Valtiovarainministeriö

Lausuntopyyntö

27.11.2025 VN/36127/2023

Lausuntopyyntö ehdotuksesta viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden ja varautumisen arviointia koskevan lainsäädännön muuttamisesta

Johdanto

Valtiovarainministeriössä on valmisteltu oheinen luonnos hallituksen esitykseksi eduskunnalle laeiksi viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annetun lain, tietoturvallisuuden arviointilaitoksista annetun lain sekä turvallisuusselvityslain muuttamisesta.

Ehdotetuilla muutoksilla selkeytettäisiin viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen arviointimenettelyjä ja 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. Muiden 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, ellei 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.

Lisäksi tarkennettaisiin Liikenne- ja viestintäviraston tehtäviä ja säädettäisiin turvallisuuskriittisten tuotteiden valmistajille oikeus hakea arviointia. Lisättäisiin Puolustusvoimille arviointitehtävä sekä tarkennettaisiin ja tehostettaisiin arviointiviranomaisten yhteistyötä, työjakoa ja tiedonsaantioikeuksia sekä mahdollistettaisiin arviointiviranomaista avustava tehtävä ja säädettäisiin VTT Oy:n avustavasta arviointitehtävästä. Yksinkertaistettaisiin ja tehostettaisiin tietoturvallisuuden arviointilaitosten luotettavuuden sääntelyä ja joustavoitettaisiin niiden pätevyyksien hyväksyntää.

Valtiovarainministeriö pyytää lausuntoanne esityksestä.

Tausta

Esityksen valmisteluun on johtanut kansainvälisen ja kansallisen toimintaympäristön ja turvallisuustilanteen merkittävä muuttuminen, mikä on lisännyt tietoturvallisuuden arviointipalvelujen kysyntää. Voimassa oleva julkisen hallinnon tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnin keskeinen sääntely on valmisteltu yli 13 vuotta sitten. Keskeistä arviointeihin liittyvää kansallista sääntelyä kuten laki julkisen hallinnon tiedonhallinnasta (906/2019) ja turvallisuusselvityslaki (726/2014) on valmistunut tämän jälkeen. Digitalisaation edistyminen ja kehittyvät teknologiat kuten pilvipalvelut, tekoäly ja kvanttilaskenta ovat vaikuttamassa sekä julkisen hallinnon toimintatapoihin että niihin menettelyihin, joilla julkisen hallinnon tietojärjestelmiä toteutetaan. Aiemmat selvitykset puoltavat tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnin sääntelyn ajantasaistamista ja arviointitoiminnan kehittämistä tehokkaammaksi.

Valtiovarainministeriö asetti 22.2.2024 arviointeja koskevan sääntelyn ajantasaistamista ja niiden tehostamista tukevan työryhmän. Työryhmän tehtävinä oli arvioida sääntelyn muutostarpeet sekä valmistella ehdotukset sääntelyn ajantasaistamiseksi. Arviointilakien ajantasaistaminen on myös yksi Suomen Kyberturvallisuusstrategian 2024-2035 toimeenpanosuunnitelman priorisoiduista toimenpiteistä. Valtioneuvoston puolustusselonteossa todetaan, että tavoitetilassa Puolustusvoimilla on itsenäinen kyky tietojärjestelmien ja salaustuotteiden arviointi- ja hyväksyntätoimintaan. Pääministeri Orpon hallituksen hallitusohjelman mukaan salaustuotteiden hyväksyntäprosessia nopeutetaan.

Tavoitteet

Hallituksen esityksen tavoitteena on mahdollistaa kustannustehokkaat viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden ja varautumisen arviointimenettelyt. Esityksellä vastataan arviointitarpeiden kasvuun, joka johtuu toimintaympäristön ja turvallisuusuhkien muutoksesta.

Tavoitteena on parantaa arviointien saatavuutta, sujuvoittaa arviointimenettelyä, selkeyttää arviointiperusteita ja tehostaa viranomaisyhteistyötä. Tavoitteena on, että viranomaiset hyödyntäisivät tietojärjestelmiensä ja tietoliikennejärjestelyjensä tietoturvallisuus- ja varautumistoimenpiteiden mitoittamisessa tilanteeseen soveltuvaa arviointimenettelyä turvallisuuden edistämiseksi.

