2-direktiivi mahdollistaa, että keskeisten ja tärkeiden toimijoiden luokat velvoitetaan käyttämään kyberturvallisuusasetuksen mukaisesti sertifioituja tuotteita. Tätä mahdollisuutta ei Suomessa ole säädetty lakiin kansallista liikkumavaraa hyödyntäen. Direktiivin mukaan komissiolla kuitenkin on valta antaa delegoituja säädöksiä keskeisten ja

tärkeiden toimijoiden luokkien velvoitteesta käyttää tiettyjä sertifioituja tuotteita. Siltä osin, jos tällaisia delegoituja säädöksiä annetaan, ei asian osalta ole kansallista liikkumavaraa.

Euroopan unionin sääntely mahdollistaa jäsenvaltioiden kansallisten viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden ja varautumisen arvioinnin sääntelyn, koska Suomessa kansallinen arviointitoiminta kohdistuu viranomaisen määräämisvallassa olevan tai hankittavaksi suunnitteleman tietojärjestelmän tai tietoliikennejärjestelyn tietoturvallisuuden ja varautumisen tapauskohtaiseen arviointiin, eikä 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.

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

Liikenne- ja viestintävirastolle säädettäisiin uusi kotimaisten turvallisuuskriittisten ratkaisujen arviointitehtävä. Turvallisuuskriittisellä ratkaisulla tarkoitettaisiin salaus-, hajasäteilysuojaus- ja muuta tieto- ja viestintäteknistä ratkaisua eli tuotetta, toteutusta tai palvelua, jolla suojataan turvallisuusluokiteltua tietoa tietojärjestelmissä ja tietoliikennejärjestelyissä. Suomalaisille valmistajille säädettäisiin mahdollisuus hakea Liikenne- ja viestintävirastolta arviointia ja hyväksyntää julkiseen luetteloon turvallisuuskriittisille ratkaisuille ja niiden valmistukselle. Lisäksi Liikenne- ja viestintäviraston tehtäviä tarkennettaisiin tietoturvallisuuden arviointiin liittyvässä neuvonnannassa ja tehtävien priorisoinnissa.

Arviointiviranomaiseksi säädettäisiin Liikenne- ja viestintäviraston lisäksi Pääesikunnan määrätty turvallisuusviranomainen. Pääesikunnan määrätylle turvallisuusviranomaiselle säädettäisiin tehtäväksi toimia itsenäisenä ja riippumattomana arviointiviranomaisena, jolla olisi toimivalta arvioida Puolustusvoimien omia järjestelmiä ja niihin kuuluvia turvallisuuskriittisiä ratkaisuja.

Valtionhallinnon viranomaisille säädettäisiin velvollisuus toteuttaa tietojärjestelmien ja tietoliikennejärjestelyjen arviointi käyttäen arviointilaissa tarkoitettuja arviointimenettelyjä. Arviointimenettely valittaisiin riskiarvioinnin perusteella siten, että valtionhallinnon viranomainen toteuttaisi vähintään itsearvioinnin. Myös muut viranomaiset, kuten kuntien ja hyvinvointialueiden viranomaiset, voisivat käyttää arviointilaissa säädettyjä arviointimenettelyjä tietojärjestelmiensä ja tietoliikennejärjestelyjensä arvioinnissa. Kaikkien viranomaisten tulisi kuitenkin pyytää arviointiviranomaisen arviointia turvallisuusluokan I ja II tietojen käsittelylle. Lisäksi kaikkien viranomaisen tulisi pyytää arviointiviranomaisen arviointia tai hankkia tietoturvallisuuden arviointilaitoksen arviointi turvallisuusluokan III tietojen käsittelylle, ellei viranomainen riskiarvioinnin perusteella päättäisi sen olevan 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. Arviointilaissa säädettyjä arviointiperusteita selkeytettäisiin ja niistä säädettäisiin vähemmän yksityiskohtaisesti.

Arviointilakiin lisättäisiin arviointiviranomaisten yhteistyötä, työjakoa ja tiedonsaantioikeuksia koskevaa sääntelyä sekä turvattaisiin arviointiviranomaisten toiminnan resurssien riittävyyttä säätämällä arviointiviranomaista avustavasta tehtävästä.

Vaatimustenmukaisuudesta annettava todistus ehdotetaan korvattavaksi arviointiraportilla lukuun ottamatta tilanteita, joissa kansainväliset tietoturvallisuusvelvoitteet tai kansainvälinen

yhteistyö taikka muu sääntely edellyttää hyväksyntäpäätöksen tai -lausunnon antamista arvioinnista.

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

Tietoturvallisuuden arviointilaitoksen arviointipätevyyden osoittamisen menettelyjä joustavoitettaisiin. Pätevyysalue liittyisi aina arviointilaitoslain 10 §:ssä säädetyn arviointiperusteen kuten säädöksen, ohjeen tai standardin tuntemukseen. Ehdotetaan, että sen lisäksi, että pätevyyden voisi osoittaa FINASin akkreditoinnilla, ja jokaisella hyväksytyllä tietoturvallisuuden 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 teknisiä muutoksia, jotta arviointilaki ja arviointilaitoslaki muodostavat myös jatkossa yhteentoimivan kokonaisuuden.

4.2 Pääasialliset vaikutukset

4.2.1 Taloudelliset vaikutukset

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 pyytäjän ja hankkijan kannalta selkeänä.

Arviointilakiin ehdotettava uusi mahdollisuus toteuttaa julkisia, salassa pidettäviä ja turvallisuusluokkaan IV luokiteltuja tietoja käsittelevien tietojärjestelmien ja tietoliikennejärjestelyjen arviointi palveluntarjoajan toteuttamana viranomaisen toimeksiannosta vaikuttaa nykyisten tietoturvallisuuden arviointilaitosten toimintaan 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 eikä yritysturvallisuusselvityksen hakeminen tai suojelupoliisin arvio. 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 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. Valtion tieto- ja viestintätekniikkakeskus Valtori käyttää turvallisuusverkkoasetuksen sekä valtiovarainministeriön määräyksen ja ohjeistuksen perusteella turvallisuusluokkiin IV ja III luokiteltuja tietoja käsittelevien tietojärjestelmien ja tietoliikennejärjestelyjen arviointeihin tietoturvallisuuden arviointilaitosten arviointeja. 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 sekä NIS2-direktiivin täytäntöönpanossa kyberturvallisuuslaissa (124/2025) ja tiedonhallintalain 4 a

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

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 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 lisää ennakoitavuutta siitä, millä edellytyksillä arviointeja voidaan tehdä, minkä on arvioitu vähentävän yritysten hallinnollista taakkaa. Hyväksyttyjen ratkaisujen julkiselle listalle tähtäävän kotimaisen valmistajan ratkaisun arviointitehtävän säätäminen Liikenne- ja viestintävirastolle selkeyttää valmistajan kannalta arvioinnin hakemista yhden luukun periaatteella. Toisaalta ehdotettu arviointiviranomaisten yhteistyötä, tiedonvaihtoa ja keskinäistä tehtävistä sopimista koskeva sääntely mahdollistaa arviointiviranomaisten tarkoituksenmukaisen työnjaon arvioinnissa, minkä arvioidaan sujuvoittavan arviointeja ja tukevan valmistajien mahdollisuuksia saada ratkaisuja nopeammin markkinoille. Edellä mainitun yhteistyön ja tehtävistä sopimisen lisäksi arviointilakiin ehdotettu soveltamiskäytännön koordinointi edistävät sitä, että turvallisuuskriittisten ratkaisujen arviointiperusteet ovat yhdenmukaiset, vaikka ratkaisun arvioisi Pääesikunnan määrätty turvallisuusviranomainen Puolustusvoimien tarpeisiin, ja valmistaja hakisi laajempaa hyväksyntää Liikenne- ja viestintävirastolta 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

Valtionhallinnon viranomaisille arviointilaissa ehdotettujen arviointivelvollisuuksien 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 tietoliikennejärjestelyiden tietoturvallisuuden ja varautumisen vaatimustenmukaisuuden toteutumista, hallinnollinen taakka kasvaisi. Toisaalta arviointien toteuttamisen arvioidaan 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. Arviointien toteuttamisesta aiheutuvien kustannusten hillitsemiseksi viranomaiset voisivat mahdollisuuksien mukaan hankkia arviointeja yhdessä.

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 säästäisi vuositasolla noin 458 000 euroa verrattuna siihen, että vastaavat arviointipalvelut ostettaisiin ulkopuolisilta arviointilaitoksilta.

Kaikkien viranomaisten 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 sekä kustannuksia häiriötilanteissa tai kriiseissä.

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.

Tietoturvahäiriöistä aiheutuvia kustannuksia voidaan arvioida karkeasti sen pohjalta, mitä jo tapahtuneet tietoturvallisuuden häiriötilanteet 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 laajentavan arviointien kattavuutta ja tihentävän niiden toteutusväliä sekä parantavan arviointien ajantasaisuutta, mikä kasvattaisi viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden ja varautumisen tasoa. Arviointilakiin lisättävien uusien arviointimenettelyiden ennakoidaan lisäävän arviointien hyödyntämistä tiedonhallintalain tarkoittamina tietoturvallisuustoimenpiteinä. Tietoturvallisuuden arviointi on myös mahdollista yhdistää tiedonhallintalaissa säädettyihin muihin prosesseihin, kuten 18 c §:ssä säädettyyn kyberturvallisuutta koskevan riskienhallinnan toimintaperiaatteiden ja kyberturvallisuuden riskienhallintatoimenpiteiden vaikuttavuuden arvioinnin ylläpitoon sekä 9 §:n mukaiseen tiedonhallinnan muutoksen lausuntomenettelyyn, mikä helpottaa tietoturvallisuuden arviointien toteuttamista.

Viranomainen voi omassa riskiarvioinnissaan pitää tarpeellisena pyytää arviointiviranomaisen arviointia myös sellaisessa tilanteessa, jossa ehdotettu sääntely ei velvoita siihen. Jo voimassa olevan arviointilain mukaisesti Liikenne- ja viestintävirasto priorisoi siltä pyydetyt arvioinnit. Ehdotettu arviointilain 4:n § 3 momentti mahdollistaisi kuitenkin myös sen, että Liikenne- ja viestintävirasto voisi päätöksellään jättää siltä pyydetyn arvioinnin tekemättä. Liikenne- ja viestintävirasto ottaa laissa ehdotettujen perusteiden valossa arviointipyyntöjen priorisoinnissa huomioon pyydettyjen toimenpiteiden yleisen merkityksen viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden yleiseen parantamiseen taikka yhteiskunnan elintärkeiden toimintojen suojaamiseen. Sinänsä minkään viranomaisen pyynnön ei voi katsoa olevan vailla yhteiskunnallista merkitystä, mutta Liikenne- ja viestintävirasto voi joutua toteamaan, ettei se voi ottaa pyydettyä arviointia tehtäväksi resurssien puutteen vuoksi. Liikenne- ja viestintävirasto voi tällöin tukea arviointia pyytävää viranomaista neuvonnalla. Arvioinnin tekeminen tai tekemättä jättäminen ei vaikuta siihen, että vastuu tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuudesta ja varautumisesta on tiedonhallintayksiköllä.

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.

Arviointilain soveltamisalan laajentaminen tietoturvallisuuden arvioinnin lisäksi varautumiseen tukee valmiuslain 12 §:ssä säädettyä viranomaisen varautumisvelvollisuutta varmistaa tehtäviensä hoitaminen myös poikkeusoloissa. Varautumisen arviointien toteuttaminen saattaa lisätä viranomaisten hallinnollista taakkaa, koska tietojärjestelmien ja tietoliikennejärjestelyjen varautumisen arviointi ei ole vakiintunut käytäntö ja sitä koskevat ehdotetut velvollisuudet olisivat viranomaisille uusia. Samalla arviointikohteiden toiminnan jatkuvuus kuitenkin paranee, mikä vähentää hallinnollista taakkaa ja kustannuksia häiriötilanteissa ja poikkeusoloissa.

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

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

Esityksessä ei ehdoteta resurssilisäyksiä arviointiviranomaisille.

Ehdotetuilla Liikenne- ja viestintäviraston tehtävillä ei ole olennaisia resurssi- tai kustannusvaikutuksia siltä osin, kun tehtävät koskevat tietojärjestelmien ja tietoliikennejärjestelyjen taikka niihin kuuluvan turvallisuuskriittisen ratkaisun 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.

Suomalaisille turvallisuuskriittisten ratkaisujen valmistajille ehdotettava oikeus hakea arviointia ja hyväksyntää Liikenne- ja viestintävirastolta ei edellytä lisäresursseja virastolle. 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 hyväksyntä- ohjaus- 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. Hajasäteilysuojaratkaisujen arviointia osana järjestelmiä tehdään jo nykytilassa korkeimpien turvallisuusluokkia käsittelevien järjestelmien arviointien yhteydessä. Näin ollen Liikenne- ja viestintäviraston tai Pääesikunnan määrätyn turvallisuusviranomaisen 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 ehdotetulla sääntelyllä arviointiviranomaisten yhteistyöstä eikä mahdollisuudella sopia tehtävän tai sen osan hoitamisesta toisen arviointiviranomaisen lukuun.

Tietojärjestelmien ja tietoliikennejärjestelyjen varautumisen arviointi on sisällöltään uusi osa-alue. 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. Tietoturvallisuuden arviointilaitosten ja turvallisuuskriittisiä ratkaisuja valmistavien ja tarjoavien yritysten määrä ei kuitenkaan ole suuri, joten vaikutus suojelupoliisiin tehtäviin olisi vähäinen. Tietoturvallisuuden arviointilaitosten osalta suojelupoliisi tekee nykyiselläänkin vastuuhenkilöiden henkilöturvallisuusselvityksiä ja voi lausua toimitiloista, mutta tehtävä laajentuisi muihinkin yritysturvallisuusselvityksen osa-alueisiin, kuten hallinnolliseen turvallisuuteen, yrityksen taustojen selvittämiseen 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 TEMPEST-yritysten pieni lukumäärä.

Arviointilaitoslakiin ehdotettu Liikenne- ja viestintäviraston velvollisuus pyytää lausuntoa pätevyyden hyväksymisen kannalta keskeisiltä viranomaisilta koskisi etenkin sosiaali- ja terveydenhuollon tietojärjestelmien vaatimuksenmukaisuudesta vastaavia viranomaisia, mutta ei suoraan vaikuttaisi näiden viranomaisten tehtäviin, vaan selkeyttäisi arviointilaitoslain, asiakastietolain ja toisiolain välistä suhdetta. Samoin ehdotettu Liikenne- ja viestintäviraston oikeus saada tietoturvallisuuden arviointilaitosten vaatimusten täyttymisen valvonnassa välttämättömiä tietoja sosiaali- ja terveydenhuollon tietojärjestelmien vaatimuksenmukaisuudesta vastaavilta viranomaisilta selkeyttäisi viranomaisten suhdetta ja yhteistyötä, jota viranomaiset tekevät jo ennestään.

Tiedonhallinnan muutokset

Ehdotetuilla arviointilain muutoksilla selvennettäisiin 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 ehkäisemään. 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 niiden toiminnan 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.

Puolustusvoimien arviointitehtävän arvioidaan vaikuttavan myönteisesti kansallisen turvallisuuden kehittymiseen, koska Puolustusvoimien tietojärjestelmien ja tietoliikennejärjestelyjen 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 tietoturvallisuuden 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 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 järjestelmiin. Siten toimeksiannosta toteutettu arviointi edellyttää huolellista arviointikohteen perusteella toteutettua kansallisten riskien arviointia sekä palveluntarjoajan luotettavuuden ja viranomaisten tietojen asianmukaiseen suojaamisen varmistamista. Täten voidaan saavuttaa edellä jaksoissa 4.2.1 ja 4.2.2.1 kuvatut palveluntarjoajien 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

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.

4.2.2.4 Tietosuoja

Ehdotettava sääntely koskee viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden ja varautumisen arviointia. Arviointien kohteena olevissa järjestelmissä käsitellään tyypillisesti henkilötietoja ja arviointitoiminta voi käytännössä edellyttää myös henkilötietojen käsittelyä. Näin ollen ehdotettavan sääntelyn vaikutuksia on tarpeen arvioida myös suhteessa henkilötietojen suojaan.

Ehdotettavalla sääntelyllä voidaan arvioida olevan myönteisiä vaikutuksia henkilötietojen suojaan siltä osin kuin se vahvistaa valtionhallinnon viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden ja varautumisen riskiperusteista arviointia koko elinkaaren ajan sekä parantaa teknisten ja organisatoristen suojatoimien suunnitelmallista toteuttamista ja ylläpitoa. Tämä on omiaan vähentämään henkilötietoihin kohdistuvia tietoturvariskejä ja lieventämään tietoturvaloukkausten todennäköisyyttä ja vaikutuksia erityisesti järjestelmissä, joissa käsitellään korostuneen suojan tarpeessa olevaa tietoa ja joissa loukkausten seuraukset voivat olla merkittäviä myös rekisteröidylle. Muiden kuin valtionhallinnon viranomaisten osalta myönteiset vaikutukset kohdistuvat erityisesti sellaisiin tietojärjestelmissä ja tietoliikennejärjestelyissä käsiteltävien henkilötietojen suojaan, joissa käsitellään turvallisuusluokkiin I–III luokiteltuja tietoja.

Tietosuoja-asetuksen (EU) 2016/679 5 artiklan 2 kohdan mukaisen osoitusvelvollisuuden mukaan rekisterinpitäjän on pystyttävä osoittamaan, että henkilötietojen käsittelyssä noudatetaan henkilötietojen käsittelyä koskevia periaatteita. Tietosuoja-asetuksen 24 artiklan mukaan rekisterinpitäjän tulee riskiperusteisesti toteuttaa tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja osoittaa, että käsittelyssä noudatetaan tietosuoja-asetusta. Lisäksi tietosuoja-asetuksen 32 artikla edellyttää, että rekisterinpitäjä varmistaa henkilötietojen käsittelyn turvallisuuden riskit huomioon ottaen. Ehdotetut arviointivelvollisuudet ja arviointimenettelyt ovat lähtökohtaisesti yhdenmukaisia tietosuoja-asetuksen riskiperusteisen lähestymistavan kanssa ja voivat käytännössä tukea rekisterinpitäjiä näiden velvoitteiden täyttämisessä erityisesti käsittelyn turvallisuutta koskevien vaatimusten osalta. Ehdotettu sääntely ei kuitenkaan korvaa rekisterinpitäjän velvollisuutta tehdä henkilötietojen käsittelyä koskeva riskinarviointi tai toteuttaa tietosuoja-asetuksen mukaiset toimenpiteet kokonaisuutena, vaan täydentää ja tukee niitä tietoturvallisuuden ja varautumisen arvioinnin näkökulmasta.

Arviointimenettelyt voivat lisätä henkilötietojen käsittelyä arviointien yhteydessä, koska arviointi voi edellyttää pääsyä järjestelmiin ja niiden teknisiin tietoihin. Arviointitoiminnan yhteydessä tapahtuva henkilötietojen käsittely on luonteeltaan pääosin tietoturvan ja varautumisen todennusta ja kontrollien arviointia, eikä arviointien tarkoituksena ole arvioida rekisteröityjä koskevia asiasisältöjä tai tehdä rekisteröityihin kohdistuvia päätelmiä. Henkilötietojen suojaan kohdistuvia riskejä kasvattaa se, että arviointeihin voi sisältyä teknisiä arviointitoimenpiteitä ja pääsyä tietojärjestelmiin sekä se, että arviointien toteuttamiseen voi osallistua arviointiviranomaisen ohella ulkopuolinen asiantuntija, palveluntarjoaja tai hyväksytty tietoturvallisuuden arviointilaitos ja sen alihankkijat.

Henkilötietojen suojaan kohdistuvien riskien hallinta perustuu tietosuoja-asetuksen periaatteisiin ja rekisterinpitäjän velvollisuuksiin. Rekisterinpitäjän on varmistettava, että arviointitoiminnan yhteydessä henkilötietoja käsitellään vain arvioinnin toteuttamiseksi välttämättömässä laajuudessa ja testidataa tai anonymisoitua/pseudonymisoitua aineistoa suositaan aina, kun se on arviointitavoitteen kannalta mahdollista. Lisäksi rekisterinpitäjän tulee varmistaa, että arviointitoimintaan osallistuvien toimijoiden roolit ja vastuut henkilötietojen käsittelyssä sekä mahdollinen alihankintaketju ovat selkeitä ja asianmukaisesti järjestettyjä ja että arviointiaineistoon kohdistuvat käyttöoikeudet ja suojatoimet vastaavat riskitasoa.

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 tietoturvallisuuden arviointilaitosten arviointitoiminnan rinnalla. Valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämismalli ja Valtorin toiminta perustuu kuitenkin erilliseen lainsäädäntöön, toisin sanoen Tori-lakiin ja julkisen hallinnon turvallisuusverkkotoiminnasta annettuun lakiin (10/2015), eikä tämän esityksen puitteissa ole prosessiekonomisista syistä mahdollista arvioida valtion yhteisten tieto- ja viestintäteknisten palvelujen vaatimustenmukaisuuden arviointiin liittyviä erityiskysymyksiä. Valtorin roolia arviointitoimijana olisi tarkoituksenmukaisempaa tarkastella valtion yhteisten toimialariippumattomien ja turvallisuusverkon toiminnan ja niihin liittyvän lainsäädännön päivittämisen yhteydessä huomioiden riskienhallintaan perustuvat arviointilain periaatteet

Esitystä valmisteltaessa on arvioitu myös mallia, jossa arviointilakiin ehdotettavat valtionhallinnon viranomaisia koskevat arviointivelvollisuudet 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.

Arviointivelvollisuus 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.

Kaikkia viranomaisia koskevaa arviointivelvollisuutta tarkasteltaessa esillä oli myös vaihtoehto, jossa valtioneuvoston asetuksella olisi voitu 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 arviointivelvollisuuksista säädettäisiin lain tasolla ja tästä velvollisuudesta asetuksella, ei ollut. Myöskään ei nähty mahdolliseksi lain tasolla tunnistaa selkeästi tarkempia kriteerejä, joiden perusteella arviointivelvollisuudesta olisi tullut säätää asetuksella. 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.