Esityksen tavoitteena on selkeyttää lainsäädännön tasolla periaatetta siitä, että viranomaisella on vastuu omien tietojärjestelmiensä ja tietoliikennejärjestelyjensä tietoturvallisuudesta ja varautumisesta sekä käyttöönottopäätöksestä. Esityksen tavoitteena on turvallisuuskriittisten ratkaisujen arvioinnin ja hyväksynnän kautta parantaa yritysten mahdollisuuksia tarjota ratkaisujaan sekä Suomessa että kansainvälisissä yhteyksissä. Tavoitteena on nopeuttaa tietojärjestelmien ja tietoliikennejärjestelyjen arviointia, kun viranomaisilla on mahdollisuus valita tietojärjestelmiinsä ja tietoliikennejärjestelyihinsä ratkaisuja, jotka on jo arvioitu ja hyväksytty. Esityksen tavoitteena on myös selkeyttää tietoturvallisuuden arviointilaitosten elinkeinotoiminnan edellytyksiä arviointien saatavuuden parantamiseksi.

Vastausohjeet vastaanottajille

Kuka tahansa voi antaa lausunnon.

Lausunto pyydetään ensisijaisesti antamaan vastaamalla lausuntopyyntöön lausuntopalvelun kautta.

Ohjeet palveluun rekisteröitymiseksi ja palvelun käyttämiseksi löytyvät lausuntopalvelun sivulta Ohjeet > Käyttöohjeet (käyttäjätuki: lausuntopalvelu.om(at)gov.fi). Ministeriöiden tulee lisäksi tallentaa lausuntopalvelussa antamansa lausunto VAHVA-asianhallintajärjestelmään asialle VN/36127/2023.

Jos lausuntoa ei ole mahdollista antaa lausuntopalvelussa, lausunto voidaan vaihtoehtoisesti toimittaa ministeriön kirjaamoon sähköpostilla osoitteeseen kirjaamo.vm@gov.fi tai postitse osoitteeseen Valtiovarainministeriö, PL 28, 00023 VALTIONEUVOSTO. Kirjaamoon toimitetussa lausunnossa pyydetään mainitsemaan asianumero VN/36127/2023. Lisäksi kirjaamoon toimitettu lausunto pyydetään lähettämään esimerkiksi sähköpostin liitetiedostona Word- tai PDF-muodossa, jotta lausuntoasiakirja ei sisällä tarpeettomia henkilötietoja, kuten yksityishenkilön sähköpostiosoitetta.

Kaikki annetut lausunnot ovat lähtökohtaisesti julkisia viranomaisten toiminnan julkisuudesta annetun lain (621/1999) mukaisesti. Lausunnot julkaistaan hankkeen julkisilla hankesivuilla (valtioneuvosto.fi/hankkeet, tunnus VM167:00/2023). Yksityishenkilön lausunto julkaistaan kuitenkin hankesivuilla tietosuojasyistä ainoastaan, jos henkilö tätä kirjallisesti pyytää esimerkiksi lausuntonsa yhteydessä tai sen saateviestissä.

Lisäksi kaikki lausuntopalvelussa annetut lausunnot, mukaan lukien yksityishenkilöiden lausunnot,
ovat automaattisesti kaikkien nähtävissä lausuntopalvelussa. Ministeriö ei julkaise kirjaamoon toimitettuja lausuntoja lausuntopalvelussa.

Lausunnossa ei tule ilmoittaa tarpeettomia henkilötietoja. Vaikka yksityishenkilön kirjaamoon toimittamaa lausuntoa ei julkaistaisi verkossa, lausunto on ministeriöltä kaikkien saatavissa viranomaisten toiminnan julkisuudesta annetun lain mukaisesti.

Aikataulu

Lausunto pyydetään toimittamaan valtiovarainministeriölle viimeistään 23.1.2026 klo 14.00.