Valmistelun yhteydessä selvitettiin mahdollisuutta säätää tietoturvallisuuden arviointilaitosten oikeudesta hakea oman tai alihankkijan henkilöstön luotettavuuden varmistamiseksi turvallisuusselvityslain mukaisia henkilöturvallisuusselvityksiä ja suojelupoliisi voisi tarpeettomien turvallisuusselvitysten laadinnan estämiseksi antaa arviointeja suorittaville henkilöille henkilöturvallisuusselvitystodistuksen. Ehdotusta selvitettiin sillä perusteella, että arviointien yhteydessä laitoksille kertyy tietoja viranomaisten tietojärjestelmien toteutuksista,

turvallisuusjärjestelyistä sekä niihin liittyvistä puutteista ja haavoittuvuuksista. Ehdotuksella ajateltiin myös voitavan välttää moninkertaiset päällekkäiset selvitykset tietoturvallisuuden arviointilaitosten viranomaisasiakkaiden hakemina. Tietoturvallisuuden arviointilaitokset pitävät henkilöturvallisuusselvityksiin liittyviä haasteita tällä hetkellä merkittävästi arviointitoimeksiantojen sujuvuuteen vaikuttavana ongelmana. Ehdotuksen valmistelusta kuitenkin luovuttiin, koska turvallisuusselvityslain vallitsevan soveltamiskäytännön lähtökohtana on, että selvitystä voi hakea se, jonka suojattavasta edusta on kysymys. Vaikka tietoturvallisuuden arviointilaitoksille annettaisiin soveltamiskäytännöstä poiketen oikeus turvallisuusselvitysten hakemiseen, viranomaisten olisi mahdollisesti silti haettava selvitystä myös itse. Asiaa olisi tarkoituksenmukaista tarkastella turvallisuusselvityslain päivityksen yhteydessä

Arviointimenettelyjen sujuvoittamisen liittyviä muutostarpeita on esityksen valmistelussa käsitelty laajemmin kuin mitä esitettyihin muutoksiin sisältyy. 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 edellä kuvatun 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 suojaamiseen liittyvät vaatimukset muista tietojärjestelmiä ja tietoliikennejärjestelyjä koskevista arviointivaatimuksista. Turvallisuusluokitellun tiedon suojaamisen vaatimuksista ja käytännöistä kattavimpina vertailukohtina voi pitää EU:n ja Naton turvallisuusluokitellun tiedon suojaamista koskevia turvallisuussääntöjä. Useissa valtioissa Nato-sääntelyn toimintamalleja sovelletaan myös kansallisen turvallisuusluokitellun tiedon suojaamisessa. Siten Nato-sääntely on merkittävin kansainvälisten ja kansallisten turvallisuusluokiteltujen tietojen käsittelyyn liittyvä arviointisääntely. EU:n turvallisuusluokitellun tiedon käsittelyä koskeva arviointiin liittyvä sääntely on Nato-sääntelyn kanssa pääsääntöisesti yhtenevää. Suomessa turvallisuusluokitellun tiedon suojaamista koskevassa sääntelyssä eli turvallisuusluokitteluasetuksessa on pyritty huomioimaan riittävä yhteensopivuus EU:n turvallisuussääntöjen kanssa.

EU:n ja Naton turvallisuussääntöjen esityksen kannalta merkityksellisimpiä 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 tietoturvallisuudesta on järjestelmän haltijalla, mutta sen liikkumavaraa riskiarvioinnissa 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 tietojärjestelmän 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, jotka liittyvät tuotteiden ja ratkaisujen valmistukseen ja tietoturvallisuusvaatimuksiin. 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. Turvallisuusäännöissä edellytetään tiukkaa ohjausta ja valvontaa, mutta ei oteta kantaa siihen, kuinka asia kansallisesti toteutetaan oikeudellisesti. TEMPEST-yritysten nimeäminen voi siten perustua kansalliseen sääntelyyn tai kansalliseen hallintosopimukseen. Suomessa myös hallintosopimuksen tulee perustua lakiin.

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

6.1 Lausuntokierros

Esitys oli lausuntokierroksella ajalla 27.11.2025.-23.1.2026. Esityksestä vastaanotettiin yhteensä 55 lausuntoa, jotka sisälsivät lausuttavaa. Lausuntopalautteesta on laadittu lausuntoyhteenveto, jossa kuvataan lausuntojen keskeisin palaute ja merkityksellisimmät näkökannat. Lausuntopalaute ja lausuntoyhteenveto on saatavilla Valtioneuvoston hankeikkunasta hanketunnuksella VM167:00/2023, osoitteessa: https://vm.fi/hanke?tunnus=VM167:00/2023.

6.2 Yleisvaikutelma lausunnoista

Yleisvaikutelma lausunnoista on, että esitystä kannatettiin. Ehdotuksia pidettiin ajankohtaisena ja perusteltuna, ja niiden katsottiin vastaavan turvallisuusympäristön muutoksiin.

Valtionhallinnon viranomaisten palautteessa nousi ennakoidusti esiin huoli mahdollisista arviointivelvollisuuksien aiheuttamista kasvavista resurssitarpeista. Lausuntopalaute vahvistaa esityksen vaikutusten arvioinnissa esitetyn mahdollisuuden, että ehdotetut arviointivelvollisuudet aiheuttavat kustannuksia valtionhallinnon viranomaisille. Ehdotettujen arviointivelvollisuuksien mukaisia arviointeja tehdään kuitenkin myös nykytilassa, joten kyse ei olisi täysin uusista kustannuksista. Jo nykytilassa valtionhallinnon viranomaisten tietojärjestelmien ja erityisesti viranomaisten turvallisuusluokan I-II tietoja käsittelevien järjestelmien arviointikustannukset ovat olennainen osa järjestelmien rakentamis- ja elinkaarikustannuksia, ja niihin vaikuttavat muun muassa teknologiset valinnat, hankintamallit sekä tavoiteltu turvallisuustaso. Viranomaiset voivat kuitenkin kattaa vähimmäistason mukaiset arviointikustannukset olemassa olevilla määrärahoillaan. Lisäksi etenkin liikenne- ja

viestintäministeriön lausunnossa nostettiin esiin, että arviointiviranomaisten käytettävissä olevat resurssit vaikuttavat arviointien toteuttamisen tehokkuuteen, vaikuttavuuteen ja aikatauluun.

Useassa lausuntopalautteessa nostettiin esiin itsearvioinnin mahdollistama joustavampi arviointi, mutta todettiin myös, että itsearviointien teettäminen edellyttää tarkempaa ohjeistusta esimerkiksi niiden laajuuden ja tarkkuuden osalta. Itsearviointien lisäksi lausuntopalautteessa toivottiin ohjausta etenkin varautumisen arvioinnin, arviointipalvelujen hankinnasta palvelutarjoajilta sekä kriteeristöjen käytön osalta. Lakimuutosten toimeenpanon yhteydessä on tarkoitus laatia ohjeistusta lausuntopalautteessa esiin nostetuista kokonaisuuksista. Tämä ei aiheuta muutostarpeita tähän esitykseen.

Kuntaliiton lausunnossa todetaan, että esityksen vaikutukset kuntiin ovat pieniä, koska valtionhallinnon viranomaisten kunnille jakamia turvallisuusluokkaan I - III luokiteltuja tietoja tulee kuntien käsiteltäväksi hyvin vähän. Hyvinvointialueiden osalta Etelä-Karjalan hyvinvointialue kannatti sitä, että soveltamisalan laajentamista ei ulotettaisi kuntiin ja hyvinvointialueisiin, sillä laajentaminen aiheuttaisi kustannusten nousua.

6.3 Lausunnoista tarkemmin ja pääasialliset muutokset jatkovalmistelussa

Eduskunnan oikeusasiamiehen, Oikeuskanslerin viraston ja Pohjois-Karjalan käräjäoikeuden lausunnoissa nostettiin esiin, että esityksessä tulisi huomioida ylimpien laillisuusvalvojien, eduskunnan virastojen ja tuomioistuinten valtiosääntöinen eritysasema. Mainittujen lausuntojen johdosta esitettyjen arviointivelvollisuuksien soveltamisalasta suljettiin pois eduskunnan oikeusasiamiehen ja valtioneuvoston oikeuskanslerin toiminta sekä tuomioistuimet ja valitusasioita käsittelemään perustetut lautakunnat, tasavallan presidentin kanslia ja eduskunnan virastot. Jatkovalmistelun aikana arviointivelvollisuuksien soveltamisesta tuomioistuimiin keskusteltiin oikeusministeriön kanssa. Soveltamisalan osalta esitykseen lisättiin organisatorista soveltamisalaa koskeva kappale jaksoon 10.

Suojelupoliisi esitti lausunnossaan itselleen arviointiviranomaisen asemaa sillä perusteella, että sen tietojärjestelmät sisältävät erittäin sensitiivistä ja arkaluonteista sisältöä. Jatkovalmistelun aikana asiasta keskusteltiin suojelupoliisin kanssa. Lausunnon ja keskustelujen perusteella päädyttiin ratkaisuun, jossa suojelupoliisiin ei sovellettaisi arviointilaissa ehdotettua velvollisuutta valita arviointimenettely riskiarvioinnin ja turvallisuusluokan perusteella.

Oikeusministeriön lausunnon perusteella esitykseen lisättiin henkilötietojen suojaa koskevien vaikutusten arviointi jaksoon 4.2.2.4 ja tietosuoja-asetuksen kansallisen liikkumavaran käytön arviointi jaksoon 10.

Lausuntopalautteessa esitettiin myös yksityiskohtaisempia tarkennustarpeita, joiden johdosta esityksen perusteluja täydennettiin. Oikeusministeriön lausunnossa esitettiin tarkennuksia arviointilain 3 d, 4, 4 b, 6 ja 7 a §:iin sekä arviointilaitoslain 5, 7, 13 §:iin, jotka on huomioitu joko tarkentamalla säädöskohtaisia perusteluita tai pykälien sanamuotoa. Arviointilaitoslain 5 §:n mukaisen viranomaiskuulemisen laajuutta ja roolia täsmennettiin perusteluihin Terveyden ja hyvinvoinnin laitoksen esittämän perusteella. Lisäksi Liikenne- ja viestintäviraston sekä liikenne- ja viestintäministeriön lausunnoissa esitettiin tarkennuksia, jotka on huomioitu jatkovalmistelussa, merkittävämpänä näistä arviointilain 6 §:ssä esitettyjen tarkastusoikeuksien laajentaminen koskemaan Pääesikunnan määrättyä turvallisuusviranomaista sen hoitaessa tehtävää ehdotetun 4 b §:n 2 momentin mukaisesti. Lisäksi esityksen jakson 10 säätämisjärjestysperusteluita on tarkennettu jatkovalmistelussa. Jatkovalmistelussa esitykseen tehtiin myös yksittäisiä tarkennuksia yhteistyössä Liikenne- ja viestintäviraston, liikenne- ja

viestintäministeriön, Puolustusvoimien ja puolustusministeriön kanssa. Liikenne- ja viestintäministeriön kanssa yhteistyössä arvioitiin etenkin arviointilaitoslain 2 §:n 1 momenttiin ehdotettua vaatimusta Suomeen sijoittautumisesta muun muassa Euroopan unionin sisämarkkinasääntelyn kannalta. Arvioinnin perusteella ehdotetusta sijoittautumisvaatimuksesta päätettiin luopua, sillä sen lisäämistä lain tasolle ei pidetty pakollisena.

Fintraffic pyysi lausunnossaan tarkentamaan, onko julkista hallintotehtävää hoitavalla toimijalla oikeus tai velvollisuus toteuttaa laissa tarkoitettuja arviointimenettelyjä. Arviointilakia sovelletaan vain sen viranomaismääritelmään sisältyviin toimijoihin, jolloin lakia eikä siinä säädettyjä velvollisuuksia tai oikeuksia sovelleta julkista hallintotehtävää hoitavan toimijan toiminnassa. Esitykseen ei tehty muutoksia tämän lausunnon johdosta.

Lausuntopalautteessa tehtiin myös joitakin uusia esityksiä koskien esimerkiksi ehdotettujen arviointilain 3–3 c §:n selkeyttä, arviointiraporttien toimittamista, ehdotetun arviointilain 8 a §:n mukaisen luettelon julkisutta sekä arviointien tekemisen riskiarvioinnin sitomista myös muihin kriteereihin kuin turvallisuusluokkiin. Näitä ehdotuksia ei jatkovalmistelussa kuitenkaan pidetty tarkoituksenmukaisina tai mahdollisina toteuttaa esityksen puitteissa. FINAS-akkreditointipalvelun esittämiä tarkennustarpeita ehdotetun arviointilaitoslain 7 §:n ja 5 §:n perusteluiden osalta ei pidetty jatkovalmistelussa mahdollisena huomioida, sillä ehdotukset perustuvat Euroopan unionin turvallisuussääntöihin, tavanomaiseen julkisuuslain mukaiseen salassa pidettävän tiedon suojaamiseen viranomaisten välisessä tehtävien kannalta välttämättömässä tiedonvaihdossa ja tavanomaiseen viranomaisyhteistyöhön sisältyvään kuulemiseen toisen viranomaisen tehtäviin ja asiantuntemukseen kuuluvissa asioissa.

7 Säännöskohtaiset perustelut

7.1 Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista

1 § *Soveltamisala.* Lain soveltamisalaa laajennettaisiin siten, että pykälän *1 momenttiin* lisättäisiin varautumisen arviointi sekä turvallisuuskriittisen ratkaisujen ja niiden valmistuksen tietoturvallisuuden arviointi.

Laissa säädettäisiin jatkossa viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioimisen lisäksi myös viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen varautumisen arvioinnista. Näin ollen arviointilain arviointimenettelyjä, arviointiperusteita ja muita säännöksiä sovellettaisiin myös varautumisen arviointiin. Soveltamisalan laajentaminen edistäisi tietojärjestelmien ja tietoliikennejärjestelyjen jatkuvuudenhallintaan ja valmissuunnitteluun vaikuttavien tekijöiden johdonmukaista huomioimista viranomaisissa.

Lisäksi laissa säädettäisiin turvallisuuskriittisten ratkaisujen ja niiden valmistuksen 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 tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuutta koskevissa määrättyjen turvallisuusviranomaisten tehtävissä, ellei kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa toisin säädetä tai kansainvälisestä tietoturvallisuusvelvoitteesta muuta johdu. Kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa säädetään muun muassa määrättyjen turvallisuusviranomaisten tehtäväjaosta. Kansainvälisiä tietoturvallisuusvelvoitteita sisältyy myös EU:n tai Naton turvallisuussääntöihin ja kahdenvälisiin tietoturvallisuussopimuksiin. Tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuutta koskeviin kansainvälisiin tietoturvallisuusvelvoitteisiin sisältyy salausratkaisujen ja muiden turvallisuuskriittisten ratkaisujen sekä hajasäteilysuojauksen eli TEMPESTin arviointi- ja hyväksyntätehtäviä. 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 voimassa olevaa 2 momenttia tietyin muutoksin. 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.

Momentti vastaisi voimassa olevaa momenttia sen osalta, että siinä viitattaisiin turvallisuusselvityslakiin Liikenne- ja viestintäviraston tehtävien osalta yritysturvallisuusselvitystä laadittaessa. Momenttiin lisättäisiin viittaus Liikenne- ja viestintäviraston kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa säädettyihin tehtäviin. Edellä mainitun lain 4 §:n mukaan virasto toimii määrättynä turvallisuusviranomaisena tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuutta koskevissa asioissa. Arviointilaissa säädettävät arviointiviranomaisen tehtävät eivät vaikuttaisi kansainvälisiin tietoturvallisuusvelvoitteisiin liittyviin arviointi- ja hyväksyntätehtäviin.

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

Pykälän *1 kohta* vastaisi voimassa olevan lain 1 kohtaa, eli tietojärjestelmällä tarkoitettaisiin tietojenkäsittelylaitteista, ohjelmistoista ja muusta tietojenkäsittelystä koostuvaa kokonaisjärjestelyä.

Pykälän *2 kohtaa* muutettaisiin siten, että 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.

Tietojärjestelmä ja tietoliikennejärjestely voivat sisältää turvallisuuskriittisiä ratkaisuja. Määritelmien mukaisella tietojen käsittelyllä viitattaisiin sähköiseen tietojen käsittelyyn.

Pykälän *3 kohdassa* 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. Siten viranomaisen määritelmään sisältyisi voimassa olevan lain määritelmän lisäksi myös julkisuuslain 4 §:n 1 momentin 8 kohdan mukaiset tiettyä tehtävää itsenäisesti hoitamaan asetetut työryhmät ja vastaavat sekä hyvinvointialueen ja hyvinvointiyhtymän, kunnan ja kuntayhtymän tilintarkastajat sekä muut niihin verrattavat toimielimet. 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.

Pykälän *4 kohta* vastaisi voimassa olevaa lakia, eli valtionhallinnon viranomaisella tarkoitettaisiin valtion hallintoviranomaisia ja muita valtion virastoja ja laitoksia sekä tuomioistuimia ja muita lainkäyttöviranomaisia.

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 tiedon käsittelyssä turvataan tiedon luottamuksellisuus eli tietosisällön suojaaminen oikeudettomalta käytöltä, tiedon eheys eli muuttumattomuus sekä tiedon saatavuus huomioiden mahdolliset tiedon luottamuksellisuudesta aiheutuvat saatavuuden rajoitukset. 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 toteuttamiseksi käytetyt menettelyt voivat olla 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 varautumisen määritelmästä. Varautumisella tarkoitettaisiin toimia, joilla huolehditaan tietojärjestelmien ja tietoliikennejärjestelyjen hyödyntäminen ja niihin perustuvan toiminnan jatkuminen mahdollisimman häiriöttömästi normaaliolojen häiriötilanteissa sekä valmiuslain mukaisissa poikkeusoloissa. 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 tarkastelua ja hallintaa ja toiminnan varajärjestelyjä.

Tiedonhallintayksikön varautumisvelvoitteesta säädetään tiedonhallintalain 13 a §:n 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 arviointilaissa tarkoitettua yritystä, yhteisöä tai viranomaista, joka tarjoaa arviointipalveluita ja jonka Liikenne- ja viestintävirasto on arviointilaitoslain mukaisesti hyväksynyt. Määritelmä vastaisi voimassa olevan lain 3 §:n viittausta tietoturvallisuuden arviointilaitoksiin ja arviointilaitoslakiin.

Pykälään lisättäisiin uusi *8 kohta,* jossa säädettäisiin turvallisuusluokan määritelmästä. Turvallisuusluokalla tarkoitettaisiin tiedonhallintalain 18 §:n 1 momentissa ja pykälän 4 momentin nojalla annetussa valtioneuvoston asetuksessa tarkoitettua turvallisuusluokkaa. Voimassa olevan turvallisuusluokitteluasetuksen 3 §:n mukaan turvallisuusluokkia ovat turvallisuusluokat I, II, III ja IV.

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 tietoliikennejärjestelyjen välillä. Määritelmä olisi teknologiariippumaton. 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 4–5 kohtien mukaiset ulkomaisen yhteisön tai säätiön Suomessa oleva sivuliike tai eurooppayhtiö, eurooppaosuuskunta ja eurooppalainen taloudellinen etuyhtymä eivät käytännössä tulisi kysymykseen ehdotetun 4 §:n 2 momentin 1 kohdassa tarkoitetun valmistuksen kotimaisuusedellytyksen ja ehdotetun 7 a §:n mukaisesti haettavassa yritysturvallisuusselvityksessä tehtävän ulkomaisen vaikutuksen mahdollisuuden poissulkemisen johdosta.

3 § *Tietoturvallisuuden ja varautumisen arviointimenettelyt.* Pykälän otsikko muutettaisiin tietoturvallisuuden arviointipalvelujen käyttämisestä tietoturvallisuuden ja varautumisen arviointimenettelyksi. Muutettu pykälä sisältäisi säännökset arviointimenettelyistä ja niiden käyttöä koskevista rajoitteista.

Pykälän *1 momenttia* muutettaisiin siten, että siinä säädettäisiin viranomaisen käytettävissä olevista arviointimenettelyistä. Arviointimenettelyjä ehdotetaan lisättäväksi nykyisestä siten, että viranomaisen toteuttama itsearviointi ja palveluntarjoajan viranomaisen toimeksiannosta toteuttama arviointi olisivat arviointimenettelyjä voimassa olevan lain mukaisten tietoturvallisuuden arviointilaitoksen 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 esimerkiksi tiedonhallintalain 9 § mukaisen tiedonhallinnan muutosta koskevan lausuntomenettelyn yhteydessä. Itsearvioinnin toteuttava viranomainen voisi myös hyödyntää Valtion tieto- ja viestintätekniikkakeskus Valtorilta saatua arvioitavaa tietojärjestelmää tai tietoliikennejärjestelyä koskevaa tietoturvallisuusraporttia.

Momentin *2 kohdassa* säädettäisiin palveluntarjoajan viranomaisen toimeksiannosta 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. Palveluntarjoajan viranomaisen toimeksiannosta toteuttamalla arvioinnilla tarkoitettaisiin muun kuin tietoturvallisuuden arviointilaitoksen tai muun viranomaisen kuin ehdotetussa 3 d §:ssä tarkoitetun arviointiviranomaisen toteuttamaa arviointia.

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

Pykälään lisättäisiin uusi *2 momentti,* jossa säädettäisiin, että viranomainen voisi toimeksiannosta hankkia palvelutarjoajalta arvioinnin tietojärjestelmistä ja tietoliikennejärjestelyistä, joissa käsitellään julkisia, salassa pidettäviä tai korkeintaan turvallisuusluokan IV tietoja. 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 2 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 tietoliikennejärjestelyjä 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.

Palveluntarjoajan luotettavuuden varmistaminen on erityisen 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. 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. Erityistä huomiota tulisi kiinnittää siihen, missä tietojärjestelmissä ja tiloissa palveluntarjoaja käsittelee viranomaisen salassa pidettäviä tai turvallisuusluokiteltuja tietoja.

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.

Viranomainen voisi hyödyntää palveluntarjoajan kanssa tehtävän hankintasopimuksen laatimisessa hankintojen tietoturvallisuusvaatimusten asettamista koskevia suosituksia, ohjeita, määräyksiä ja työkaluja sekä yhteishankintajärjestelyjä. Yhteishankintajärjestelyihin voitaisiin sisällyttää 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 *3 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. Tietoturvallisuuden arviointilaitoksista ja niiden riippumattomuudesta, luotettavuudesta ja pätevyydestä säädetään arviointilaitoslaissa. Tietoturvallisuuden arviointilaitokset on arvioitu turvallisiksi ja osaaviksi arvioida turvallisuusluokkaa III käsitteleviä tietojärjestelmiä ja tietoliikennejärjestelyitä.

3 a § *Valtionhallinnon viranomaisen arviointivelvollisuudet.* Lakiin lisättäisiin uusi 3 a §, jossa säädettäisiin valtionhallinnon viranomaisten arviointivelvollisuuksista. Lisäksi pykälässä säädettäisiin tietyistä arviointivelvollisuuksien soveltamisen rajauksista.

Pykälän *1 momentissa* säädettäisiin valtionhallinnon viranomaisten arviointivelvollisuudesta arvioida tietojärjestelmiensä ja tietoliikennejärjestelyjensä tietoturvallisuutta ja varautumista

käyttäen 3 §:ssä säädettyjä menettelyjä, toisin sanoen itsearviointia, palveluntarjoajan toteuttamaa arviointia, tietoturvallisuuden arviointilaitoksen toteuttamaa arviointia tai arviointiviranomaisen toteuttamaa arviointia.

Pykälän *2 momentissa* säädettäisiin arviointimenettelyn valinnasta. Valtionhallinnon viranomainen valitsisi riskiarvioinnin perusteella millä menettelyllä tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuutta 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 ehdotetun 3 §:n 2 ja 3 momenteissa säädettäväksi ehdotettujen rajoitteiden lisäksi momentin 1 ja 2 kohdassa ehdotetut arviointivelvollisuudet.

Momentin *1 kohdassa* säädettäisiin valtionhallinnon viranomaisille velvollisuus pyytää turvallisuusluokkaan I tai II luokiteltuja tietoja käsittelevien tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden ja varautumisen arviointi arviointiviranomaiselta. Velvollisuus olisi perusteltu, koska korkeimpien turvallisuusluokkiin luokiteltuja tietoja käsittelevien tietojärjestelmien ja tietoliikennejärjestelyjen arviointi vaatii tiettyä erityisosaamisista korkeimpien turvallisuusluokkien toiminnallisista vaatimuksista, toimintaympäristöstä ja turvallisuusjärjestelystä, joista arviointiviranomaisilla on vankka osaaminen.

Momentin *2 kohdassa* säädettäisiin valtionhallinnon viranomaisille velvollisuus pyytää tai hankkia turvallisuusluokkaan III luokiteltuja tietoja käsittelevien tietojärjestelmien tai tietoliikennejärjestelyjen tietoturvallisuuden ja varautumisen arviointi arviointiviranomaiselta tai tietoturvallisuuden arviointilaitokselta, ellei se olisi valtionhallinnon viranomaisen riskiarvion perusteella tarpeetonta. Riskiarviossa tulisi huomioida samat seikat, kuin momentin johdantokappaleen 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 valtionhallinnon viranomainen päättäisi riskiarvion perusteella olla pyytämättä arviointiviranomaisen tai hankkimatta tietoturvallisuuden arviointilaitoksen arviointia, tulisi päätös tehdä viranomaisen sisäisen ratkaisuvallan mukaisesti, mikä usein edellyttää johdon hyväksyntää.

Momentin *3 kohdassa* säädettäisiin valtionhallinnon viranomaisten arviointivelvollisuuden minimitasosta, eli siitä, että valtionhallinnon viranomaisen tulisi toteuttaa aina vähintään tietojärjestelmiensä ja tietoliikennejärjestelyjensä tietoturvallisuuden ja varautumisen itsearviointi.

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. Ehdotettuja arviointivelvollisuuksia ei siten olisi välttämätöntä sitoa ainoastaan tietojärjestelmän ja tietoliikennejärjestelyn käyttöönottoon, vaan arviointeja olisi tarkoituksenmukaista toteuttaa säännöllisesti tietojärjestelmien ja tietoliikennejärjestelyjen elinkaaren ajan. Turvallisuusluokkaan I, II ja III luokiteltuja tietoja käsittelevien tietojärjestelmien ja tietoliikennejärjestelyjen arviointien uusiminen olisi tarkoituksenmukaista punnita riskiarvioinnin perusteella esimerkiksi muutosten yhteydessä.

Pykälän *3 momentissa* säädettäisiin tiettyjen viranomaisten rajaamisesta arviointimenettelyn valintaa koskevien velvollisuuksien ulkopuolelle.

Ensinnäkin momentissa säädettäisiin, että ehdotetun 2 momentin mukaisia arviointimenettelyn valintaa koskevia velvollisuuksia ei sovellettaisi suojelupoliisin toimintaan. Ehdotus olisi perusteltu, sillä suojelupoliisin tietojärjestelmät sisältävät erittäin sensitiivistä ja arkaluonteista sisältöä, jonka potentiaalinenkin päätyminen kolmannelle osapuolelle voisi vaarantaa suojelupoliisin tiedonhankintaa ja siten kansallista turvallisuutta. Suojelupoliisin arvion mukaan sillä, että arvioinnin suorittaisi suojelupoliisista ulkopuolinen taho olisi kansallista turvallisuutta heikentävä vaikutus.

Lisäksi momentissa säädettäisiin, että pykälän 2 momentin mukaisia arviointimenettelyn valintaa koskevia velvollisuuksia ei sovellettaisi eduskunnan oikeusasiamiehen eikä valtioneuvoston oikeuskanslerin toimintaan, tuomioistuimiin, valitusasioita käsittelemään perustettuihin lautakuntiin, tasavallan presidentin kansliaan eikä eduskunnan virastoihin. Ehdotetut soveltamisalan rajoitukset johtuvat pääosin näiden julkiseen sektoriin kuuluvien organisaatioiden perustuslaissa säädetystä asemasta, jonka perusteella valtion keskushallintoon kuuluvien viranomaisten ohjaustoimivaltaa ei voida ulottaa näiden organisaatioiden sisäisen hallinnon ohjaukseen.

Ehdotettujen pykälän 2 momentin mukaisten arviointivelvollisuuksien ulkopuolelle rajatut viranomaiset valitsisivat käyttämänsä arviointimenettelyt oman harkintansa perusteella 3 §:ssä säädetyistä menettelyistä. Tämä tarkoittaisi sitä, että ne voisivat myös pyytää tietoturvallisuuden arviointia Liikenne- ja viestintävirastolta tai hankkia arvioinnin tietoturvallisuuden arviointilaitokselta. Pykälän 2 momentin velvollisuuksien ulkopuolelle rajatut viranomaiset vastaavat itse käyttämiensä tietojärjestelmien tietoturvallisuustoimenpiteistä. Näin ollen edellä mainitut viranomaiset päättävät myös itse missä määrin ne huomioisivat Liikenne- ja viestintävirastolta tai tietoturvallisuuden arviointilaitokselta saadun arviointiraportin tehdessään tietojärjestelmiään koskevia päätöksiä.

3 b § *Muiden kuin valtionhallinnon viranomaisten arviointivelvollisuudet.* Lakiin lisättäisiin uusi 3 b §, jossa säädettäisiin muiden kuin valtionhallinnon viranomaisten, eli muiden kuin ehdotetussa 3 a §:ssä tarkoitettujen viranomaisten arviointivelvollisuuksista, jotka koskisivat turvallisuusluokiteltuja tietoja käsittelevien tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden ja varautumisen arviointia.

Pykälän *1 momentissa* säädettäisiin muille kuin valtionhallinnon viranomaiselle ehdotetun 3 a §:n 2 momentin 1 kohtaa vastaava velvollisuus pyytää turvallisuusluokkaan I tai II luokiteltuja tietoja käsittelevien tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden ja varautumisen arviointi arviointiviranomaiselta.

Pykälän *2 momentissa* säädettäisiin muille kuin valtionhallinnon viranomaiselle ehdotetun 3 a §:n 2 momentin 2 kohtaa vastaava velvollisuus pyytää tai hankkia turvallisuusluokkaan III luokiteltuja tietoja käsittelevien tietojärjestelmien tai tietoliikennejärjestelyjen tietoturvallisuuden ja varautumisen arviointi arviointiviranomaiselta tai tietoturvallisuuden

arviointilaitokselta, ellei se olisi viranomaisen riskiarvion perusteella tarpeetonta. Riskiarvion toteuttaminen vastaisi myös ehdotetun 3 a §:n mukaista riskiarvioita.

Vaikka tiedonhallintalaissa ja turvallisuusluokitteluasetuksessa säädetty velvollisuus turvallisuusluokitella asiakirjoja ei koske muita kuin valtion viranomaisia, on mahdollista, että muutkin viranomaiset käsittelevät turvallisuusluokiteltua tietoa tietojärjestelemässään tai tietoliikennejärjestelyssään, jolloin ehdotetun pykälän arviointivelvollisuudet tulisivat sovellettaviksi. Tietojen käsittelyllä tarkoitettaisiin 2 §:n 5 kohdan perusteluihin kirjatusti myös tietojen säilyttämistä ja arkistointia, joten velvoite koskisi myös viranomaisia, jotka säilyttäisivät tai arkistoisivat turvallisuusluokan I, II ja III tietoja tietojärjestelmissä tai tietoliikennejärjestelyissä.

Ehdotettujen muita kuin valtionhallinnon viranomaisia koskevien arviointivelvollisuuksien lisäksi nämä viranomaiset, esimerkiksi kunnat, voisivat hyödyntää arviointilain mukaisia tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden ja varautumisen arviointimenettelyjä laajemminkin osana tiedonhallintalain 13§:n mukaista tietojenkäsittelyn riskien selvittämistä ja tietoturvallisuustoimenpiteiden mitoittamista. Tietoturvallisuuden ja varautumisen arviointien toteuttaminen tai hankkiminen tukisi viranomaisten tietojenkäsittelyyn liittyvää riskienhallintaa. Arviointilain mukaisia arviointeja toteuttaessaan muita kuin valtionhallinnon viranomaisia koskisivat myös ehdotetun 3 a §:n 2 ja 3 momenttien rajoitukset arviointimenettelyjen käytössä.

3 c § *Vaatimusten täyttymisen osoittaminen.* Lakiin lisättäisiin uusi 3 c §, jossa säädettäisiin viranomaisen mahdollisuudesta pyytää arviointiviranomaisen hyväksyntää tietojärjestelmälleen tai tietoliikennejärjestelylleen osoittaakseen tietoturvallisuutta koskevien vaatimusten täyttyminen pykälän tarkoittamissa tilanteissa. 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 tarkoittaisi, 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. 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.

Pykälän *1 kohdassa* tarkoitettu kansainvälisistä tietoturvavelvoitteista annetun lain mukainen kansainvälinen tietoturvallisuusvelvoite voisi perustua esimerkiksi EU:n tai Naton turvallisuussääntöihin taikka Suomen tietoturvallisuussopimusten sopimusmääräyksiin. Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 4 §:n mukaan tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuutta koskevat asiat ovat määrättynä turvallisuusviranomaisena Liikenne- ja viestintäviraston tehtäviä.

Pykälän *2 kohdassa* tarkoitettu muun kansainvälisen yhteistyön tilanne voisi syntyä esimerkiksi, kun toisen valtion kanssa ei ole solmittu tietoturvallisuussopimusta, eikä siten synny 1 kohdassa tarkoitettua valtiosopimukseen perustuvaa kansainvälisistä tietoturvallisuusvelvoitteista annetun lain tarkoittamaa kansainvälistä tietoturvallisuusvelvoitetta, mutta riippumaton arviointi ja tietoturvallisuusvaatimusten täyttymisen toteaminen on käytännössä välttämätöntä kansainvälisen yhteistyön toteutumiseksi. Tällöin pääesikunnan määrätty

turvallisuusviranomainen Puolustusvoimien pyynnöstä ja Liikenne- ja viestintävirasto muun viranomaisen pyynnöstä voisi tarvittaessa laatia hyväksynnän, jota kansainvälisessä yhteistyössä edellytetään.

Pykälän *3 kohdassa* tarkoitettuja säädettyjä edellytyksiä arviointiviranomaisen hyväksynnästä vaatimuksenmukaisuudelle ei voimassa olevassa sääntelyssä ole.

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

Pykälän *1 momentissa* säädettäisiin arviointiviranomaisista, joita olisivat Liikenne- ja viestintävirasto ja kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 4 §:n 1 momentissa tarkoitettu Pääesikunnan määrätty turvallisuusviranomainen (DSA Designated Security Authority). Liikenne- ja viestintävirasto hoitaa arviointitehtäviä jo voimassa olevan lain nojalla, mutta Pääesikunnan määrätylle turvallisuusviranomaiselle tehtävä olisi uusi. Puolustusvoimien arviointitehtävä on tarpeen säätää nimenomaisesti Pääesikunnan määrätylle turvallisuusviranomaiselle toiminnan riippumattomuuden varmistamiseksi. Pääesikunnan määrätyn turvallisuusviranomaisen tehtävistä säädetään muutoin kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa.

Arviointien tekeminen kuuluisi pääsääntöisesti Liikenne- ja viestintäviraston toimivaltaan. Pääesikunnan määrätyn turvallisuusviranomaisen toimivaltaan kuuluisivat arvioinnit, jotka koskevat 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 Puolustusvoimien omien tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden ja varautumisen arviointeja sekä Puolustusvoimien omassa toiminnassa tarvitsemien turvallisuuskriittisten ratkaisujen arviointeja.

Pykälän *2 momentissa* säädettäisiin, että 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. Säännöksen tarkoituksena olisi varmistaa toiminnan riippumattomuus.

Pykälän *3 momentissa* säädettäisiin, että arviointiviranomaiselta edellytettäisiin organisatorista ja päätöksenteon riippumattomuutta sille kuuluvien arviointitehtävien hoitamisessa. Arviointiviranomaisen tulisi pystyä tuottamaan arvioinnin kohteesta objektiivista tietoa, joka perustuu sen arvioinnissa saamiin selvityksiin tai muuten arvioinnissa hankkimaan tietoon. Arviointiviranomaisen tulisi siten olla tehtävissään riippumaton arvioinnin kohteen päätöksenteosta eikä arvioinnin kohteen tulisi voida vaikuttaa arviointiviranomaisen havaintoihin tai päätelmiin. Riippumattomuus voitaisiin varmistaa esimerkiksi viranomaisen työjärjestyksessä.

Riippumattomuuden edellytys koskisi 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 tietoliikennejärjestelyn suunnittelua, rakentamista tai ylläpitoa.

Lisäksi 3 momentissa säädettäisiin, että arviointiviranomaisen olisi varmistettava, että sen palveluksessa olevilla tai lukuun toimivilla olisi oltava tarkastuksen laatuun ja laajuuteen nähden riittävä koulutus ja kokemus. Lukuun toimivalla viitattaisiin Pääesikunnan määrätyn turvallisuusviranomaisen nimeämään Puolustusvoimien palkattuun henkilöstöön kuuluvaan henkilöön. Arviointiviranomaisen olisi varmistettava, että arvioinnin suorittajalla on kyseisten tehtävien suorittamiseen vaadittavat taidot ja että tarkastus toteutetaan objektiivisesti. Osana riittävän koulutuksen ja kokemuksen varmistamista, arviointiviranomaisen tulisi seurata teknistä kehitystä ja ylläpitää ja kehittää osaamistaan jatkuvasti arvioinnin kohteiden edellyttämällä tavalla.

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 arviointiviranomaisten eli Liikenne- ja viestintäviraston sekä Pääesikunnan määrätyn turvallisuusviranomaisen tehtävästä arvioida viranomaisen pyynnöstä tietojärjestelmän tai tietoliikennejärjestelyn taikka niihin kuuluvan turvallisuuskriittisen ratkaisun tietoturvallisuutta ja varautumista. Momentti vastaisi voimassa olevan 1 momentin 1 kohtaa muutettuna siten, että siihen lisättäisiin turvallisuuskriittisten ratkaisujen tietoturvallisuuden arviointi osana tietojärjestelmien ja tietoliikennejärjestelyjen arviointia sekä varautumisen arviointi uutena arviointitehtävänä. Tehtävään sisältyisivät myös ehdotetussa 3 c §:ssä tarkoitetun hyväksynnän antaminen viranomaisen hakemuksesta sekä ehdotetussa 8 §:ssä tarkoitettujen arviointiraportin, hyväksyntäpäätöksen ja -lausunnon antaminen.

Pykälän *2 momenttia* muutettaisiin siten, että siinä säädettäisiin tehtävistä, jotka olisi osoitettu vain Liikenne- ja viestintävirastolle. Momentin *1 kohdan* mukaan viraston tehtävänä olisi käsitellä Suomeen sijoittuneiden valmistajien arviointipyynnöt turvallisuuskriittisten ratkaisujen ja niiden valmistuksen tietoturvallisuuden 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. 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.

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 1 momentissa säädetyn mukaisesti.

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 tietoturvallisuuden arviointilaitosten hyödyntämistä viranomaisen tietojärjestelmän tai tietoliikennejärjestelyn arvioinnissa. Liikenne- ja viestintävirasto voisi antaa neuvontaa tietojärjestelmän ja tietoliikennejärjestelyn suunnitteluvaiheessa, arvioinnin kohdentamisessa ja arviointiperusteiden valinnassa, jolloin tietoturvallisuuden arviointilaitoksen arviointitehtävä voitaisiin suunnata tehokkaasti testaamiseen ja todentamiseen.

Momentin *3 kohdassa* säädettäisiin Liikenne- ja viestintäviraston uudesta tehtävästä ohjata ja valvoa 8 § 3 momentin mukaisen hyväksyntäpäätöksen saaneen hajasäteilysuojausratkaisuja valmistavan turvallisuuskriittisen ratkaisun valmistajan toimintaa ja antaa tarvittaessa päätös valmistuksen ja ratkaisun vaatimuksista. Tarkoituksena olisi edistää 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 loisivat 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 Liikenne- ja viestintäviraston tulisi ottaa huomioon asettaessaan tehtäviään tärkeysjärjestykseen huomioiden käytettävissä olevat voimavarat, ja tehdessään päätöksen siitä, ottaako virasto pyydetyn arvioinnin tehtäväksi. Virasto voisi myös ottaa haetun arvioinnin tehtäväksi vain osittain. Arvioinnin kohteen teknisestä määrittämisestä säädetään muutoin 7 §:ssä.

Momentin *1 kohdan* mukaan Liikenne- ja viestintäviraston tulisi jatkossakin huolehtia ensisijaisesti kansainvälisten tietoturvallisuusvelvoitteiden edellyttämistä arvioinneista. Momentin *2 kohdan* mukaan viraston tulisi myös huomioida ehdotettujen 3 a ja 3 b §:n mukaiset viranomaisten arviointivelvollisuudet, *3 kohdan* mukaan tiedon turvallisuusluokka ja *4 kohdan* mukaan muun riippumattoman arvioinnin saatavuus. Käytännössä Liikenne ja viestintäviraston tulisi siis ottaa turvallisuusluokkiin I ja II luokiteltua tietoa käsittelevien järjestelmien arviointi

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.

Lisäksi Liikenne- ja viestintäviraston tulisi huomioida *5 kohdan* mukaan suomalaisten turvallisuuskriittisten ratkaisujen tarjonnan edistäminen ja *6 kohdan* mukaan arvioinnin pyytäjien ja hakijoiden yhdenvertainen kohtelu. Momentin *7 kohta* vastaisi voimassa olevan momentin säädöstä pyydettyjen toimenpiteiden yleisen merkityksen huomioimisesta viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden yleiseen parantamiseen, sillä lisäyksellä, että huomioon tulisi ottaa myös yhteiskunnan elintärkeiden toimintojen suojaaminen.

Pykälään lisättäisiin uusi *4 momentti*, joka vastaisi voimassa olevan pykälän 2 momenttia. Momentissa säädettäisiin näin ollen siitä, että 1 momentin mukaisen arviointipyynnön Liikenne- ja viestinvirastolle voisi tehdä viranomaisen toimeksiannosta tehdä myös se, joka tekee viranomaisen lukuun hankintoja taikka tuottaa tietojenkäsittely- tai tietoliikennepalveluja taikka hoitaa niiden järjestämiseen liittyviä palvelutehtäviä. Voimassa olevan lain esitöiden mukaan säädöksellä on haluttu varmistaa se, että tietojenkäsittely- ja tietoliikennepalveluja käyttävät voisivat varmistua, että heidän valtionhallinnon eri viranomaisille tarjoamat palvelut täyttävät valtionhallinnon tietoturvallisuudelle asetettavat vaatimukset (HE 45/2011 vp s. 11).

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. Henkilöresurssien hankkiminen yksityisilta markkinoilta tulisi mahdollistaa viranomaisarviointien resurssien varmistamiseksi. Arviointiviranomaisten voi olla vaikeaa saada rekrytoitua riittävästi henkilöstöä arviointitehtäviin, sillä osaavia henkilöresursseja on niukasti. Arvioinnista aiheutuvista kustannuksista vastaisi sama taho kuin arviointiviranomaisen tekemästä arvioinnista. Arviointiviranomaisen tulisi siten sopia ulkopuolisen asiantuntijan käytöstä arvioinnin kustannuksista vastaavan tahon kanssa.

Arviointiin osallistuvalla ulkopuolisella asiantuntijalla olisi oltava arviointitehtävän laatuun ja laajuuteen nähden riittävä koulutus ja kokemus. 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 sovellettaisiin rikosoikeudellisia

virkavastuuta koskevia säännöksiä. Lisäksi 1 momentin loppuun lisättäisiin informatiivinen säännös siitä, että vahingonkorvauksesta säädetään vahingonkorvauslaissa (412/1974).

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, testauksen, 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 salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä. Tiedonvaihto olisi olennainen osa yhteistyötä. Yhteistyön ja tiedonvaihdon tarkoituksena olisi ehkäistä päällekkäistä työtä, edistää yhteistä tilannekuvaa julkisen hallinnon arviointitarpeista ja osaamisen jakamista sekä teknisen kehityksen ja tietoturvauhkien huomioimista ja yhdenmukaista vaatimusten tulkintaa arviointitoiminnassa.

Pykälän *2 momentissa* säädettäisiin, että 3 d §:n 1 momentissa säädettyjen toimivaltuuksien ja 4 §:n 1 ja 2 momentissa säädettyjen arviointiviranomaisten tehtävien estämättä arviointiviranomaiset voisivat 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.