Valmistelijat

Lisätietoja lausuntopyyntöön liittyen antavat neuvotteleva virkamies Marika Kalliotie, +358 295 530 491, (poissa 23.12.-31.12.2025) ja tietohallintoneuvos Tuija Kuusisto, +358 295 530 065, (poissa 19.12.-23.12.2025), etunimi.sukunimi@gov.fi

Linkit

https://vm.fi/hanke?tunnus=VM167:00/2023 - Hankeikkuna/Statsrådets projektportal: Julkisen hallinnon tietojärjestelmien vaatimustenmukaisuuden arvioinnin ajan-tasaistamisen ja tehostamisen työryhmä

Liitteet:

Luonnos hallituksen esitykseksi.pdf

Utkast till regeringens proposition.pdf

Jakelu:

Aalto-yliopisto
Ahvenanmaan hallintotuomioistuin
Ahvenanmaan oikeusrekisterikeskus
Ahvenanmaan valtionvirasto
Akaan kaupunki
Alajärven kaupunki
Alavieskan kunta
Alavuden kaupunki
AllWipe Oy
Ammattiopisto Livia
Arcada
Asikkalan kunta
Askolan kunta
Asumisen rahoitus- ja kehittämiskeskus ARA
Auran kunta
Brändö kommun
Business Finland
Celia
Centria-ammattikorkeakoulu
CMC Finland
Diakonia-ammattikorkeakoulu
Digi- ja väestötietovirasto
Digia Finland Oy
Eckerö kommun
Eduskunnan oikeusasiamies
Eduskunta
Energiavirasto
Enonkosken kunta
Enontekiön kunta
Espoon kaupunki - Esbo stad
Etelä-Karjalan hyvinvointialue
Etelä-Karjalan käräjäoikeus
Etelä-Karjalan liitto
Etelä-Pohjanmaan ELY-keskus
Etelä-Pohjanmaan hyvinvointialue
Etelä-Pohjanmaan käräjäoikeus

Etelä-Pohjanmaan liitto
Etelä-Pohjanmaan TE-toimisto
Etelä-Savon ELY-keskus
Etelä-Savon hyvinvointialue
Etelä-Savon hyvinvointialue
Etelä-Savon kampuskiinteistöt kuntayhtymä
Etelä-Savon käräjäoikeus
Etelä-Savon maakuntaliitto
Etelä-Savon TE-toimisto
Etelä-Suomen aluehallintovirasto
Etelä-Suomen ulosottopiiri
Etelä-Suomen ulosottopiiri
Etelä-Suomen ulosottopiiri
Etelä-Suomen ulosottopiiri
Etelä-Suomen ulosottopiiri
Eurajoen kunta
Euran kunta
Evijärven kunta
Fimea
Finas
Finströms kommun
Forssan kaupunki
Forssan seudun hyvinvointikuntayhtymä
Föglö kommun
Geologian tutkimuskeskus
Geta kommun
Haaga-Helia ammattikorkeakoulu
Haapajärven kaupunki
Haapaveden kaupunki
Hailuodon kunta
Halsuan kunta
Haminan kaupunki
Hammarlands kommun
Hangon kaupunki - Hangö stad
Hankasalmen kunta
Hanken
Harjavallan kaupunki
Hartolan kunta
Hattulan kunta
Hausjärven kunta
Heinolan kaupunki
Heinäveden kunta
Helsingin hallinto-oikeus
Helsingin hovioikeus
Helsingin kaupunki - Helsingfors stad
Helsingin käräjäoikeus
Helsingin poliisilaitos
Helsingin ranskalais-suomalainen koulu
Helsingin yliopisto
Heuni
Hirvensalmen kunta