Arviointiviranomaiset voisivat sopia toisen arviointiviranomaisen lukuun hoidettavista tehtävistä siltä osin, kun kyse ei olisi hallintopäätöksellä ratkaistavasta asiasta, kuten

hyväksyntä- tai valvontatehtävästä. Hallintopäätöksellä ratkaistavien asioiden osalta arviointiviranomaiset voisivat sopia vain asian selvittämiseen liittyvän tehtävän hoitamisesta toisen lukuun. Näin ollen ehdotetun yhteistyön tarkoituksena ei olisi siirtää arviointiviranomaisen päätös- ja toimivaltaa toiselle, vaan kyse olisi enemmänkin avustavasta tehtävästä.

Pykälän *3 momentissa* velvoitettaisiin Liikenne- ja viestintävirasto ohjaamaan ja 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. Koordinaation avulla tulisi huolehtia siitä, että Puolustusvoimien toiminnalliset vaatimukset saatettaisiin valmistajien tietoon.

5 § *Selvitykset valtiovarainministeriön toimeksiannosta.* Pykälää muutettaisiin siten, että toimivaltaisen viranomaisen nimeksi muutettaisiin teknisenä muutoksena 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 voimassa olevan yksikössä olevan selvitys-termin sijaan.

Pykälän *2 momentissa* voimassa olevan lain tiedonsaantioikeus sen estämättä mitä tietojen salassapidosta säädetään, päivitettäisiin muotoon salassapitosäännösten tai muiden tiedon luovuttamista koskevien rajoitusten estämättä. Liikenne- ja viestintäviraston antaman arvion sijaan säädettäisiin Liikenne- ja viestintäviraston antamasta selvityksestä. Kyse on teknisestä muutoksesta, jotta terminologia saadaan vastamaan 1 momenttiin ehdotettuja muutoksia.

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

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.

Tiedonsaantioikeudet sidottaisiin välttämättömyysperusteeseen voimassa olevassa pykälässä säädetyn tarpeellisuusperusteen sijaan. Tietojen välttämättömyyden arviointi olisi arviointiviranomaisen tehtävä, jolloin sen olisi perusteltava tietojen välttämättömyys pyytäessään niitä viranomaisilta ja yrityksiltä arviointien, selvitysten tai valvonnan suorittamiseksi. Lisäksi voimassa olevan lain tiedonsaantioikeus sen estämättä mitä tietojen salassapidosta säädetään, päivitettäisiin muotoon salassapitosäännösten tai muiden tiedon luovuttamista koskevien rajoitusten estämättä. Muita tiedon luovuttamista koskevia rajoituksia voivat olla esimerkiksi yrityksen liike- tai ammattisalaisuudet.

Pykälän 1 momenttia muutettaisiin myös siten, että arvioitavana tai selvityksen kohteena olevaa tietojärjestelmää tai tietoliikennejärjestelyjä koskevien tietojen sijaan tiedonsaantioikeudet koskisivat tässä laissa säädettyjä tehtäviä. Muutos olisi perusteltu, koska ehdotetut uudet arviointiviranomaistehtävät sisältävät tietojärjestelmän tai tietoliikennejärjestelyn arvioinnin lisäksi myös esimerkiksi turvallisuuskriittisten ratkaisujen ja niiden valmistuksen arvioinnin sekä ohjauksen ja valvonnan.

Pykälän 1 momentissa säädettyä arviointiviranomaisen oikeutta päästä tiloihin ja tietojärjestelmään tarkennettaisiin siten, että pääsyoikeuksiin lisättäisiin myös tietoliikennejärjestely. Lisäksi tiedonsaantioikeuden kohteiksi lisättäisiin 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 ja Pääesikunnan määrätyn turvallisuusviranomaisen, sen hoitaessa tehtävää arviointilain 4 b §:n 2 momentissa tarkoitetulla tavalla Liikenne- ja viestintäviraston lukuun, tarkastusoikeudesta hajasäteilysuojausratkaisuja tarjoavan valmistajan ehdotetun 4 § 2 momentin 3 kohdassa tarkoitetussa valvonnassa. Liikenne- ja viestintävirastoa ja Pääesikunnan määrättyä turvallisuusviranomaista voisi tarkastuksessa avustaa 4 a §:ssa tarkoitettu avustava asiantuntija. Tarkastuksen tarkoituksena olisi selvittää, noudattaako valmistaja tämän lain nojalla annettuja päätöksiä. Tämän lain nojalla annetuilla päätöksillä viitattaisiin ehdotetun 8 §:n 3 momentin mukaiseen hyväksyntäpäätökseen sekä ehdotetun 4 §:n 2 momentin 3 kohdan mukaiseen päätöksentekoon. Erotuksena 1 momentissa tarkoitetuissa arvioinneissa ja selvityksissä tehtäviin arviointitoimenpiteisiin hajasäteilysuojaratkaisujen valvontaan liittyvissä tarkastuksissa olisi kysymys hallintolain 39 §:n mukaisesta tarkastuksesta. 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 ehdotetussa 2 momentissa tarkoitettua 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* johdantokappaletta täydennettäisiin siten, että viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden lisäksi pykälän arviointiperusteet soveltuisivat tietojärjestelmien ja tietoliikennejärjestelyjen varautumisen sekä turvallisuuskriittisten ratkaisujen ja niiden valmistuksen tietoturvallisuuden arviointiin.

Pykälän 1 momentin arviointiperusteiden luettelon tarkoituksena olisi mahdollistaa laajasti eri arviointiperusteiden käyttäminen. Momentin *1 kohtaan* lisättäisiin kyberturvallisuus- ja

varautumisvaatimukset tietoturvallisuusvaatimusten lisäksi. Viranomaisten toiminnalle 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 voimassa olevan 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, määräysten tai ohjeiden mahdollisena antajana. Kohtaan lisättäisiin myös viranomaisten ohjeet kansainvälisten toimielimien säännösten ja ohjeiden soveltamisesta. 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. Säädetyillä vaatimuksilla tarkoitettaisiin esimerkiksi julkisuuslain, tiedonhallintalain ja turvallisuusluokitteluasetuksen säännöksiä. Riskiarvion tekeminen perustuisi uhkien tunnistamiseen. 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, viranomaisen toiminnalle, arvioinnin kohteen toiminnan kiinnostavuuteen pahantahtoisten toimijoiden kannalta, yhteisöjen ja kansalaisten palvelujen saatavuudelle tai tiettyyn tekniseen toteutustapaan. Arviointiperusteiden määrittämisen riskiarviossa tulisi myös 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. Arviointi voi perustua suppeaankin joukkoon vaatimuksiin perustuvia arviointikriteerejä.

Arvioinnin kohteen määrittämisellä tarkoitettaisiin niitä rajauksia, joita arvioinnin suunnittelussa tehdään. Arvioinnin kohde voi vaihdella aina yhdestä työasemasta monen toimipisteen verkkoon tai olla esimerkiksi organisaatiossa laajasti käytössä oleva monikansallisen toimittajan pilvipalvelu. 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.

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

Viranomaisen itsearvioinnissa ja palveluntarjoajan viranomaisen toimeksiannosta toteuttamassa arvioinnissa viranomainen asettaisi arviointiperusteet, arvioinnin kohteen ja sen kohdentamisen. Arviointiperusteista tietoturvallisuuden arviointilaitoksen ja sen asiakkaan toimeksiantosuhteessa säädetään arviointilaitoslaissa.

Pykälään lisättäisiin uusi *3 momentti,* jossa säädettäisiin turvallisuuskriittisten ratkaisujen ja niiden valmistuksen arviointiperusteiden määrittämisestä. Arviointiviranomainen määrittäisi ratkaisuun ja valmistukseen soveltuvat arviointiperusteet 1 momentin arviointiperusteiden kokonaisuudesta hyvän hallintotavan mukaisesti valmistajaa kuultuaan. 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 tulisi pyrkiä edistämään 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 § *Turvallisuuskriittisen ratkaisun valmistajan arviointiin liittyvät selvitykset.* Lakiin lisättäisiin uusi 7 a §, jossa säädettäisiin turvallisuuskriittisen ratkaisun valmistajan arviointiin liittyvistä selvityksistä.

Pykälän *1 momentissa* säädettäisiin Liikenne- ja viestintävirastolle uusi menettelyyn liittyvä velvoite hakea turvallisuusselvityslaissa tarkoitettua yritysturvallisuusselvitystä arviointia hakevasta valmistajasta 4 §:n 2 momentin 1 kohdassa tarkoitetun turvallisuuskriittisen ratkaisun ja sen valmistuksen 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 erityisesti ulkomaisen vaikutuksen riskit. Valmistuksen turvallisuus ja luotettavuus tarkoittaisi esimerkiksi yrityksen omistukseen, vastuuhenkilöihin, taloudelliseen tilanteeseen, turvallisuuskriittisten ratkaisujen valmistukseen kuuluvien toimitusketjujen sekä toimitilojen ja valmistukseen vaikuttavien tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuutta. Valmistukseen liittyvien seikkojen merkitystä tulisi punnita suhteessa turvallisuuskriittisen ratkaisun turvallisuusluokkaan ja luonteeseen ja alttiuteen luotettavuuden vaarantumiselle.

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.

Ehdotus 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.

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 tehtävästä antaa hyväksyntäpäätös tai -lausunto, kun viranomainen on hakenut hyväksyntää ehdotetun 3 c §:n mukaisesti ja arvioitava tietojärjestelmä tai tietoliikennejärjestely täyttää sille arvioinnissa asetetut vaatimukset. Lisäksi momentissa säädettäisiin hyväksyntäpäätökseen tai -

lausuntoon merkittävistä tiedoista. Päätökseen tai lausuntoon tulisi merkitä arviointiviranomaisen hyväksymät arvioinnin kohde ja sen tekninen rajaus, arviointiperusteet, arvioinnin laajuus, arvioinnin tulos ja jäännösriski sekä tarvittaessa voimassaoloaika.

EU:n ja Naton turvallisuusluokitellun tiedon käsittelyyn hyväksyttyjen tietojärjestelmien hyväksynnän 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.

Tietoturvallisuuden arviointilaitoksen myöntämästä todistuksesta säädetään arviointilaitoslaissa.

Pykälään lisättäisiin uusi *3 momentti,* jossa säädettäisiin Liikenne- ja viestintäviraston uudesta tehtävästä antaa suomalaisen valmistajan turvallisuuskriittisen ratkaisun ja sen valmistuksen arvioinnista tekemään hakemukseen ja hajasäteilysuojausratkaisujen valmistajan tekemään hakemukseen valmistajan hyväksymisestä valituskelpoinen hallintopäätös, josta ilmenee arvioinnin tulos. Jos turvallisuuskriittinen ratkaisu täyttää arvioinnille määritetyt vaatimukset, päätös olisi ratkaisun hyväksyntäpäätös, josta tulisi ilmetä hyväksynnän voimassaolo ja ehdot, jotka ovat tarpeen ratkaisun turvallisessa käytössä. 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 turvalliseen käyttöön liittyvien valintojen ja määrittelyjen ehdot voitaisiin merkitä päätökseen tai esimerkiksi sen liitteenä annettavaan käyttöohjeeseen eli käyttöpolitiikkaan. Hajasäteilysuojaratkaisun eli TEMPEST-laitteiden valmistajaa koskevaan hyväksyntäpäätökseen voitaisiin merkitä valmistuksen luotettavuuteen liittyvä tarpeellisia ehtoja.

Jos turvallisuuskriittiselle ratkaisulle ja sen valmistukselle asetetut vaatimukset eivät täyttyisi, valmistaja voisi hyödyntää saamaansa arviointiraporttia ja päätöstä ratkaisun kehittämisessä ja tarjoamisessa.

8 a § *Hyväksyttyjen turvallisuuskriittisten ratkaisujen ja valmistajien luettelo.* Pykälää muutettaisiin siten, että sen sijaan, että siinä säädettäisiin viranomaisen velvollisuudesta hankkia todistus, pykälässä säädettäisiin Liikenne- ja viestintävirastolle uusi tehtävä ylläpitää ja julkaista hyväksyttyjen turvallisuuskriittisten ratkaisujen ja valmistajien luetteloa.

Pykälässä säädettäisiin, että hyväksyttyään turvallisuuskriittisen ratkaisun ehdotetun 4 §:n 2 momentin 1 kohdassa säädetyn tehtävän mukaisesti ja annettuaan ehdotetussa 8 §:n 3 momentissa tarkoitetun hyväksyvän päätöksen turvallisuuskriittisen ratkaisun ja sen valmistuksen 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. Pykälän *1 kohdan* mukaan luettelosta tulisi ilmetä turvallisuuskriittisen ratkaisun nimi, käyttötarkoitus ja versio. Käyttötarkoituksella tarkoitettaisiin esimerkiksi tuotteen tai palvelun tyyppiä tai teknistä käyttötarkoitusta, jota hyväksyntä koskee. Esimerkiksi salausratkaisun käyttötarkoitus voi olla tiedostojen salaaminen tai tietoliikenteen salaaminen.

Pykälän *2 kohdan* mukaan luettelosta tulisi ilmetä tiedon turvallisuusluokka, jonka suojaamiseen ratkaisu on todettu riittäväksi. Luetteloon merkittäisiin tieto kansallisen turvallisuusluokan perusteella ja tarvittaessa EU:n tai Naton turvallisuusluokan perusteella tehdystä arvioinnista.

Pykälän *3 kohdan* mukaan 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.

Pykälän *4 kohdan* mukaan luettelosta tulisi ilmetä hyväksynnän voimassaolo, muutos tai lakkaaminen. 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.

Pykälän 5 *kohdan* mukaan luettelosta tulisi ilmetä hyväksyntään liittyvät turvallisen käytön ehdot ja rajoitukset. Turvallisen käytön ehdoilla tarkoitettaisiin esimerkiksi käyttöpolitiikkaa (*SecOps eli Security Operating Rules*), jossa selostetaan teknisesti käyttötavat, joita turvallisuusluokan mukainen suojaaminen edellyttää. Käyttöpolitiikka tai ratkaisuun liittyvä ohjeistus voi olla salassa pidettävä, mutta luetteloon voidaan merkitä tarvittavat julkiset tiedot sen olemassaolosta. Hyväksyntään voi liittyä myös teknisiä rajoituksia tai rajauksia, joiden olisi tarkoituksenmukaista ilmetä luettelosta.

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

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 tiedonsaanti- ja tarkastusoikeuksista sekä oikeudesta päästä tiloihin ja järjestelmiin säädettään 6 §:ssä.

10 § *Hyväksyntäpäätöksen kumoaminen tai -lausunnon peruuttaminen.* Pykälä ja sen otsikko muutettaisiin vastaamaan ehdotetun 8 §:n muutosta siten, että todistuksen peruuttamisen sijaan pykälässä säädettäisiin hyväksyntäpäätöksen tai -lausunnon peruuttamisesta. Lisäksi Viestintävirasto korvattaisiin arviointiviranomaisella, jotta pykälä kattaisi molemmat arviointiviranomaiset.

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 korvattaisiin viittauksella ehdotetun 8 §:n mukaiseen arviointiraporttiin, lausuntoon tai päätökseen. Lisäksi arviointiviranomaisen antama neuvonta lisättäisiin maksullisiin palveluihin. Muutos vastaisi osittain nykytilaa ja se olisi yhtenevä vallitsevan Liikenne- ja viestintäviraston maksuasetuskäytännön kanssa.

7.2 Laki tietoturvallisuuden arviointilaitoksista

1 § *Lain tarkoitus.* Pykälää täydennettäisiin siten, että lain tarkoituksena olisi voimassa olevan säännöksen lisäksi säätää menettelystä, jonka avulla viranomaiset voivat hankkia riippumattoman tietoturvallisuuden ja varautumisen arvioinnin. Pykälään ehdotettava muutos olisi yhdenmukainen arviointilakiin ehdotettavan 3 §: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 yhdenmukaisesti arviointilakiin ehdotetun kanssa, että tietoturvallisuuden 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* selkeytettäisiin siten, että tietoturvallisuuden arviointilaitos voisi toimintansa hyväksymisen hakemisen lisäksi

hakea hyväksyntää arvioinnin pätevyysaluetta varten Liikenne- ja viestintävirastolta. Tietoturvallisuuden arviointilaitokselle hyväksytyt pätevyysalueet rajaavat mitä tietoturvallisuuden ja varautumisen arviointiperusteita laitos voi käyttää arviointitehtävissään. Tietoturvallisuuden 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.

Lisäksi 1 momentissa Viestintävirasto muutettaisiin Liikenne- ja viestintävirastoksi teknisenä muutoksena.

4 § *Hakemuksen käsittely*. Pykälän *1 momenttiin* lisättäisiin uutena tietoturvallisuuden arviointilaitoksen luotettavuuden selvitysmenettelynä yritysturvallisuusselvitys. Yritysturvallisuusselvitys mahdollistaisi tietoturvallisuuden arviointilaitoksen omistuspohjan selvittämisen ja seurannan sekä vastuuhenkilöiden turvallisuusselvitykset ja nuhteettomuusseurannan. Yritysturvallisuusselvitys kattaisi myös tietoturvallisuuden arviointilaitoksen toimitilat ja tietojärjestelmät, jolloin niiden turvallisuutta ei tarvitsisi tarkastaa erikseen. Liikenne- ja viestintäviraston olisi haettava yritysturvallisuusselvitystä silloin, kun tietoturvallisuuden 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 voimassa olevan lain mukaista selvitysmenettelyä, jossa suojelupoliisille varataan tilaisuus lausua tietoturvallisuuden arviointilaitoksen vastuuhenkilöistä ja toimitiloista. Lisäksi 1 momenttiin lisättäisiin sana selvitys, jotta se kattaisi myös yritysturvallisuusselvitykset.

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

Lisäksi 1 momentissa Viestintävirasto muutettaisiin Liikenne- ja viestintävirastoksi teknisenä muutoksena.

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).

Pykälän 2 momentissa Viestintävirasto muutettaisiin Liikenne- ja viestintävirastoksi teknisenä muutoksena.

5 § *Arviointilaitoksen hyväksyminen.* Pykälän *1 momentin 1–3 ja 5 kohta* vastaisivat voimassa olevaa sääntelyä. Momentin *4 kohtaan* lisättäisiin tietoturvallisuuden arviointilaitoksen hyväksymisen edellytykseksi se, että laitoksen yritysturvallisuusselvityksestä ei ole ilmennyt sellaista arviointilaitoksen omistuspohjaan, alihankintaan, taloudelliseen tilanteeseen tai henkilöstö-, toimitila- ja tietojärjestelmäturvallisuuteen liittyvää seikkaa, joka kokonaisharkinnan perusteella vaarantaisi yrityksen tai vastuuhenkilöiden luotettavuuden tai sitoumustenhoitokyvyn ottaen huomioon myös ulkomaisen vaikutuksen riskin viranomaisen turvallisuusluokitellun tiedon käsittelyn arviointiin liittyvässä 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. Tietoturvallisuuden 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.

Pykälän *2 momentti* vastaisi voimassa olevaa sääntelyä, eli siinä säädettäisiin, että 1 momentin 1–3 kohdassa tarkoitettujen vaatimusten täyttäminen on osoitettava vaatimustenmukaisuuden arviointipalvelujen pätevyyden toteamisesta annetussa laissa (920/2005) säädetyn menettelyn avulla.

Pykälän *3 momenttia* muutettaisiin siten, että siinä säädettäisiin Liikenne- ja viestintäviraston mahdollisuudesta päättää hyväksytyn tietoturvallisuuden arviointilaitoksen uuden pätevyysalueen hyväksynnästä kuultuaan hyväksymisen kannalta keskeisiä viranomaisia, sen estämättä mitä 2 momentissa säädetään. Voimassa olevan pykälän 2 momentin mukaan tietoturvallisuuden arviointilaitoksen riippumattomuus ja pätevyys osoitetaan vaatimustenmukaisuuden arviointipalvelujen pätevyyden toteamisesta annetussa laissa säädetyn menettelyn avulla eli kansallisen akkreditointiyksikön FINASin tekemällä akkreditoinnilla. Muutetun 3 momentin tarkoituksena olisi mahdollistaa lisäpätevyyksien hyväksyntä tietoturvallisuuden 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 tietoturvallisuuden 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 tietoturvallisuuden 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. Ehdotettu keskeisten viranomaisten kuuleminen perustuisi hallintolain 10 §:n mukaiseen toisen viranomaisten avustamiseen. 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. Uuden menettelyn tavoitteena olisi myös keventää ja joustavoittaa uusien pätevyysalueiden hyväksyntäprosessia sekä vähentää tietoturvallisuuden arviointilaitoksille niistä aiheutuvia kustannuksia ja hallinnollista taakkaa.

Pykälän *4 momentti* vastaisi voimassa olevan lain 3 momenttia sillä erotuksella, että momenttiin tehtäisiin tekninen muutos, jossa Viestintävirasto päivitetään Liikenne- ja viestintävirastoksi.

Pykälään lisättäisiin uusi *5 momentti*, joka vastaisi voimassa olevan lain 4 momenttia. Momentissa säädettäisiin siis hyväksymisen määräaikaisuudesta ja hyväksymisen ehdoista.

6 § *Arviointilaitoksen hyväksymisen peruuttaminen.* Pykälän *1 momenttia* muutettaisiin siten, että Liikenne- ja viestintäviraston olisi mahdollista peruuttaa koko arviointilaitoshyväksynnän lisäksi yksittäinen tietoturvallisuuden arviointilaitokselle hyväksytty pätevyysalue. Tietoturvallisuuden arviointilaitoksen laiminlyönnit ja puutteet sen toiminnassa voivat liittyä tietoturvallisuuden arviointilaitoksena toimimiseen yleisemmin tai vain jonkin pätevyysalueen

arviointeihin, minkä 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.

Lisäksi pykälän 1 momenttiin tehtäisiin tekninen muutos, jossa Viestintävirasto päivitetään Liikenne- ja viestintävirastoksi.

Pykälän *2 momenttiin* tehtäisiin 1 momenttia vastaavasti tekninen muutos, jossa Viestintävirasto päivitetään Liikenne- ja viestintävirastoksi.

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 ulotettaisiin koskemaan myös tietoturvallisuuden arviointilaitoksen alihankkijan tiloja ja se koskisi Liikenne- ja viestintäviraston lisäksi, sen toimeksiannosta toimivan asiantuntijan sijaan, sitä avustavaa asiantuntijaa. Pykälän sanamuotoa tarkennettaisiin lisäksi siten, että asiantuntija voisi avustaa Liikenne- ja viestintävirastoa tarkastuksen suorittamisessa, mutta tarkastusoikeus säädettäisiin olevan Liikenne- ja viestintävirastolla. Muutos vastaisi 4 §:n 2 momenttiin ehdotettavaa mahdollisuutta antaa vain avustavia tehtäviä ulkopuoliselle asiantuntijalle. Avustavassa tehtävässä toimivaa ulkopuolista asiantuntijaa voitaisiin käyttää tietoturvallisuuden arviointilaitoksen ja sen 9 a §:ssä tarkoitetun alihankkijan toimitiloja ja menetelmiä koskevassa tarkastuksessa. Lisäksi momenttiin tehtäisiin tekninen muutos, jossa Viestintävirasto päivitetään Liikenne- ja viestintävirastoksi.

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 tai muiden tiedon luovuttamista koskevien rajoitusten estämättä pyynnöstä tietoja, jotka ovat välttämättömiä sen valvomiseksi, että tietoturvallisuuden arviointilaitos täyttää toimintaansa koskevat vaatimukset. Tiedonsaantioikeus koskisi suojelupoliisilta, kansalliselta akkreditointiyksiköltä tai pätevyysalueen arviointiperusteen soveltamista ohjaavalta tai valvovalta viranomaiselta, arviointilaitokselta sekä sen alihankkijalta ja 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.

Pykälää muutettaisiin siten, että siinä olisi jatkossa vain yksi momentti, joka vastaisi voimassa olevan lain 1 momenttia sillä teknisellä muutoksella, että Viestintävirasto muutettaisiin Liikenne- ja viestintävirastoksi.

Voimassa olevan pykälän 2 momentin mukaisista Liikenne- ja viestintäviraston tiedonsaantioikeuksista säädettäisiin jatkossa lain 7 §:n 2 momentissa.

3 luvun otsikkoa muutettaisiin siten, että 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.

Pykälän *3 momenttia* muutettaisiin siten, että todistuksen sijaan siinä säädettäisiin arviointiraportin laatimisesta. Hyväksytyn tietoturvallisuuden arviointilaitoksen olisi laadittava arviointiraportti kaikista suorittamistaan arvioinneista ja siitä tulisi käydä ilmi arvioinnin kohde, 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 sillä erotuksella, 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. Uusi 4 momentti eroaisi voimassa olevasta 3 momentista 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 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 samaan konserniin kuuluvalla yhtiöllä tai muun alihankintana vain, jos konserniyhtiö tai muu alihankkija täyttää 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 tietoturvallisuuden arviointilaitoksella itsellään on pätevyys toimia ja sen tulee pystyä kontrolloimaan alihankkijan toimia kaikissa vaiheissa. Hyväksytyllä tietoturvallisuuden 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 tietoturvallisuuden 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.

Arviointilain ehdotusta vastaavasti ehdotettaisiin tiettyjen viranomaisten, kuten valtiovaranministeriön ja kansallisen turvallisuusviranomaisen ohjeiden mainitsemisen sijaan yleisesti viranomaisen ohjeet säädösten soveltamisesta. Tämä olisi 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, määräysten tai ohjeiden mahdollisena antajana. Kohtaan lisättäisiin myös viranomaisten ohjeet kansainvälisten toimielimien säännösten ja ohjeiden soveltamisesta. Momentin 1 kohdan tavoin myös 2 kohtaan lisättäisiin tietoturvallisuuden lisäksi kyberturvallisuus ja varautuminen. Vaikka arviointiperusteina säädetään kansainvälisistä lähteistä, tietoturvallisuuden arviointilaitosten 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 vallitsevan Liikenne- ja viestintäviraston maksuasetuskäytännön kanssa. 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). Lisäksi pykälään tehtäisiin tekninen muutos, jossa Viestintävirasto muutettaisiin Liikenne- ja viestintävirastoksi.

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). Hallinnon yleislakien soveltaminen sidottaisiin tietoturvallisuuden arviointilaitosten julkisen hallintotehtävien hoitamiseen. Julkisia hallintotehtäviä olisivat arviointilaitoslaissa säädetyt hyväksyttyjen tietoturvallisuuden arviointilaitosten tehtävät. Tehtävät rinnastuvat arviointilaissa säädettyihin arviointiviranomaisen arviointitehtäviin. Lisäksi esimerkiksi asiakastietolaissa ja toisiolaissa säädetään vaatimuksista, jossa toimijalta edellytetään tietoturvallisuuden arviointilaitoksen arviointia tai sen antamaa todistusta, jonka antamiseen voidaan katsoa liittyvän julkisen vallan käyttöä. Hallinnon yleislakeja ei sovellettaisi tietoturvallisuuden arviointilaitosten harjoittaessa muuta, kuin arviointilaitoslain mukaista toimintaa.

Pykälään lisättäisiin uusi *2 momentti*, jossa säädettäisiin tietoturvallisuuden arviointilaitosten vastuuhenkilöiden ja palveluksessa olevien henkilöiden sekä alihankkijoiden palveluksessa olevien henkilöiden virkavastuusta. Rikosoikeudellinen vastuu perustuisi siihen, että hyväksytyn tietoturvallisuuden arviointilaitoksen arviointilaitoslain mukainen toiminta katsottaisiin julkiseksi hallintotehtäväksi. Lisäksi 2 momentin loppuun lisättäisiin informatiivinen säännös siitä, että vahingonkorvauksesta säädetään vahingonkorvauslaissa.

13 a § *Turvallisuusselvitysrekisteriin merkittävät tiedot* Pykälään tehtäisiin tekniset muutokset, jossa Viestintävirasto muutettaisiin Liikenne- ja viestintävirastoksi ja hyväksyttyjen arviointilaitosten sijaan pykälässä käytettäisiin termiä hyväksytty tietoturvallisuuden arviointilaitos.

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

Esityksessä ehdotetaan muutettavaksi arviointilain 8 a §:ä siten, että jatkossa pykälässä säädettäisiin hyväksyttyjen turvallisuuskriittisten ratkaisujen ja valmistajien luettelosta. Voimassa olevan 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. Tämä asetuksenantovaltuus poistettaisiin pykälän muutoksen myötä. Asetuksenantovaltuutta ei ole käytetty sen voimassaoloaikana.

9 Voimaantulo

Ehdotetaan, että lait tulevat voimaan syksyllä 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 ja varautumisen arviointimenettelyjen saattamisen ehdotettujen uusien arviointivelvollisuuksien 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 valtionhallinnon viranomaisen olisi arvioitava tietojärjestelmänsä ja tietoliikennejärjestelynsä ehdotettujen uusien arviointilain 3 a §:ssä säädettyjen velvollisuuksien mukaisesti viiden vuoden kuluessa, kuitenkin siten, että turvallisuusluokkaan I ja II luokiteltua tietoa käsittelevien järjestelmien arviointia olisi pyydettävä arviointiviranomaiselta kahden vuoden kuluessa lain voimaatulosta ja turvallisuusluokkaan III luokiteltua tietoja käsittelevien järjestelemien arviointia olisi pyydettävä arviointiviranomaiselta tai se olisi hankittava tietoturvallisuuden arviointilaitokselta kolmen vuoden kuluessa lain voimaantulosta, mikäli viranomainen ei pitäisi sitä riskiarvioinnin perusteella tarpeettomana. Myös muiden kuin valtionhallinnon viranomaisten tulisi arvioida turvallisuusluokkaan I, II ja III luokiteltuja tietoja käsittelevien tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuus ja varautuminen vastaavissa aikarajoissa kuin valtiohallinnon viranomaisen, eli turvallisuusluokkaan I ja II luokiteltuja tietoja käsittelevät järjestelmät kahden vuoden kuluessa ja turvallisuusluokkaan III luokiteltuja tietoja käsittelevät järjestelmät kolmen vuoden kuluessa lain voimaantulosta.

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

Arviointilaitoslakia koskevat muutokset sisältäisivät siirtymäsäännöksen, koska lain voimaantullessa hyväksytyillä tietoturvallisuuden arviointilaitoksilla voi olla voimassa olevia turvallisuusluokitellun tiedon käsittelyn arviointiin hyväksyttyjä pätevyysalueita, esimerkiksi Katakri turvallisuusluokan IV ja turvallisuusluokan III pätevyysalueet. Näiden pätevyysalueiden hyväksymisen edellytyksenä olisi ehdotettujen arviointilaitoslain 4 §:n ja 5 §:n 1 momentin 4 kohdan mukaisesti yritysturvallisuusselvitys, jossa ei ole ilmennyt sellaista seikkaa, joka kokonaisharkinnan perusteella vaarantaisi yrityksen tai vastuuhenkilöiden luotettavuuden tai sitoumustenhoitokyvyn arviointitehtävässä. Liikenne- ja viestintäviraston tulisi ehdotetun arviointilaitoslain 4 §:n mukaisesti hakea yrityksistä yritysturvallisuusselvitykset. Ehdotettujen muutosten voimaantullessa tietoturvallisuuden arviointilaitoksilla ei olisi mahdollisuuksia välittömästi noudattaa uusia turvallisuusluokittelun tiedon käsittelyn arvioinnin pätevyyden hyväksymiselle asetettuja vaatimuksia.

Arviointilaitoslakiin ehdotetaan siirtymäaikaa siten, että arviointilaitoslain 4 §:n ja 5 §:n 1 momentin 4 kohdan vaatimuksia yritysturvallisuusselvityksen osalta koskisi kahden vuoden siirtymäaika. Liikenne- ja viestintäviraston tulisi hakea arviointilaitoslain 4 §:n mukaisesti yritysturvallisuusselvitykset niistä hyväksytyistä tietoturvallisuuden arviointilaitoksista, joille on ennen ehdotetun muutoksen voimaantuloa hyväksytty pätevyysalue turvallisuusluokitellun tiedon käsittelyn arviointiin, viimeistään kahden vuoden kuluessa lain voimaantulosta. Liikenne- ja viestintäviraston tulisi ottaa huomioon arviointilaitosten toiveet kyseisten selvitysten hakemisen ajankohdasta. Mikäli hyväksytty arviointilaitos hakee uutta turvallisuusluokitellun tiedon käsittelyn arvioinnin pätevyyttä lain voimaantulon jälkeen, yritysturvallisuusselvitys tulee hakea hakemuksen käsittelyn yhteydessä.

10 Suhde perustuslakiin ja säätämisjärjestys

Esitys sisältää merkityksellisiä ehdotuksia suhteessa perustuslain 10 §:ssä turvattuun yksityiselämän, henkilötietojen ja luottamuksellisen viestinnän suojaan, 15 §:ssä turvattuun omaisuudensuojaan, 18 §:ssä turvattuun elinkeinovapauteen, sekä 124 §:ssä hallintotehtävän antamisesta muulle kuin viranomaiselle säädettyyn. Lisäksi esitystä on arvioitu sen organisatorisen soveltamisalan osalta.

Julkinen hallintotehtävä

Esityksessä ehdotetaan säädettäväksi arviointitoiminnassa avustavasta tehtävästä arviointilain 4 a §:ssä ja Liikenne- ja viestintäviranomaisen tietoturvallisuuden arviointilaitosten hakemusten käsittelyssä avustavasta 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). Jos sellaista sääntelyn selkeyden vuoksi kuitenkin pidetään tarpeellisena, on viittauksen oltava vastakohtaispäätelmän vuoksi kattava (PeVL 42/2005 vp, s. 3). Arviointilaitoslain 13 §:n viittaus hallinnon yleislakeihin ehdotetaan säilytettävän ja täydennettävän siten, että listasta tulee kattava. Esityksessä täsmennetään myös, että arviointilaitoslain mukaiset tietoturvallisuuden arviointilaitosten tehtävät ovat julkisia hallintotehtäviä, joiden hoitamiseen sovelletaan hallinnon yleislakeja. Tarkoitus on tarkentaa voimassa olevan arviointilaitoslain säätämisen yhteydessä (HE 45/2011 vp s.10) omaksuttua käytännössä epäselväksi todettua lähtökohtaa siitä, että hallinnon yleislakien soveltamista ei olisi sidottu julkisen hallintotehtävien hoitamiseen, vaan niitä sovellettaisiin kaikkien arviointilaitoslain mukaisten tehtävien hoitamiseen.

Arviointilaitoslain ehdotetun 9 a §:n mukaan hyväksytty tietoturvallisuuden arviointilaitos voisi käyttää alihankkijaa sille kuuluvien tehtävien suorittamiseen. Yksityiselle siirretyn julkisen hallintotehtävän edelleen siirtämiseen (subdelegointiin) on perustuslakivaliokunnan käytännössä suhtauduttu lähtökohtaisesti kielteisesti. Ehdotonta kieltoa tällaiselle siirtämiselle ei kuitenkaan ole ollut osoitettavissa tilanteissa, joissa on kyse teknisluonteisesta tehtävästä ja joissa alihankkijaan kohdistuvat samat laatuvaatimukset ja vastaava valvonta kuin alkuperäiseen palveluntuottajaan (PeVL 26/2017 vp, s. 51, PeVL 6/2013 vp, s. 4). Ehdotetun sääntelyn mukaan hyväksytty tietoturvallisuuden arviointilaitos olisi velvollinen antamaan alihankinnasta selvityksen Liikenne- ja viestintävirastolle, joka valvoisi, että alihankkija täyttää soveltuvin osin laissa säädetyt arviointilaitoksen hyväksymisen edellytykset. Hyväksytty tietoturvallisuuden arviointilaitos olisi myös oikeudellisessa vastuussa alihankkijalla toteuttamastaan työstä ja sillä olisi kokonaisvastuu asiakkaaseen nähden. Alihankkijoiden käytön ei siten nähdä muodostavan ehdotetun lain yhteydessä perustuslain 124 §:n kannalta sellaista subdelegointia, että se olisi perustuslain kannalta ongelmallinen, koska kyse on teknisluonteisista tehtävistä ja alihankkijaa koskevat samat vaatimukset kuin hyväksyttyä tietoturvallisuuden arviointilaitostakin.

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 paljastuisi. Palveluntarjoajien on lisäksi mahdollista hakea tietoturvallisuuden arviointilaitoksiksi, jos ne haluaisivat arvioida turvallisuusluokkaan III luokiteltuja tietoja käsitteleviä tietojärjestelmiä ja tietoliikennejärjestelyjä. Ehdotuksen ei katsota olevan ongelmallinen elinkeinovapauden kannalta, koska palveluntarjoajan toteuttamien arviointien sallittavuudesta säädettäisiin tarkkarajaisesti lain tasolla ja tarkoituksena olisi suojata turvallisuusluokiteltua tietoa.

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. Ehdotuksen ei katsota olevan ongelmallinen elinkeinovapauden kannalta, koska tietoturvallisuuden arviointilaitoksen toteuttamien arviointien sallittavuudesta säädettäisiin tarkkarajaisesti lain tasolla ja tarkoituksena olisi suojata turvallisuusluokiteltua tietoa.

Tietoturvallisuuden arviointilaitosten hyväksymismenettelyn suhdetta perustuslain vaatimuksiin on kuvattu voimassa olevan arviointilaitoslain esitöissä (HE 45/2011 vp s. 13). Arviointilaitoslain 4 §:ään ehdotetaan lisättäväksi yritysturvallisuusselvityksen teettäminen osaksi arviointilaitoksen hyväksyntäprosessia, kun kyseessä on turvallisuusluokitellun tiedon käsittelyn arvioinnin pätevyysalue. Ehdotetun muutoksen ei arvioida vaikuttavan voimassa olevan arviointilaitoslain säätämisen yhteydessä esitettyyn elinkeinovapauteen liittyvään perustuslailliseen arvioon, koska arviointilaitosten hyväksymisprosessi pysyisi samana edellä esitettyä lisäystä 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 turvallisuuskriittisten 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. Ehdotuksen ei katsota olevan ongelmallinen elinkeinovapauden kannalta, koska laissa ei säädettäisi elinkeinotoiminnan harjoittamisen edellytyksistä ja hyväksymispäätöksen perumista edeltäisi päätöksen saaneen mahdollisuus korjata puute.

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 salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä. Arviointilaitoslain 7 §:ään ehdotetaan lisättävän Liikenne- ja viestintävirastolle tiedonsaantioikeudet suojelupoliisilta, kansalliselta akkreditointiyksiköltä tai pätevyysalueen arviointiperusteen soveltamista ohjaavalta tai valvovalta viranomaiselta, arviointilaitokselta sekä sen alihankkijalta ja asiakkaalta salassapitosäännösten tai muiden tiedon luovuttamista koskevien rajoitusten estämättä niistä tiedoista, jotka ovat välttämättömiä sen valvomiseksi, että tietoturvallisuuden arviointilaitos 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.

Henkilötietojen suoja

Perustuslakivaliokunta on korostanut, että siltä osin kuin Euroopan unionin lainsäädäntö edellyttää kansallista sääntelyä tai mahdollistaa sen, tätä kansallista liikkumavaraa käytettäessä otetaan huomioon perus- ja ihmisoikeuksista seuraavat vaatimukset (ks. esim. PeVL 1/ 2018 vp, PeVL 25/2005 vp). Perustuslakivaliokunta on painottanut, että hallituksen esityksessä on erityisesti perusoikeuksien kannalta merkityksellisen sääntelyn osalta syytä tehdä selkoa kansallisen liikkumavaran alasta (ks. esim. PeVL 17/2019 vp, s. 2–3, PeVL 29/2018 vp, s. 3, PeVL 26/2018 vp, s. 4, PeVL 14/2018 vp, s. 7, PeVL 1/2018 vp, s. 3, PeVL 26/2017 vp, s. 42, PeVL 2/2017 vp, s. 2, PeVL 44/2016 vp, s. 4).

Esitykseen sisältyvissä arviointilain 3, 7, 8 ja 9 §:n muutoksissa sekä uusissa 3 a–3 c §:ssä säädettäisiin viranomaisen tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden ja varautumisen arviointimenettelyistä, viranomaisten arviointivelvollisuuksista, vaatimusten täyttymisen osoittamisesta, arviointiperusteista, arviointiraportin, hyväksyntäpäätöksen ja -lausunnon antamisesta sekä tietoturvallisuuden ylläpidosta ja seurannasta. Sääntelyn tarkoituksena on varmistaa viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuutta. Sääntely vaikuttaa myös henkilötietojen käsittelyyn siltä osin kuin viranomaisen tietojärjestelmissä ja tietoliikennejärjestelyissä käsitellään henkilötietoja. Viranomaisten järjestelmissä tapahtuva henkilötietojen käsittely liittyy tietosuoja-asetuksen 6 artiklan 1 kohdan c ja e alakohdissa tarkoitettuihin perusteisiin. Näiden käsittelyn perustasta olisi säädetty joko tietosuojalaissa tai erityislaeissa. Tietosuoja-asetuksen 6 artiklan 3 kohta mahdollistaa kansallisen sääntelyn 1 kohdan c ja e alakohtien perusteella tapahtuvaan henkilötietojen käsittelyyn muun muassa laillisen ja asianmukaisen tietojenkäsittelyn varmistamiseen tarkoitetuista toimenpiteistä. Tietoturvallisuuden ja varautumisen arviointia koskevien säännösten voidaan katsoa olevan laillisen ja asianmukaisen tietojenkäsittelyn varmistamista koskevia toimenpiteitä henkilötietojen suojan toteuttamiseksi.

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 § 2 momenttiin lisättäisiin oikeus tehdä tarkastus hajasäteilysuojaratkaisun valmistajan ja sen alihankkijan tiloihin. Arviointilaitoslain 7 §:n 1 momentin Liikenne- ja viestintäviraston ja sitä avustavan asiantuntijan oikeutta tarkastaa hyväksyntää hakevan ja hyväksytyn tietoturvallisuuden arviointilaitoksen tilat ja menetelmät ulotettaisiin koskemaan myös arviointilaitoslain 9 a §:ssä tarkoitettua arviointilaitoksen alihankkijaa.

Säännökset ovat merkityksellisiä perustuslain 10 §:n 1 momentissa säädetyn kotirauhan näkökulmasta. Voimassa olevan arviointilain ja arviointilaitoslain säätämisen yhteydessä tarkastusoikeuksia 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 on nimenomaisesti rajattu tällaiset tilat tarkastusoikeuden ulkopuolelle (mm. PeVL 2/2002 vp, PeVL 18/2006 vp). Tätä rajausta ei ole tarkoitus arviointilain 6 §:n 1 momentin tai arviointilaitoslain 7 §:n 1 momentin tarkastusoikeuksien osalta muuttaa tämän esityksen yhteydessä. Tarkoitus on ulottaa rajoitus myös koskemaan esitettyä arviointilain 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 täsmällinen ja tarkkarajainen sekä riittävän oikeasuhtainen suhteessa niihin tavoitteisiin, joita esityksen taustalla on, sillä tarkastustoimenpiteiden suorittaminen on sidottu tarpeellisuusvaatimukseen, siitä säädetään laintasoisesti eikä sillä puututa omaisuudensuojan ydinalueelle.

Organisatorinen soveltaminen

Arviointilakiin ehdotettavat muutokset koskisivat ylimpiä laillisuusvalvojia, eduskunnan virastoja, tasavallan presidentin kansliaa sekä lainkäyttöä. Tämän vuoksi ehdotettavia muutoksia olisi tarpeen arvioida suhteessa perustuslaissa säädettyyn.

Arviointilain 3 a §:n 1 momentissa ehdotetaan säädettäväksi valtionhallinnon viranomaisille velvollisuus arvioida tietojärjestelmiensä ja tietoliikennejärjestelyjensä tietoturvallisuutta ja varautumista käyttäen 3 §:ssä tarkoitettuja menettelyjä. Arviointilain 3 a §:n 2 momentissa säädetään tarkemmin arviointimenettelyn valinnasta ja velvollisuudesta pyytää arviointiviranomaisen tai hankkia tietoturvallisuuden arviointilaitoksen arviointi tietojärjestelmälle tai tietoliikennejärjestelylle, jossa käsitellään turvallisuusluokkaan I-III luokiteltuja tietoja. Arviointilain 3 a §:n 3 momentin perusteella 2 momenttia ei sovellettaisi suojelupoliisin, eduskunnan oikeusasiamiehen eikä valtioneuvoston oikeuskanslerin toimintaan, tasavallan presidentin kansliaan eikä eduskunnan virastoihin.