Hollolan kunta
HSL
HSY
Huittisten kaupunki
Humanistinen ammattikorkeakoulu
Humppilan kunta
Huoltovarmuuskeskus
Hyrynsalmen kunta
Hyvinkään kaupunki
Hämeen ammattikorkeakoulu
Hämeen ELY-keskus
Hämeen liitto
Hämeen poliisilaitos
Hämeen TE-toimisto
Hämeenkyrön kunta
Hämeenlinnan hallinto-oikeus
Hämeenlinnan kaupunki
Hätäkeskuslaitos
Iin kunta
Iisalmen kaupunki
Iitin kunta
Ikaalisten kaupunki
Ilmajoen kunta
Ilmatieteen laitos
Ilomantsin kunta
Imatran kaupunki
Inarin kunta
Ingå kommun - Inkoon kunta
Insta Advance Oy
Into Certification Oy
Isojoen kunta
Isokyrön kunta
Itä-Lapin kuntayhtymä
Itä-Suomen aluehallintovirasto
Itä-Suomen hallinto-oikeus
Itä-Suomen hovioikeus
Itä-Suomen poliisilaitos
Itä-Suomen yliopisto
Itä-Uudenmaan hyvinvointialue
Itä-Uudenmaan käräjäoikeus
Itä-Uudenmaan poliisilaitos
Jakobstad - Pietarsaaren kaupunki
Janakkalan kunta
Jatkuvan oppimisen ja työllisyyden palvelukeskus
Joensuun kaupunki
Jokilaaksojen koulutuskuntayhtymä
Jokioisten kunta
Jomala kommun
Joroisten kunta
Joutsan kunta
Juukan kunta

Juupajoen kunta
Juvan kunta
Jyväskylän ammattikorkeakoulu
Jyväskylän kaupunki
Jyväskylän yliopisto
Jyvöskylän koulutuskuntayhtymä
Jämijärven kunta
Jämsän kaupunki
Järvenpään kaupunki
Järviseudun ammatti-instituutti
Kaakkois-Suomen ammattikorkeakoulu
Kaakkois-Suomen ELY-keskus
Kaakkois-Suomen poliisilaitos
Kaakkois-Suomen TE-toimisto
Kaarinan kaupunki
Kaavin kunta
Kainuun ELY-keskus
Kainuun hyvinvointialue
Kainuun jätehuollon kuntayhtymä
Kainuun käräjäoikeus
Kainuun liitto
Kainuun TE-toimisto
Kajaanin ammattikorkeakoulu
Kajaanin kaupunki
Kalajoen kaupunki
Kangasalan kunta
Kangasniemen kunta
Kankaanpään kaupunki
Kannonkosken kunta
Kannuksen kaupunki
Kansallinen audiovisuaalinen instituutti
Kansallinen koulutuksen arviointikeskus
Kansallisarkisto
Kanta-Hämeen hyvinvointialue
Kanta-Hämeen käräjäoikeus
Karelia-ammattikorkeakoulu
Karijoen kunta
Karkkilan kaupunki
Karstulan kunta
Karvian kunta
Kaskisten kaupunki - Kaskis stad
Kauhajoen kaupunki
Kauhavan kaupunki
Kauniaisten kaupunki - Grankulla stad
Kaustisen kunta
KEHA-keskus
Keiteleen kunta
Kemijärven kaupunki
Kemin kaupunki
Keminmaan kunta
Kemi-Tornionlaakson koulutuskuntayhtymä

Kemi-Tornionlaakson koulutuskuntayhtymä
Kempeleen kunta
Keravan kaupunki
Keski-Pohjanmaan hyvinvointialue
Keski-Pohjanmaan liitto
Keski-Savon Jätehuolto liikelaitoskuntayhtymä
Keski-Suomen ELY-keskus
Keski-Suomen hyvinvointialue
Keski-Suomen hyvinvointialue
Keski-Suomen hyvinvointialue
Keski-Suomen käräjäoikeus
Keski-Suomen liitto
Keski-Suomen TE-toimisto
Keski-Uudenmaan hyvinvointialue
Keski-Uudenmaan koulutuskuntayhtymä
Keski-Uudenmaan Vesi ja Vesiensuojelu
Keskusrikospoliisi
Keuruun kaupunki
Kihniön kunta
Kimitoö kommun - Kemiönsaaren kunta
Kinnulan kunta
Kirjaamo
Kirkkonummen kunta - Kyrkslätt kommun
Kiteen kaupunki
Kittilän kunta
Kiuruveden kaupunki
Kiwa Sertifiointi Oy
Kivijärven kunta
Kokemäen kaupunki
Kokkolan kaupunki - Karleby stad
Kolarin kunta
Kolpeneen tuki- ja osaamiskeskus
Konkurssiasiamiehen toimisto
Konneveden kunta
Kontiolahden kunta
Korkein hallinto-oikeus
Korkein oikeus
Korpelan Voima kuntayhtymä
Korsholm kommun - Mustasaaren kunta
Korsnäs kommun
Kotimaisten kielten keskus
Kotkan kaupunki
Kotkan-Haminan seudun koulutuskuntayhtymä
Koulutuskeskus Salpaus
Koulutuskuntayhtymä Brahe
Koulutuskuntayhtymä OSAO
Koulutuskuntayhtymä Tavastia
Kouvolan kaupunki
KPMG IT Sertifiointi Oy
Kristinestad - Kristiinankaupunki
Kronoby kommun - Kruunupyyn kunta