Esityksessä on huomioitu ylimpien laillisuusvalvojien perustuslaissa säädetty asema sekä perustuslakivaliokunnan tätä asemaa koskeva kannanotto (PeVL 14/2018 vp). Ylimpiä laillisuusvalvojia koskisi ehdotettava 3 a §:n 1 momentin säännös velvollisuudesta arvioida tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuutta ja varautumista käyttäen 3 §:ssä tarkoitettuja menettelyjä, mutta ylimmät laillisuusvalvojat olisi rajattu ehdotettavan 2 momentin soveltamisalan ulkopuolelle. Näin ylimpiä laillisuusvalvojia ei koskisi arviointimenettelyn valintaa koskevat velvoitteet, eikä niitä velvoitettaisi pyytämään arviointia arviointiviranomaiselta tai hankkimaan arviointia tietoturvallisuuden arviointilaitokselta, vaan arviointimenettelyn valinta jätettäisiin niiden omaan harkintaan.

Vastaavasti kuin ylimpien laillisuusvalvojien osalta, arviointilain 3 a §:n 1 momentissa ehdotettava arviointivelvollisuus koskisi myös eduskunnan virastoja, mutta eduskunnan virastot olisi rajattu ehdotettavan 3 a §:n 2 momentin soveltamisalan ulkopuolelle. Sääntelyssä on tältä osin huomioitu perustuslakivaliokunnan kannanotto (PeVL 46/2010 vp).

Arviointilain 3 a §:n 2 momenttia ei myöskään sovellettaisi tuomioistuinten ja valitusasioita käsittelemään perustettujen lautakuntien toimintaan. Näin huomioitaisiin perustuslain 3 §:n 3 momentissa taattu tuomiovallan riippumattomuus ja perustuslakivaliokunnan kannanotot siitä, että valtion keskushallintoon kuuluvien viranomaisten ohjaustoimivaltaa ei tulisi ulottaa tuomioistuinten sisäisen hallinnon ohjaukseen tai lainkäyttöön (esim. PeVL 46/2010 vp ja PeVL 14/2018 vp). Sen sijaan ohjaustoimivaltaa voitaisiin käyttää niihin tietojärjestelmiin, joita tuomioistuimet käyttävät, koska järjestelmien tuottaminen kuuluu pääosin Oikeusrekisterikeskukselle sekä niiden kehittäminen ja ylläpitäminen Tuomioistuinvirastolle, joiden toimintaan ehdotettuja arviointivelvollisuuksia sovellettaisiin.

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 b §, sellaisena kuin se on laissa 728/2014,

muutetaan 1–8, 8 a ja 9–12 §, sellaisina kuin niistä ovat 1 § osaksi laissa 728/2014 ja 8 a § laissa 728/2014, sekä

lisätään lakiin uusi 3 a–3 d, 4 a, 4 b ja7 a § seuraavasti:

1 §

Lain soveltamisala

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

Tätä lakia sovelletaan kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa (588/2004) tarkoitetun kansainvälisen tietoturvallisuusvelvoitteen edellyttämään erityissuojattavan tietoaineiston käsittelyyn tarkoitetun tietojärjestelmän, tietoliikennejärjestelyn ja turvallisuuskriittisen ratkaisun ja sen valmistuksen tietoturvallisuuden arviointiin, jollei mainitussa laissa toisin säädetä tai mainitussa laissa tarkoitetusta kansainvälisestä tietoturvallisuusvelvoitteesta muuta johdu.

Liikenne- ja viestintäviraston tehtävistä yritysturvallisuusselvitystä laadittaessa säädetään turvallisuusselvityslaissa (726/2014) ja tehtävistä kansainvälisten tietoturvallisuusvelvoitteiden tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuutta koskevissa asioissa kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa.

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 mainitun lain mukaisesti hyväksynyt;

8) *turvallisuusluokalla*, julkisen hallinnon tiedonhallinnasta annetun lain (906/2019) 18 §:n 1 momentissa ja mainitun pykälän 4 momentin nojalla annetussa valtioneuvoston asetuksessa tarkoitettuja turvallisuusluokkia;

9) *turvallisuuskriittisellä ratkaisulla* salaus-, hajasäteilysuojaus- ja muuta tieto- ja viestintäteknistä ratkaisua, tuotetta, toteutusta tai palvelua, 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 arviointimenettelyt

Tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden ja varautumisen arviointimenettelyjä ovat:

1) viranomaisen toteuttama itsearviointi;

2) palveluntarjoajan viranomaisen toimeksiannosta toteuttama arviointi;

3) tietoturvallisuuden arviointilaitoksen toteuttama arviointi; sekä

4) 3 d §:ssä tarkoitetun arviointiviranomaisen toteuttama arviointi.

Viranomainen voi toteuttaa arvioinnin 1 momentin 2 kohdan mukaisella menettelyllä vain, jos arvioinnin kohteena olevalla tietojärjestelmällä tai tietoliikennejärjestelyllä käsitellään julkisia, salassa pidettäviä tai korkeintaan turvallisuusluokkaan IV luokiteltuja tietoja. Viranomaisen on tällöin ennakolta varmistuttava palveluntarjoajan luotettavuudesta toimeksiannon edellyttämässä laajuudessa.

Viranomainen voi toteuttaa arvioinnin 1 momentin 3 kohdan mukaisella menettelyllä vain, jos arvioinnin kohteena olevalla tietojärjestelmällä tai tietoliikennejärjestelyllä käsitellään korkeintaan turvallisuusluokkaan III luokiteltuja tietoja.

3 a §

Valtionhallinnon viranomaisen arviointivelvollisuudet

Valtionhallinnon viranomaisen on arvioitava tietojärjestelmiensä ja tietoliikennejärjestelyjensä tietoturvallisuutta ja varautumista käyttäen 3 §:n 1 momentissa tarkoitettuja menettelyjä.

Valtionhallinnon viranomaisen on valittava arviointimenettely tietojärjestelmän tai tietoliikennejärjestelyn riskiarvioinnin perusteella, kuitenkin siten, että sen on:

1) pyydettävä arviointiviranomaisen arviointi tietojärjestelmälleen tai tietoliikennejärjestelylleen, jossa käsitellään turvallisuusluokkaan I tai II luokiteltuja tietoja;

2) pyydettävä arviointiviranomaisen tai hankittava tietoturvallisuuden arviointilaitoksen arviointi tietojärjestelmälleen tai tietoliikennejärjestelylleen, jossa käsitellään turvallisuusluokkaan III luokiteltuja tietoja, jollei se päätä arvioinnin pyytämisen tai hankkimisen olevan tietojärjestelmän tai tietoliikennejärjestelyn riskiarvioinnin perusteella tarpeetonta; ja

3) toteutettava aina vähintään itsearviointi.

Mitä 2 momentissa säädetään, ei sovelleta suojelupoliisin, eduskunnan oikeusasiamiehen eikä valtioneuvoston oikeuskanslerin toimintaan, tuomioistuimiin, valitusasioita käsittelemään perustettuihin lautakuntiin, tasavallan presidentin kansliaan eikä eduskunnan virastoihin.

3 b §

Muun kuin valtionhallinnon viranomaisen arviointivelvollisuudet

Muun kuin 3 a §:ssä tarkoitetun viranomaisen on arvioitava tietojärjestelmänsä tai tietoliikennejärjestelynsä, jossa käsitellään turvallisuusluokkaan I tai II luokiteltuja tietoja 3 a §:n 2 momentin 1 kohdassa tarkoitetulla tavalla.

Muun kuin 3 a §:ssä tarkoitetun viranomaisen on arvioitava tietojärjestelmänsä tai tietoliikennejärjestelynsä, jossa käsitellään turvallisuusluokkaan III luokiteltuja tietoja 3 a §:n 2 momentin 2 kohdassa tarkoitetulla tavalla, jollei se päätä arvioinnin pyytämisen tai hankkimisen olevan tietojärjestelmän tai tietoliikennejärjestelyn riskiarvioinnin perusteella tarpeetonta, jolloin sen on toteutettava itsearviointi.

3 c §

Vaatimusten täyttymisen osoittaminen

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

1) kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa tarkoitetussa tilanteessa tai mainitussa laissa tarkoitetussa kansainvälisessä tietoturvallisuusvelvoitteessa tarkoitetussa tilanteessa;

2) jos muu kuin 1 kohdassa tarkoitettu kansainvälinen yhteistyö sitä edellyttää; tai

3) jos vaatimustenmukaisuuden osoittamisesta erikseen säädetään.

3 d §

Arviointiviranomaiset

Toimivaltainen arviointiviranomainen on Liikenne- ja viestintävirasto. Jos arviointi koskee Puolustusvoimien tietojärjestelmien tai tietoliikennejärjestelyjen taikka niihin kuuluvien turvallisuuskriittisten ratkaisujen tietoturvallisuutta ja varautumista, toimivaltainen arviointiviranomainen on kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 4 §:n 1 momentissa tarkoitettu Pääesikunnan määrätty turvallisuusviranomainen.

Pääesikunnan määrätyn turvallisuusviranomaisen arviointitehtäviä voi myös hoitaa Puolustusvoimien palkattuun henkilöstöön kuuluva henkilö, jonka Pääesikunnan määrätty turvallisuusviranomainen on tähän tehtävään nimennyt ja jonka toimintaa se ohjaa ja valvoo.

Arviointiviranomaisen on organisaatioltaan ja päätöksenteoltaan oltava riippumaton arviointitehtävien hoitamisessa. Lisäksi arviointiviranomaisen on varmistettava, että sen palveluksessa olevilla tai lukuun toimivilla henkilöillä on arviointitehtävän laatuun ja laajuuteen nähden riittävä koulutus ja kokemus.

4 §

Arviointiviranomaisen tehtävät

Arviointiviranomaisen tehtävänä on arvioida viranomaisen pyynnöstä tietojärjestelmän tai tietoliikennejärjestelyn taikka niihin kuuluvan turvallisuuskriittisen ratkaisun tietoturvallisuutta ja varautumista.

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

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

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

3) ohjata ja valvoa 8 §:n 3 momentissa tarkoitetun hyväksyntäpäätöksen saaneen hajasäteilysuojausratkaisuja valmistavan turvallisuuskriittisen ratkaisun valmistajan toimintaa ja antaa tarvittaessa päätös valmistuksen toimenpiteiden tai ratkaisun vaatimuksista.

Liikenne- ja viestintävirasto asettaa tässä laissa sille säädetyt arviointiviranomaisen tehtävät tärkeysjärjestykseen ja suorittaa tehtävät käytettävissään olevien voimavarojen mukaisesti. Liikenne- ja viestintävirasto voi päätöksellään jättää siltä pyydetyn arvioinnin tekemättä tai ottaa arvioinnin suoritettavakseen vain osittain. Tehtävien tärkeysjärjestyksessä ja päätöksessä on otettava huomioon:

1) kansainvälisten tietoturvallisuusvelvoitteiden noudattaminen;

2) 3 a ja 3 b §:ssä tarkoitetut viranomaisten arviointivelvollisuudet;

3) tiedon turvallisuusluokka;

4) muun riippumattoman arvioinnin kuin Liikenne- ja viestintäviraston toteuttaman arvioinnin saatavuus;

5) suomalaisten turvallisuuskriittisten ratkaisujen tarjonnan edistäminen;

6) arvioinnin pyytäjien ja hakijoiden yhdenvertainen kohtelu; sekä

7) pyydettyjen toimenpiteiden yleinen merkitys viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden yleiseen parantamiseen taikka yhteiskunnan elintärkeiden toimintojen suojaamiseen.

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

4 a §

Arviointiviranomaista avustava tehtävä

Arviointiviranomainen voi käyttää arvioinnissa apuna ulkopuolista asiantuntijaa, jos se on arvioinnin laadun, käytettävissä olevien voimavarojen tai arviointiin liittyvien teknisten syiden vuoksi tarpeellista. Ulkopuolisella asiantuntijalla on oltava arviointitehtävän laatuun ja laajuuteen nähden riittävä koulutus ja kokemus. 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 ulkopuolisesta asiantuntijasta.

4 b §

Arviointiviranomaisten tiedonvaihto ja yhteistyö

Arviointiviranomaisten on toimittava yhteistyössä tämän lain mukaisten tehtävien hoitamiseksi ja annettava salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä toisilleen tässä tarkoituksessa välttämättömät tiedot.

Sen estämättä, mitä 3 d §:n 1 momentissa ja 4 §:n 1 ja 2 momentissa säädetään, arviointiviranomaiset voivat sopia tietyn tässä laissa säädetyn tehtävän tai sen osan hoitamisesta toisen arviointiviranomaisen lukuun, jos järjestely on tarpeen tehtävien hoitamiseksi tarkoituksenmukaisesti, taloudellisesti ja joutuisasti.

Liikenne- ja viestintävirasto vastaa arviointiviranomaisten yhteistyön ohjaamisesta 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 ja muiden tietojen luovuttamista koskevien rajoitusten estämättä sisällyttää valtiovarainministeriölle antamaansa selvitykseen sellaisia tietoja, jotka ovat välttämättömiä selvityksen tarkoituksen toteuttamiseksi.

6 §

Arviointiviranomaisen tiedonsaantioikeus, tarkastusoikeus sekä oikeus päästä tiloihin ja tietojärjestelmiin

Arviointiviranomaisella ja 4 a §:ssä tarkoitetulla sitä avustavalla ulkopuolisella asiantuntijalla on oikeus salassapitosäännösten tai muiden tiedon luovuttamista koskevien rajoitusten estämättä saada käyttöönsä tässä laissa säädettyjen 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 on oikeus tehdä hajasäteilysuojausratkaisun valmistajan ja sen alihankkijan tiloissa tarkastus sen selvittämiseksi, noudattavatko valmistaja ja sen alihankkija tämän lain nojalla annettuja päätöksiä. Pääesikunnan määrätyllä turvallisuusviranomaisella on oikeus tehdä edellä tarkoitettu tarkastus, jos se hoitaa tehtävää 4 b §:n 2 momentissa tarkoitetulla tavalla Liikenne- ja viestintäviraston lukuun. Tarkastuksen suorittamisessa Liikenne- ja viestintävirastoa ja Pääesikunnan määrättyä turvallisuusviranomaista voi avustaa 4 a §:ssä tarkoitettu avustava ulkopuolinen asiantuntija. Liikenne- ja viestintäviraston, Pääesikunnan määrätyn turvallisuusviranomaisen ja avustavan ulkopuolisen asiantuntijan oikeuteen päästä tiloihin ja saada tutkittavakseen välttämättömät tiedot sekä suorittaa arviointitoimenpiteitä sovelletaan, mitä 1 momentissa säädetään. Tarkastuksessa on noudatettava, mitä hallintolain (434/2003) 39 §:ssä säädetään.

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 sekä turvallisuuskriittisten ratkaisujen ja niiden valmistuksen tietoturvallisuuden arviointiperusteina voidaan käyttää:

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

2) Euroopan unionin, Pohjois-Atlantin liiton tai muun kansainvälisen toimielimen antamia tietoturvallisuutta, kyberturvallisuutta tai varautumista koskevia säännöksiä, määräyksiä ja ohjeita sekä viranomaisten ohjeita niiden soveltamisesta;

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.

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

Arviointiviranomainen asettaa turvallisuuskriittisten ratkaisujen arviointiperusteet turvallisuuskriittisen ratkaisun valmistajaa kuultuaan. Sen lisäksi, mitä 1 ja 2 momentissa säädetään, turvallisuuskriittisten ratkaisujen arviointiperusteiden määrittelyssä tulee ottaa huomioon tiedon 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 ja sen valmistuksen arvioinnissa hakea turvallisuusselvityslaissa tarkoitettu yritysturvallisuusselvitys arviointia hakevasta valmistajasta. Turvallisuuskriittisen ratkaisun hyväksyntä edellyttää, että valmistajan yritysturvallisuusselvityksessä ei ole ilmennyt mitään, mikä kokonaisharkinnan perusteella vaarantaisi valmistuksen turvallisuuden ja luotettavuuden ottaen huomioon erityisesti 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 c §:ssä tarkoitetusta pyynnöstä viranomaisen tietojärjestelmän tai tietoliikennejärjestelyn hyväksyntäpäätöksen tai -lausunnon, jos tietojärjestelmä tai tietoliikennejärjestely täyttää vaatimukset. Päätökseen tai

lausuntoon on merkittävä tiedot arvioinnin kohteesta, käytetyistä 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 tietoturvallisuuden arvioinnista päätös, josta ilmenee arvioinnin tulos. Hyväksyntäpäätöksestä tulee ilmetä hyväksynnän voimassaolo, ja siihen 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 varmistamiseksi.

8 a §

Hyväksyttyjen turvallisuuskriittisten ratkaisujen ja valmistajien luettelo

Liikenne- ja viestintävirasto ylläpitää julkista luetteloa 8 §:n 3 momentin mukaisesti hyväksyntäpäätöksen saaneista turvallisuuskriittisistä ratkaisuista ja turvallisuuskriittisten ratkaisujen valmistajista. Luettelosta tulee käydä ilmi:

1) turvallisuuskriittisen ratkaisun nimi, käyttötarkoitus ja versio;
2) tiedon turvallisuusluokka, jonka suojaamiseen ratkaisu on todettu riittäväksi;
3) turvallisuuskriittisen ratkaisun valmistaja;
4) hyväksynnän voimassaolo, muutos tai lakkaaminen; sekä
5) hyväksyntään liittyvät turvallisen käytön ehdot ja rajoitukset.

9 §

Tietoturvallisuuden ylläpito ja seuranta

Edellä 8 §:ssä tarkoitetun päätöksen tai lausunnon saaneen 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 peruuttamisen tekemistä kuultava päätöksen tai lausunnon saanutta sekä varattava tälle tilaisuus korjata puute.

Arviointiviranomainen voi 1 momentissa tarkoitetussa peruuttamista koskevassa 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 sekä arviointiraportin, lausunnon tai päätöksen antamisesta, neuvonnasta ja selvityksestä peritään asian vireille saattajalta maksu noudattaen, mitä valtion maksuperustelaissa (150/1992) säädetään.

_____

Tämä laki tulee voimaan päivänä kuuta 2026.

Valtionhallinnon viranomaisen on saatettava tietojärjestelmiensä ja tietoliikennejärjestelyjensä tietoturvallisuuden ja varautumisen arviointi vastaamaan 3 a §:ssä säädettyä viiden vuoden kuluessa tämän lain voimaatulosta, kuitenkin siten, että arviointi on saatettava vastaamaan mainitun pykälän 2 momentin 1 kohdassa säädettyä kahden vuoden kuluessa lain voimaantulosta ja 2 kohdassa säädettyä kolmen vuoden kuluessa lain voimaantulosta.

Muiden kuin valtionhallinnon viranomaisten on saatettava tietojärjestelmiensä ja tietoliikennejärjestelyjensä tietoturvallisuuden ja varautumisen arviointi vastaamaan 3 b §:n 1 momentissa säädettyä kahden vuoden kuluessa lain voimaantulosta ja mainitun pykälän 2 momentissa säädettyä kolmen vuoden kuluessa lain voimaantulosta.

Tietoturvallisuuden vaatimustenmukaisuudesta annettu todistus, joka on annettu tämän lain voimaan tullessa voimassa olleiden säännösten mukaisesti, vastaa 8 §:ssä tarkoitettua päätöstä, ja on voimassa todistukseen merkityn ajan.

_____

2.

Laki

tietoturvallisuuden arviointilaitoksista annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti

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

lisätään lakiin uusi 9 a § seuraavasti:

1 luku

Yleiset säännökset

1 §

Lain tarkoitus

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

2 §

Lain soveltamisala

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

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

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 turvallisuusselvityslaissa (726/2014) tarkoitettu yritysturvallisuusselvitys. Suojelupoliisi noudattaa lausuntoa tai selvitystä laatiessaan, mitä turvallisuusselvityslaissa säädetään.

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:

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 4) laitoksen yritysturvallisuusselvityksessä ei ole ilmennyt sellaista seikkaa, joka 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;

5) laitoksella on asianmukaiset ohjeet toimintaansa ja sen seurantaa varten.

Edellä 1 momentin 1–3 kohdassa tarkoitettujen vaatimusten täyttäminen on osoitettava vaatimustenmukaisuuden arviointipalvelujen pätevyyden toteamisesta annetussa laissa (920/2005) säädetyn menettelyn avulla.

Sen estämättä, mitä 2 momentissa säädetään, hyväksytyn arviointilaitoksen hakiessa hyväksymistä 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 hyväksyntää.

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 on oikeus tarkastaa hyväksymistä hakevan ja hyväksytyn tietoturvallisuuden arviointilaitoksen ja sen 9 a §:ssä tarkoitetun alihankkijan tilat sekä sen käytössä olevat menetelmät. Tarkastuksen suorittamisessa Liikenne- ja viestintävirastoa voi avustaa 4 §:n 2 momentissa tarkoitettu ulkopuolinen asiantuntija. Tarkastusta ei saa suorittaa pysyväisluonteiseen asumiseen käytetyissä tiloissa.

Liikenne- ja viestintävirastolla on oikeus salassapitosäännösten tai muiden tiedon luovuttamista koskevien rajoitusten estämättä saada pyynnöstä suojelupoliisilta, kansalliselta akkreditointiyksiköltä, pätevyysalueen arviointiperusteen soveltamista ohjaavalta tai valvovalta viranomaiselta, arviointilaitokselta sekä sen alihankkijalta ja asiakkaalta ne tiedot, jotka ovat välttämättömiä sen valvomiseksi, että tietoturvallisuuden arviointilaitos 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 arvioinnin kohteesta, 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 tietoturvallisuuden ja varautumisen 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 samaan konserniin kuuluvalla yhtiöllä tai muuna alihankintana vain, jos konserniyhtiö tai muu alihankkija täyttää tietoturvallisuuden arviointilaitoksen hyväksymisen edellytykset ja alihankinnasta on annettu selvitys Liikenne- ja viestintävirastolle ja Liikenne- ja viestintävirasto on todennut edellytysten täyttymisen.

Hyväksytty tietoturvallisuuden arviointilaitos voi teettää alihankintana tai tytäryhtiöllään 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, määräyksiä ja ohjeita sekä viranomaisten ohjeita niiden soveltamisesta;

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.

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 julkisia hallintotehtäviä 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).

Hyväksytyn tietoturvallisuuden arviointilaitosten vastuuhenkilöön ja palveluksessa olevaan henkilöön sekä 9 a §:ssä tarkoitettujen alihankkijoiden palveluksessa olevaan henkilöön sovelletaan rikosoikeudellista virkavastuuta koskevia säännöksiä hänen suorittaessaan tässä laissa tarkoitettuja tehtäviä. Vahingonkorvausvastuusta säädetään vahingonkorvauslaissa.

13 a §

Turvallisuusselvitysrekisteriin merkittävät tiedot

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

Hyväksytty tietoturvallisuuden 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 päivänä kuuta 2026.

Liikenne- ja viestintäviraston tulee kahden vuoden kuluessa tämän lain voimaantulosta hakea 4 §:n mukaisesti yritysturvallisuusselvitys hyväksytystä tietoturvallisuuden arviointilaitoksesta, jolle on tämän lain voimaan tullessa voimassa olleiden säännösten mukaisesti hyväksytty pätevyysalue turvallisuusluokitellun tiedon käsittelyn arviointiin.

3.

Laki

turvallisuusselvityslain 18 ja 48 § muuttamisesta

Eduskunnan päätöksen mukaisesti

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

muutetaan 18 §:n 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 2026.

_____

Helsingissä 7.5.2026

Pääministeri

Petteri Orpo

Kunta- ja alueministeri Anna-Kaisa Ikonen

Liite
Rinnakkaistekstit

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 b §, sellaisena kuin se on laissa 728/2014,

muutetaan 1–8, 8 a ja 9–12 §, sellaisina kuin niistä ovat 1 § osaksi laissa 728/2014 ja 8 a § laissa 728/2014, sekä

lisätään lakiin uusi 3 a–3 d, 4 a, 4 b ja7 a § seuraavasti:

Voimassa oleva laki	*Ehdotus*
1 §	1 §
Lain soveltamisala	*Lain soveltamisala*
Tässä laissa säädetään viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista. Viestintäviraston tehtävistä yritysturvallisuusselvitystä laadittaessa säädetään turvallisuusselvityslaissa (726/2014) .	Tässä laissa säädetään viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden *ja varautumisen* arvioinnista. *Lisäksi tässä laissa säädetään turvallisuuskriittisten ratkaisujen ja niiden valmistuksen tietoturvallisuuden arvioinnista.* *Tätä lakia sovelletaan kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa (588/2004) tarkoitetun kansainvälisen tietoturvallisuusvelvoitteen edellyttämään erityissuojattavan tietoaineiston käsittelyyn tarkoitetun tietojärjestelmän, tietoliikennejärjestelyn ja turvallisuuskriittisen ratkaisun ja sen valmistuksen tietoturvallisuuden arviointiin, jollei mainitussa laissa toisin säädetä tai mainitussa laissa tarkoitetusta kansainvälisestä tietoturvallisuusvelvoitteesta muuta johdu.* *Liikenne- ja viestintäviraston* tehtävistä yritysturvallisuusselvitystä laadittaessa säädetään turvallisuusselvityslaissa (726/2014) *ja tehtävistä kansainvälisten tietoturvallisuusvelvoitteiden tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuutta koskevissa asioissa*

Voimassa oleva laki

2 §

Määritelmät

Tässä laissa tarkoitetaan:

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

2)*tietoliikennejärjestelyllä* tiedonsiirtoverkosta, tiedonsiirtolaitteista, ohjelmistoista ja muista tietojenkäsittelystä koostuvista järjestelyistä muodostuvaa järjestelmää;

3)*viranomaisella* viranomaisten toiminnan julkisuudesta annetun lain (621/1999) 4 §:n 1 momentin 1–7 kohdassa tarkoitettuja toimielimiä;

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

Ehdotus

kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa.

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 mainitun lain mukaisesti hyväksynyt;

8) turvallisuusluokalla, julkisen hallinnon tiedonhallinnasta annetun lain (906/2019) 18 §:n 1 momentissa ja mainitun pykälän 4 momentin nojalla annetussa valtioneuvoston asetuksessa tarkoitettuja turvallisuusluokkia;

9) turvallisuuskriittisellä ratkaisulla salaus-, hajasäteilysuojaus- ja muuta tieto- ja viestintäteknistä ratkaisua, tuotetta, toteutusta tai palvelua, jolla suojataan turvallisuusluokiteltua tietoa

Voimassa oleva laki

Ehdotus

tietojärjestelmissä ja tietoliikennejärjestelyissä;

10) turvallisuuskriittisen ratkaisun valmistajalla yritystä, joka vastaa turvallisuuskriittisen ratkaisun kehittämisestä, suunnittelusta, valmistamisesta, kokoamisesta ja ylläpidosta.

3 §

Tietoturvallisuuden arviointipalvelujen käyttäminen

Valtionhallinnon viranomaiset saavat käyttää tietojärjestelmiensä ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnissa vain tässä laissa tarkoitettua menettelyä taikka sellaista arviointilaitosta, joka on saanut Viestintäviraston hyväksynnän tietoturvallisuuden arviointilaitoksista annetun lain (1405/2011) mukaan.

3 §

*Tietoturvallisuuden **ja varautumisen arviointimenettelyt***

Tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden ja varautumisen arviointimenettelyjä ovat:

1) viranomaisen toteuttama itsearviointi;

2) palveluntarjoajan viranomaisen toimeksiannosta toteuttama arviointi;

3) tietoturvallisuuden arviointilaitoksen toteuttama arviointi; sekä

4) 3 d §:ssä tarkoitetun arviointiviranomaisen toteuttama arviointi.

Viranomainen voi toteuttaa arvioinnin 1 momentin 2 kohdan mukaisella menettelyllä vain, jos arvioinnin kohteena olevalla tietojärjestelmällä tai tietoliikennejärjestelyllä käsitellään julkisia, salassa pidettäviä tai korkeintaan turvallisuusluokkaan IV luokiteltuja tietoja. Viranomaisen on tällöin ennakolta varmistuttava palveluntarjoajan luotettavuudesta toimeksiannon edellyttämässä laajuudessa.

Viranomainen voi toteuttaa arvioinnin 1 momentin 3 kohdan mukaisella menettelyllä vain, jos arvioinnin kohteena olevalla tietojärjestelmällä tai tietoliikennejärjestelyllä käsitellään korkeintaan turvallisuusluokkaan III luokiteltuja tietoja.

3 a §

Valtionhallinnon viranomaisen arviointivelvollisuudet

Valtionhallinnon viranomaisen on arvioitava tietojärjestelmiensä ja tietoliikennejärjestelyjensä tietoturvallisuutta ja varautumista käyttäen 3 §: n 1 momentissa tarkoitettuja menettelyjä.

Voimassa oleva laki

Ehdotus

Valtionhallinnon viranomaisen on valittava arviointimenettely tietojärjestelmän tai tietoliikennejärjestelyn riskiarvioinnin perusteella, kuitenkin siten, että sen on:

1) pyydettävä arviointiviranomaisen arviointi tietojärjestelmälleen tai tietoliikennejärjestelylleen, jossa käsitellään turvallisuusluokkaan I tai II luokiteltuja tietoja;

2) pyydettävä arviointiviranomaisen tai hankittava tietoturvallisuuden arviointilaitoksen arviointi tietojärjestelmälleen tai tietoliikennejärjestelylleen, jossa käsitellään turvallisuusluokkaan III luokiteltuja tietoja, jollei se päätä arvioinnin pyytämisen tai hankkimisen olevan tietojärjestelmän tai tietoliikennejärjestelyn riskiarvioinnin perusteella tarpeetonta; ja

3) toteutettava aina vähintään itsearviointi.

Mitä 2 momentissa säädetään, ei sovelleta suojelupoliisin, eduskunnan oikeusasiamiehen eikä valtioneuvoston oikeuskanslerin toimintaan, tuomioistuimiin, valitusasioita käsittelemään perustettuihin lautakuntiin, tasavallan presidentin kansliaan eikä eduskunnan virastoihin.

3 b §

Muun kuin valtionhallinnon viranomaisen arviointivelvollisuudet

Muun kuin 3 a §:ssä tarkoitetun viranomaisen on arvioitava tietojärjestelmänsä tai tietoliikennejärjestelynsä, jossa käsitellään turvallisuusluokkaan I tai II luokiteltuja tietoja 3 a §:n 2 momentin 1 kohdassa tarkoitetulla tavalla.

Muun kuin 3 a §:ssä tarkoitetun viranomaisen on arvioitava tietojärjestelmänsä tai tietoliikennejärjestelynsä, jossa käsitellään turvallisuusluokkaan III luokiteltuja tietoja 3 a §:n 2 momentin 2 kohdassa tarkoitetulla tavalla, jollei se päätä arvioinnin pyytämisen tai hankkimisen olevan tietojärjestelmän tai tietoliikennejärjestelyn riskiarvioinnin perusteella tarpeetonta, jolloin sen on toteutettava itsearviointi.

Voimassa oleva laki

Ehdotus

3 c §

Vaatimusten täyttymisen osoittaminen

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

1) kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa tarkoitetussa tilanteessa tai mainitussa laissa tarkoitetussa kansainvälisessä tietoturvallisuusvelvoitteessa tarkoitetussa tilanteessa;

2) jos muu kuin 1 kohdassa tarkoitettu kansainvälinen yhteistyö sitä edellyttää; tai

3) jos vaatimustenmukaisuuden osoittamisesta erikseen säädetään.

3 d §

Arviointiviranomaiset

Toimivaltainen arviointiviranomainen on Liikenne- ja viestintävirasto. Jos arviointi koskee Puolustusvoimien tietojärjestelmien tai tietoliikennejärjestelyjen taikka niihin kuuluvien turvallisuuskriittisten ratkaisujen tietoturvallisuutta ja varautumista, toimivaltainen arviointiviranomainen on kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 4 §:n 1 momentissa tarkoitettu Pääesikunnan määrätty turvallisuusviranomainen.

Pääesikunnan määrätyn turvallisuusviranomaisen arviointitehtäviä voi myös hoitaa Puolustusvoimien palkattuun henkilöstöön kuuluva henkilö, jonka Pääesikunnan määrätty turvallisuusviranomainen on tähän tehtävään nimennyt ja jonka toimintaa se ohjaa ja valvoo.

Arviointiviranomaisen on organisaatioltaan ja päätöksenteoltaan oltava riippumaton arviointitehtävien hoitamisessa. Lisäksi arviointiviranomaisen on varmistettava, että sen palveluksessa olevilla tai lukuun toimivilla henkilöillä on arviointitehtävän laatuun ja laajuuteen nähden riittävä koulutus ja kokemus.

Voimassa oleva laki

4 §

Viestintäviraston tehtävät

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

1)arvioida viranomaisen pyynnöstä tämän määräämisvallassa olevan tai hankittavaksi suunnitteleman tietojärjestelmän tai tietoliikennejärjestelyjen tietoturvallisuuden vaatimuksenmukaisuutta;

2)antaa tietojärjestelmälle tai tietoliikennejärjestelylle sen hyväksymistä osoittava todistus 8 §:ssä säädetyllä tavalla;

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

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

Viestintävirasto suorittaa tässä laissa tarkoitetut tehtävät käytettävissään olevien voimavarojen mukaisesti ottaen huomioon kansainvälisten tietoturvallisuusvelvoitteiden noudattaminen sekä pyydettyjen toimenpiteiden merkitys viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden yleiseen parantamiseen.

Ehdotus

4 §

***Arviointiviranomaisen** tehtävät*

Arviointiviranomaisen tehtävänä on arvioida viranomaisen pyynnöstä tietojärjestelmän tai tietoliikennejärjestelyn taikka niihin kuuluvan turvallisuuskriittisen ratkaisun tietoturvallisuutta ja varautumista.

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

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

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

3) ohjata ja valvoa 8 §:n 3 momentissa tarkoitetun hyväksyntäpäätöksen saaneen hajasäteilysuojausratkaisuja valmistavan turvallisuuskriittisen ratkaisun valmistajan toimintaa ja antaa tarvittaessa päätös valmistuksen toimenpiteiden tai ratkaisun vaatimuksista.

Liikenne- ja viestintävirasto asettaa tässä laissa sille säädetyt arviointiviranomaisen tehtävät tärkeysjärjestykseen ja suorittaa tehtävät käytettävissään olevien voimavarojen mukaisesti. Liikenne- ja viestintävirasto voi päätöksellään jättää siltä pyydetyn arvioinnin tekemättä tai ottaa arvioinnin suoritettavakseen vain osittain. Tehtävien tärkeysjärjestyksessä ja päätöksessä on otettava huomioon:

1) kansainvälisten tietoturvallisuusvelvoitteiden noudattaminen;

2) 3 a ja 3 b §:ssä tarkoitetut viranomaisten arviointivelvollisuudet;

3) tiedon turvallisuusluokka;

4) muun riippumattoman arvioinnin kuin Liikenne- ja viestintäviraston toteuttaman arvioinnin saatavuus;

5) suomalaisten turvallisuuskriittisten ratkaisujen tarjonnan edistäminen;

Voimassa oleva laki | *Ehdotus*

6) arvioinnin pyytäjien ja hakijoiden yhdenvertainen kohtelu; sekä

7) pyydettyjen toimenpiteiden yleinen merkitys viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden yleiseen parantamiseen taikka yhteiskunnan elintärkeiden toimintojen suojaamiseen.

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

4 a §

Arviointiviranomaista avustava tehtävä

Arviointiviranomainen voi käyttää arvioinnissa apuna ulkopuolista asiantuntijaa, jos se on arvioinnin laadun, käytettävissä olevien voimavarojen tai arviointiin liittyvien teknisten syiden vuoksi tarpeellista. Ulkopuolisella asiantuntijalla on oltava arviointitehtävän laatuun ja laajuuteen nähden riittävä koulutus ja kokemus. 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 ulkopuolisesta asiantuntijasta.

4 b §

Arviointiviranomaisten tiedonvaihto ja yhteistyö

Arviointiviranomaisten on toimittava yhteistyössä tämän lain mukaisten tehtävien hoitamiseksi ja annettava salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä

Voimassa oleva laki	*Ehdotus*
	toisilleen tässä tarkoituksessa välttämättömät tiedot. *Sen estämättä, mitä 3 d §:n 1 momentissa ja 4 §:n 1 ja 2 momentissa säädetään, arviointiviranomaiset voivat sopia tietyn tässä laissa säädetyn tehtävän tai sen osan hoitamisesta toisen arviointiviranomaisen lukuun, jos järjestely on tarpeen tehtävien hoitamiseksi tarkoituksenmukaisesti, taloudellisesti ja joutuisasti.* *Liikenne- ja viestintävirasto vastaa arviointiviranomaisten yhteistyön ohjaamisesta yhtenäisen soveltamiskäytännön luomiseksi.*
5 §	5 §
Selvitykset valtiovarainministeriön toimeksiannosta	*Selvitykset valtiovarainministeriön toimeksiannosta*
Valtiovarainministeriö voi pyytää valtionhallinnon tietoturvallisuudesta annettujen säännösten täytäntöönpanon seuraamiseksi sekä niiden kehittämiseksi Viestintävirastoa laatimaan selvityksen valtionhallinnon viranomaisten tietojärjestelmien tai tietoliikennejärjestelyjen yleisestä tietoturvallisuuden tasosta. Selvityksen piiriin tulevat tietojärjestelmät voidaan määritellä tietojärjestelmien käyttötarkoituksen, niihin talletettavien tietojen laadun tai muun vastaavan yleisen tekijän mukaan. Viestintävirasto voi salassapitosäännösten estämättä sisällyttää valtiovarainministeriölle antamaansa arvioon sellaisia tietoja, jotka ovat välttämättömiä arvioinnin tarkoituksen toteuttamiseksi.	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 *ja muiden tietojen luovuttamista koskevien rajoitusten* estämättä sisällyttää valtiovarainministeriölle antamaansa selvitykseen sellaisia tietoja, jotka ovat välttämättömiä selvityksen tarkoituksen toteuttamiseksi.
6 §	6 §
Viestintäviraston tiedonsaantioikeus ja oikeus päästä tiloihin ja tietojärjestelmiin	*Arviointiviranomaisen tiedonsaantioikeus, tarkastusoikeus sekä oikeus päästä tiloihin ja tietojärjestelmiin*
Viestintävirastolla ja sen toimeksiannosta toimivalla asiantuntijalla on oikeus sen estämättä, mitä tietojen salassapidosta säädetään, saada käyttöönsä Viestintäviraston arvioitavana tai selvityksen kohteena olevaa	*Arviointiviranomaisella ja 4 a §:ssä tarkoitetulla sitä avustavalla ulkopuolisella asiantuntijalla on oikeus salassapitosäännösten tai muiden tiedon luovuttamista koskevien rajoitusten estämättä*

Voimassa oleva laki	*Ehdotus*
tietojärjestelmää tai tietoliikennejärjestelyjä koskevat tiedot sekä oikeus siinä laajuudessa kuin se on tarpeen arvioinnin suorittamiseksi päästä tietojärjestelmään tai tiloihin, joissa siihen kuuluvia tietoja käsitellään. Edellä 1 momentissa tarkoitettua tarkastusta ei saa suorittaa pysyväisluonteiseen asumiseen käytetyissä tiloissa.	*saada käyttöönsä tässä laissa säädettyjen 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 on oikeus tehdä hajasäteilysuojausratkaisun valmistajan ja sen alihankkijan tiloissa tarkastus sen selvittämiseksi, noudattavatko valmistaja ja sen alihankkija tämän lain nojalla annettuja päätöksiä. Pääesikunnan määrätyllä turvallisuusviranomaisella on oikeus tehdä edellä tarkoitettu tarkastus, jos se hoitaa tehtävää 4 b §:n 2 momentissa tarkoitetulla tavalla Liikenne- ja viestintäviraston lukuun. Tarkastuksen suorittamisessa Liikenne- ja viestintävirastoa ja Pääesikunnan määrättyä turvallisuusviranomaista voi avustaa 4 a §:ssä tarkoitettu avustava ulkopuolinen asiantuntija. Liikenne- ja viestintäviraston, Pääesikunnan määrätyn turvallisuusviranomaisen ja avustavan ulkopuolisen asiantuntijan oikeuteen päästä tiloihin ja saada tutkittavakseen välttämättömät tiedot sekä suorittaa arviointitoimenpiteitä sovelletaan, mitä 1 momentissa säädetään. Tarkastuksessa on noudatettava, mitä hallintolain (434/2003) 39 §:ssä säädetään.* Edellä 1 *ja 2* momentissa tarkoitettua tarkastusta ei saa suorittaa pysyväisluonteiseen asumiseen käytetyissä tiloissa.
7 §	7 §
Tietoturvallisuuden arviointiperusteet	*Tietoturvallisuuden **ja varautumisen** arviointiperusteet*
Viestintävirasto voi käyttää viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arviointiperusteina:	Tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden *ja varautumisen sekä turvallisuuskriittisten ratkaisujen ja niiden valmistuksen*

Voimassa oleva laki

1)lailla tai asetuksella säädettyjä viranomaisten toimintaa koskevia tietoturvallisuusvaatimuksia ja valtiovarainministeriön tietoturvallisuutta koskevia ohjeita;

2)kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa tarkoitetun kansallisen turvallisuusviranomaisen antamia kansainvälisten tietoturvallisuusvelvoitteiden toteuttamista koskevia ohjeita;

3)Euroopan unionin tai muun kansainvälisen toimielimen antamia tietoturvallisuutta koskevia säännöksiä ja ohjeita;

4)julkaistuja ja yleisesti tai alueellisesti sovellettuja tietototurvallisuutta koskevia säännöksiä, määräyksiä tai ohjeita;

5)vahvistettuun standardiin sisältyviä tietoturvallisuutta koskevia vaatimuksia.

Viestintävirasto selvittää, täyttääkö tietojärjestelmä tai tietoliikennejärjestely ne tietoturvallisuutta koskevat vaatimukset, jotka on otettu arviointiperusteeksi. Arviointi voidaan tehdä myös osittaisena.

Ehdotus

tietoturvallisuuden arviointiperusteina voidaan käyttää:

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

2*) Euroopan unionin, Pohjois-Atlantin liiton tai muun kansainvälisen toimielimen antamia tietoturvallisuutta, kyberturvallisuutta tai varautumista koskevia säännöksiä, määräyksiä ja ohjeita sekä viranomaisten ohjeita niiden soveltamisesta;*

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.

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

Arviointiviranomainen asettaa turvallisuuskriittisten ratkaisujen arviointiperusteet turvallisuuskriittisen ratkaisun valmistajaa kuultuaan. Sen lisäksi mitä 1 ja 2 momentissa säädetään, turvallisuuskriittisten ratkaisujen arviointiperusteiden määrittelyssä tulee ottaa huomioon tiedon 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 ja sen valmistuksen arvioinnissa hakea turvallisuusselvityslaissa tarkoitettu yritysturvallisuusselvitys arviointia hakevasta

Voimassa oleva laki

Ehdotus

valmistajasta. Turvallisuuskriittisen ratkaisun hyväksyntä edellyttää, että valmistajan yritysturvallisuusselvityksessä ei ole ilmennyt mitään, mikä kokonaisharkinnan perusteella vaarantaisi valmistuksen turvallisuuden ja luotettavuuden ottaen huomioon erityisesti 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 §

Todistuksen antaminen

Viestintävirasto voi pyydettäessä antaa todistuksen tietoturvallisuutta koskevat vaatimukset täyttävästä tietojärjestelmästä tai tietoliikennejärjestelystä. Todistukseen merkitään käytetyt arviointiperusteet sekä tiedot arvioinnin laajuudesta sekä tarvittaessa todistuksen voimassaoloajasta.

Todistus voidaan antaa määräajaksi, jos siihen on erityinen syy.

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 c §:ssä tarkoitetusta pyynnöstä viranomaisen tietojärjestelmän tai tietoliikennejärjestelyn hyväksyntäpäätöksen tai -lausunnon, jos tietojärjestelmä tai tietoliikennejärjestely täyttää vaatimukset. Päätökseen tai lausuntoon on merkittävä tiedot arvioinnin kohteesta, käytetyistä 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 tietoturvallisuuden arvioinnista päätös, josta ilmenee arvioinnin tulos. Hyväksyntäpäätöksestä tulee ilmetä hyväksynnän voimassaolo, ja siihen voidaan sisällyttää sellaisia rajoituksia ja ehtoja, jotka ovat tarpeen ratkaisun turvallisessa käytössä. Hajasäteilysuojausratkaisuja valmistavan turvallisuuskriittisen ratkaisun valmistajaa koskevaan hyväksyntäpäätökseen voidaan

Voimassa oleva laki	*Ehdotus*
	sisällyttää ehtoja, jotka ovat tarpeen valmistuksen luotettavuuden varmistamiseksi.
8 a §	8 a §
Viranomaisen velvollisuus hankkia todistus	***Hyväksyttyjen turvallisuuskriittisten ratkaisujen ja valmistajien luettelo***
Valtioneuvoston asetuksella voidaan säätää, että 8 §:ssä tarkoitettu todistus on hankittava sellaisen valtionhallinnon viranomaisen määräysvallassa olevasta tietojärjestelmästä tai tietoliikennejärjestelystä, jossa käsitellään turvallisuusluokkaan I tai II kuuluviksi luokiteltuja asiakirjoja.	*Liikenne- ja viestintävirasto ylläpitää julkista luetteloa 8 §:n 3 momentin mukaisesti hyväksyntäpäätöksen saaneista turvallisuuskriittisistä ratkaisuista ja turvallisuuskriittisten ratkaisujen valmistajista. Luettelosta tulee käydä ilmi:* *1) turvallisuuskriittisen ratkaisun nimi, käyttötarkoitus ja versio;* *2) tiedon turvallisuusluokka, jonka suojaamiseen ratkaisu on todettu riittäväksi;* *3) turvallisuuskriittisen ratkaisun valmistaja;* *4) hyväksynnän voimassaolo, muutos tai lakkaaminen; sekä* *5) hyväksyntään liittyvät turvallisen käytön ehdot ja rajoitukset.*
8 b §	
Turvallisuusselvitysrekisteriin merkittävät tiedot ja merkinnän poistaminen	
Viestintävirasto voi tallettaa antamastaan todistuksesta 8 §:ssä mainitut tiedot turvallisuusselvityslaissa tarkoitettuun turvallisuusselvitysrekisteriin. Viestintäviraston on poistettava merkintä kuuden kuukauden kuluessa siitä, kun todistuksessa asetettu määräaika on päättynyt. Merkintä poistetaan kuukauden kuluessa siitä, kun peruuttamista koskeva ratkaisu on tullut lainvoimaiseksi.	(kumotaan)
9 §	9 §
*Tietoturvallisuuden **tason** ylläpito ja seuranta*	*Tietoturvallisuuden ylläpito ja seuranta*
Sen, joka haluaa 8 §:ssä tarkoitetun todistuksen, on annettava sitoumus tietoturvallisuustason säilyttämisestä. Todistuksen saaneen on ilmoitettava Viestintävirastolle sellaisista muutoksista, joilla on vaikutusta tietoturvallisuustasoon,	*Edellä 8 §:ssä tarkoitetun päätöksen tai lausunnon saaneen on ylläpidettävä tietoturvallisuus lausunnon tai päätöksen mukaisena. Päätöksen tai lausunnon saaneen on ilmoitettava arviointiviranomaiselle sellaisista muutoksista, joilla voi olla*

Voimassa oleva laki	*Ehdotus*
sekä sallittava Viestintävirastolle pääsy tietojärjestelmiin ja tietoliikennejärjestelyihin sen selvittämiseksi, täyttävätkö ne edelleen todistuksen mukaiset vaatimukset.	*vaikutusta päätöksen tai lausunnon mukaisiin vaatimuksiin.*
10 §	10 §
Todistuksen peruuttaminen	*Hyväksyntäpäätöksen tai -lausunnon peruuttaminen*
Viestintävirasto voi peruuttaa tämän lain nojalla annetun todistuksen, jos arvioinnin kohteena ollut tietojärjestelmä tai tietoliikennejärjestely ei enää täytä niitä vaatimuksia, jotka ovat olleet edellytyksenä todistuksen antamiselle.	*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.
Viestintäviraston on ennen 1 momentissa tarkoitetun ratkaisun tekemistä kuultava todistuksen saanutta sekä varattava tälle tilaisuus korjata puute.	*Arviointiviranomaisen* on ennen 1 momentissa tarkoitetun *peruuttamisen* tekemistä kuultava *päätöksen tai lausunnon saanutta* sekä varattava tälle tilaisuus korjata puute.
Viestintävirasto voi 1 momentissa tarkoitetussa päätöksessään määrätä, että päätöstä on noudatettava muutoksenhausta huolimatta, jollei muutoksenhakuviranomainen toisin määrää.	*Arviointiviranomainen* voi 1 momentissa tarkoitetussa *peruuttamista koskevassa* päätöksessään määrätä, että päätöstä on noudatettava muutoksenhausta huolimatta, jollei muutoksenhakuviranomainen toisin määrää.
11 §	11 §
Muutoksenhaku	*Muutoksenhaku*
Muutoksenhausta Viestintäviraston tämän lain nojalla tekemään päätökseen säädetään hallintolainkäyttölaissa (586/1996).	Muutoksenhausta *arviointiviranomaisen* tämän lain nojalla tekemään päätökseen säädetään *oikeudenkäynnistä hallintoasioissa annetussa laissa (808/2019).*
12 §	12 §
Maksut	*Maksut*
Asian vireille saattajalta Viestintäviraston arvioinnista, todistuksen antamisesta ja selvityksestä perittävistä maksuista säädetään valtion maksuperustelaissa (150/1992) ja sen nojalla.	*Arviointiviranomaisen arvioinnista sekä arviointiraportin, lausunnon tai päätöksen antamisesta, neuvonnasta ja selvityksestä peritään asian vireille saattajalta maksu noudattaen, mitä valtion maksuperustelaissa (150/1992) säädetään.*

Voimassa oleva laki

Ehdotus

_____

Tämä laki tulee voimaan päivänä kuuta 2026.

Valtionhallinnon viranomaisen on saatettava tietojärjestelmiensä ja tietoliikennejärjestelyjensä tietoturvallisuuden ja varautumisen arviointi vastaamaan 3 a §:ssä säädettyä viiden vuoden kuluessa tämän lain voimaatulosta, kuitenkin siten, että arviointi on saatettava vastaamaan mainitun pykälän 2 momentin 1 kohdassa säädettyä kahden vuoden kuluessa lain voimaantulosta ja 2 kohdassa säädettyä kolmen vuoden kuluessa lain voimaantulosta.

Muiden kuin valtionhallinnon viranomaisten on saatettava tietojärjestelmiensä ja tietoliikennejärjestelyjensä tietoturvallisuuden ja varautumisen arviointi vastaamaan 3 b §:n 1 momentissa säädettyä kahden vuoden kuluessa lain voimaantulosta ja mainitun pykälän 2 momentissa säädettyä kolmen vuoden kuluessa lain voimaantulosta.

Tietoturvallisuuden vaatimustenmukaisuudesta annettu todistus, joka on annettu tämän lain voimaan tullessa voimassa olleiden säännösten mukaisesti, vastaa 8 §:ssä tarkoitettua päätöstä, ja on voimassa todistukseen merkityn ajan.

_____

2.

Laki

tietoturvallisuuden arviointilaitoksista annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti

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

lisätään lakiin uusi 9 a § seuraavasti:

Voimassa oleva laki	*Ehdotus*
1 luku	1 luku
Yleiset säännökset	**Yleiset säännökset**
1 §	1 §
Lain tarkoitus	*Lain tarkoitus*
Tässä laissa säädetään menettelystä, jonka avulla yritykset voivat osoittaa luotettavasti ulkopuolisille, että niiden toiminnassa on toteutettu määrätty tietoturvallisuuden taso.	Tässä laissa säädetään menettelystä, jonka avulla viranomaiset voivat *hankkia riippumattoman tietoturvallisuuden tai varautumisen arvioinnin* ja *jonka avulla* yritykset voivat osoittaa luotettavasti ulkopuolisille, että niiden toiminnassa on toteutettu määrätty tietoturvallisuuden taso.
2 §	2 §
Lain soveltamisala	*Lain soveltamisala*
Tätä lakia sovelletaan elinkeinonharjoittajiin ja palvelutehtäviä julkishallinnolle tarjoaviin yksiköihin, jotka toimeksiannosta arvioivat tietoturvallisuustason (tietoturvallisuuden arviointilaitos) ja jotka haluavat toiminnalleen Viestintäviraston hyväksynnän. Lisäksi tätä lakia sovelletaan hyväksymismenettelyyn. Viestintäviraston tehtävistä viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnissa sekä yhteisöturvallisuusselvitysten laadinnassa säädetään erikseen.	Tätä lakia sovelletaan elinkeinonharjoittajiin ja palvelutehtäviä julkishallinnolle tarjoaviin yksiköihin, jotka toimeksiannosta arvioivat *tietoturvallisuuden tason taikka tietojärjestelmän tai tietoliikennejärjestelyn varautumisen tason* (***tietoturvallisuuden arviointilaitos***) ja jotka haluavat toiminnalleen *Liikenne- ja viestintäviraston hyväksymisen*. Lisäksi tätä lakia sovelletaan hyväksymismenettelyyn. *Arviointiviranomaisten* tehtävistä viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden *ja varautumisen* arvioinnissa sekä yritysturvallisuusselvitysten laadinnassa säädetään erikseen.

Voimassa oleva laki	*Ehdotus*
3 §	3 §
Arviointilaitoksen hyväksymistä koskeva hakemus	*Arviointilaitoksen hyväksymistä koskeva hakemus*
Tietoturvallisuuden arviointilaitos voi hakea Viestintäviraston hyväksyntää toimintaansa varten. — — — — — — — — — — — — — — —	Tietoturvallisuuden arviointilaitos voi hakea *Liikenne- ja viestintäviraston* hyväksyntää toimintaansa *ja arvioinnin pätevyysaluetta* varten. — — — — — — — — — — — — — — —
4 §	4 §
Hakemuksen käsittely	*Hakemuksen käsittely*
Viestintäviraston on ennen tietoturvallisuuden arviointilaitoksen hyväksymistä varattava suojelupoliisille tilaisuus lausua arviointilaitoksen vastuuhenkilöiden luotettavuudesta ja sen toimitilojen turvallisuudesta. Suojelupoliisi noudattaa lausuntoaan laatiessaan, mitä turvallisuusselvityslaissa *(726/2014)* säädetään. Viestintävirasto voi hakemusta käsiteltäessä hankkia lausuntoja sekä antaa hakemuksen ja siinä esitettyjen tietojen arvioimiseksi toimeksiannostaan suoritettavia tehtäviä ulkopuolisille asiantuntijoille.	*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 turvallisuusselvityslaissa (726/2014) tarkoitettu yritysturvallisuusselvitys.* Suojelupoliisi noudattaa lausuntoa tai selvitystä laatiessaan, mitä turvallisuusselvityslaissa säädetään. *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 §	5 §
Arviointilaitoksen hyväksyminen	*Arviointilaitoksen hyväksyminen*
Tietoturvallisuuden arviointilaitoksen hyväksymisen edellytyksenä on, että: 1)laitos on toiminnallisesti ja taloudellisesti riippumaton arvioinnin kohteesta;	Tietoturvallisuuden arviointilaitoksen hyväksymisen edellytyksenä on, että: 1)laitos on toiminnallisesti ja taloudellisesti riippumaton arvioinnin kohteesta;

Voimassa oleva laki

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

4)laitoksen vastuuhenkilöiden luotettavuus on varmistettu ja laitoksella on luotettavaksi arvioitu ja valvottu menetelmä, jonka avulla laitoksen toimitilojen ja tietojenkäsittelyn turvallisuus varmistetaan;

5) laitoksella on asianmukaiset ohjeet toimintaansa ja sen seurantaa varten.

Edellä 1 momentin 1–3 kohdassa tarkoitettujen vaatimusten täyttäminen on osoitettava vaatimustenmukaisuuden arviointipalvelujen pätevyyden toteamisesta annetussa laissa (920/2005) säädetyn menettelyn avulla.

Viestintävirasto hyväksyy saamiensa ja laatimiensa selvitysten sekä suorittamiensa tarkastusten perusteella vaatimukset täyttävän laitoksen hyväksytyksi tietoturvallisuuden arviointilaitokseksi. Tällainen laitos voi markkinoinnissaan ja muussa viestinnässään käyttää Viestintäviraston hyväksymistä koskevaa ilmaisua edellyttäen, ettei hyväksymisen voimassaoloa koskeva määräaika ole päättynyt tai 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.

Ehdotus

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

4) *laitoksen yritysturvallisuusselvityksessä ei ole ilmennyt sellaista seikkaa, joka 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;*

5) laitoksella on asianmukaiset ohjeet toimintaansa ja sen seurantaa varten.

Edellä 1 momentin 1–3 kohdassa tarkoitettujen vaatimusten täyttäminen on osoitettava vaatimustenmukaisuuden arviointipalvelujen pätevyyden toteamisesta annetussa laissa (920/2005) säädetyn menettelyn avulla.

Sen estämättä mitä 2 momentissa säädetään, hyväksytyn arviointilaitoksen hakiessa hyväksymistä 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 *hyväksyntää.*

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

Voimassa oleva laki

Ehdotus

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, Viestintäviraston on kehotettava arviointilaitosta korjaamaan puute määräajassa. Jos puutetta ei korjata määräajassa, Viestintävirasto voi peruuttaa hyväksymisen.

Viestintävirasto voi päätöksessään määrätä, että päätöstä on noudatettava muutoksenhausta huolimatta, jollei muutoksenhakuviranomainen toisin määrää.

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 §

Viestintäviraston tarkastusoikeus

Viestintävirastolla ja sen toimeksiannosta toimivalla asiantuntijalla on oikeus tarkastaa hyväksyntää hakeneen tai hyväksytyn tietoturvallisuuden arviointilaitoksen tilat sekä sen käytössä olevat menetelmät. Tarkastusta ei saa suorittaa pysyväisluonteiseen asumiseen käytetyissä tiloissa.

7 §

Liikenne- ja viestintäviraston tiedonsaanti ja tarkastusoikeus

Liikenne- ja viestintävirastolla on oikeus tarkastaa *hyväksymistä hakevan ja* hyväksytyn tietoturvallisuuden arviointilaitoksen *ja sen 9 a §:ssä tarkoitetun alihankkijan* tilat sekä sen käytössä olevat menetelmät. Tarkastuksen suorittamisessa Liikenne- ja viestintävirastoa voi avustaa 4 §:n 2 momentissa tarkoitettu ulkopuolinen asiantuntija. Tarkastusta ei saa suorittaa pysyväisluonteiseen asumiseen käytetyissä tiloissa.

Liikenne- ja viestintävirastolla on oikeus salassapitosäännösten tai muiden tiedon luovuttamista koskevien rajoitusten estämättä saada pyynnöstä suojelupoliisilta, kansalliselta akkreditointiyksiköltä, pätevyysalueen arviointiperusteen soveltamista ohjaavalta tai valvovalta viranomaiselta, arviointilaitokselta sekä sen alihankkijalta ja asiakkaalta ne tiedot, jotka ovat välttämättömiä sen valvomiseksi, että tietoturvallisuuden arviointilaitos täyttää toimintaansa koskevat vaatimukset.

Voimassa oleva laki	*Ehdotus*
8 §	8 §
Arviointilaitoksen tiedonanto- ja ilmoitusvelvollisuus	*Arviointilaitoksen* ***ilmoitusvelvollisuus***
Hyväksytyn tietoturvallisuuden arviointilaitoksen on ilmoitettava Viestintävirastolle sellaisesta toimintaansa koskevasta muutoksesta, jolla on merkitystä laitosta koskevien velvoitteiden kannalta. *Viestintävirastolla on sen lisäksi, mitä 1 momentissa säädetään, oikeus pyynnöstä saada arviointilaitokselta ne tiedot, jotka ovat tarpeen sen valvomiseksi, että laitos täyttää toimintaansa koskevat vaatimukset.*	Hyväksytyn tietoturvallisuuden arviointilaitoksen on *ilmoitettava Liikenne- ja viestintävirastolle* sellaisesta toimintaansa koskevasta muutoksesta, jolla on merkitystä laitosta koskevien velvoitteiden kannalta.
3 luku	3 luku
Tietoturvallisuuden arviointi	**Tietoturvallisuuden *ja varautumisen* arviointi**
9 §	9 §
Arviointilaitoksen tehtävät	*Arviointilaitoksen tehtävät*
Hyväksytyn tietoturvallisuuden arviointilaitoksen on saamaansa tietoturvallisuuden arviointitehtävää suorittaessaan noudatettava huolellisuutta ja pidettävä huolta siitä, että arvioinnin aikana: 1)tarkastetaan arvioinnin kohteen toimitilat; 2) selvitetään, onko arvioinnin kohteen toiminnassa asianmukaisella tavalla toteutettu 10 §:ssä tarkoitetut tietoturvallisuutta koskevat vaatimukset, jotka on otettu selvityksen perustaksi (tietoturvallisuuden arviointiperusteet). Arviointi voidaan tehdä myös osittaisena. Hyväksytty tietoturvallisuuden arviointilaitos antaa selvitysten ja tarkastuksen perusteella todistuksen, jos arvioitavan kohteen toimitilat ja toiminta on selvityksen perustana olleiden arviointiperusteiden mukainen. Todistuksessa tulee yksilöidä arvioinnissa käytetyt tietoturvallisuuden arviointiperusteet ja arvioinnin laajuus.	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 arvioinnin kohteesta, käytetyistä arviointiperusteista, arvioinnin laajuudesta ja havainnoista*. *Hyväksytty tietoturvallisuuden arviointilaitos voi pyynnöstä, tai jos niin erikseen säädetään* antaa selvitysten ja tarkastuksen perusteella todistuksen, jos

Voimassa oleva laki

Ehdotus

arvioitava *kohde on selvityksen perustana olleiden tietoturvallisuuden ja varautumisen 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 samaan konserniin kuuluvalla yhtiöllä tai muuna alihankintana vain, jos konserniyhtiö tai muu alihankkija täyttää tietoturvallisuuden arviointilaitoksen hyväksymisen edellytykset ja alihankinnasta on annettu selvitys Liikenne- ja viestintävirastolle ja Liikenne- ja viestintävirasto on todennut edellytysten täyttymisen.

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

10 §

Tietoturvallisuuden arviointiperusteet

Tietoturvallisuuden arviointiperusteina voidaan tässä laissa tarkoitetussa arvioinnissa käyttää arvioinnin kohteen valinnan mukaan:

1)lailla tai asetuksella säädettyjä viranomaisten toimintaa koskevia tietoturvallisuusvaatimuksia ja valtiovarainministeriön tietoturvallisuutta koskevia ohjeita;

2)kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa tarkoitetun kansallisen turvallisuusviranomaisen antamia kansainvälisten tietoturvallisuusvelvoitteiden toteuttamista koskevia ohjeita;

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, määräyksiä ja ohjeita sekä viranomaisten ohjeita niiden soveltamisesta;*

Voimassa oleva laki	*Ehdotus*
3)Euroopan unionin tai muun kansainvälisen toimielimen antamia tietoturvallisuutta koskevia säännöksiä tai ohjeita; 4)julkaistuja ja yleisesti tai alueellisesti sovellettuja tietototurvallisuutta koskevia säännöksiä, määräyksiä tai ohjeita; *5)vahvistettuun standardiin sisältyviä tietoturvallisuutta koskevia vaatimuksia.*	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.*
11 § *Maksut* Tietoturvallisuuden arviointilaitoksen hyväksymistä koskevan asian käsittelystä Viestintävirastossa perittävästä maksusta säädetään valtion maksuperustelaissa (150/1992) ja sen nojalla.	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 Viestintäviraston tämän lain nojalla tekemään päätökseen säädetään hallintolainkäyttölaissa (586/1996).	12 § *Muutoksenhaku* Muutoksenhausta *Liikenne- ja viestintäviraston* tämän lain nojalla tekemään päätökseen säädetään *oikeudenkäynnistä hallintoasioissa annetussa laissa (808/2019).*
13 § *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) *sekä* kielilakia (423/2003).	13 § *Virkavastuuta ja hyvää hallintoa koskevien säännösten soveltaminen* Hyväksytyn tietoturvallisuuden arviointilaitoksen on tässä laissa tarkoitettuja *julkisia hallintotehtäviä* 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).* *Hyväksytyn tietoturvallisuuden arviointilaitosten vastuuhenkilöön ja palveluksessa olevaan henkilöön sekä 9 a §:ssä tarkoitettujen alihankkijoiden palveluksessa olevaan henkilöön sovelletaan rikosoikeudellista virkavastuuta koskevia säännöksiä hänen suorittaessaan tässä laissa tarkoitettuja tehtäviä.*

Voimassa oleva laki

13 a §

Turvallisuusselvitysrekisteriin merkittävät tiedot

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 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.

Ehdotus

Vahingonkorvausvastuusta säädetään vahingonkorvauslaissa.

13 a §

Turvallisuusselvitysrekisteriin merkittävät tiedot

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

Hyväksytty *tietoturvallisuuden* 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 päivänä -kuuta 2026.

Liikenne- ja viestintäviraston tulee kahden vuoden kuluessa tämän lain voimaantulosta hakea 4 §:n mukaisesti yritysturvallisuusselvitys hyväksytystä tietoturvallisuuden arviointilaitoksesta, jolle on tämän lain voimaan tullessa voimassa olleiden säännösten mukaisesti hyväksytty pätevyysalue turvallisuusluokitellun tiedon käsittelyn arviointiin.

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:

Voimassa oleva laki	*Ehdotus*
18 §	18 §
Turvallisuusvaatimusten toteuttaminen yleisenä edellytyksenä	*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 todistuksella, turvallisuussuunnitelmalla tai muulla turvallisuusselvityksen tekemisestä päättävän toimivaltaisen viranomaisen hyväksymällä tavalla.	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.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
48 §	
Turvallisuusselvitysrekisteri, rekisterin käyttötarkoitus ja tietojen tallettaminen rekisteriin	
— — — — — — — — — — — — — — —	
Liikenne- ja viestintävirasto voi tallettaa turvallisuusselvitysrekisteriin tiedot:	
1)*viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annetun lain mukaan antamistaan todistuksista ja niihin merkityistä tiedoista*;	(kumotaan)
— — — — — — — — — — — — — — —	

———

Voimassa oleva laki	*Ehdotus*
	Tämä laki tulee voimaan päivänä kuuta 20 .

_____