Kuhmoisten kunta
Kuhmon kaupunki
Kuluttajariitalautakunta
Kumlinge kommun
Kuntaliitto
Kuopion kaupunki
Kuortaneen kunta
Kurikan kaupunki
Kustavin kunta
Kuusamon kaupunki
Kymenlaakson hyvinvointialue
Kymenlaakson käräjäoikeus
Kymenlaakson liitto
Kyyjärven kunta
Kårkulla kuntayhtymä
Kärkölän kunta
Kärsämäen kunta
Kökar kommun
LAB-ammattikorkeakoulu
LAB-ammattikorkeakoulu
Lahden kaupunki
Laihian kunta
Laitilan kaupunki
Lapin aluehallintavirasto
Lapin ammattikorkeakoulu
Lapin ELY-keskus
Lapin hyvinvointialue
Lapin Jätehuolto kuntayhtymä
Lapin käräjäoikeus
Lapin liitto
Lapin poliisilaitos
Lapin TE-toimisto
Lapin yliopisto
Lapinjärven kunta - Lappträsk kommun
Lapinlahden kunta
Lappajärven kunta
Lappeenrannan kaupunki
Lapsiasiavaltuutettu
Lapuan kaupunki
Larsmo kommun - Luodon kunta
Laukaan kunta
Laurea-ammattikorkeakoulu
Leader Pohjoisin Lappi
Lemin kunta
Lemlands kommun
Lempäälän kunta
Leppävirran kunta
Lestijärven kunta
Liedon kunta
Lieksan kaupunki
Liikenne- ja viestintäministeriö

Limingan kunta
Liperin kunta
Lohjan kaupunki - Lojo stad
Loimaan kaupunki
Lopen kunta
Lounais-Hämeen koulutuskuntayhtymä
Lounais-Suomen aluehallintovirasto
Lounais-Suomen koulutuskuntayhtymä
Lounais-Suomen poliisilaitos
Loviisan kaupunki - Lovisa stad
Luhangan kunta
Lumijoen kunta
Lumparlands kommun
Luonnonvarakeskus
LUT-yliopisto
Luumäen kunta
Länsi-Suomen aluehallintovirasto
Länsi-Uudenmaan hyvinvointialue
Länsi-Uudenmaan koulutuskuntayhtymä
Länsi-Uudenmaan käräjäoikeus
Länsi-Uudenmaan poliisilaitos
Maa- ja metsätalousministeriö
Maahanmuuttovirasto
Maanmittauslaitos
Maanpuolustuskorkeakoulu
Malax kommun - Maalahden kunta
Mariehamns stad
Markkinaoikeus
Marttilan kunta
Maskun kunta
Merijärven kunta
Merikarvian kunta
Meriturva
Metropolia Ammattikorkeakoulu
Metsähallitus
Metsäkeskus
Miehikkälän kunta
Mikkelin kaupunki
Muhoksen kunta
Multian kunta
Muonion kunta
Museovirasto
Muuramen kunta
Mynämäen kunta
Myrskylän kunta - Mörskom kommun
Mäntsälän kunta
Mänttä-Vilppulan kaupunki
Mäntyharjun kunta
Naantalin kaupunki
Nakkilan kunta
Navielektro Ky

Niuvaniemen sairaala
Nivalan kaupunki
Nixu Certification Oy
Nokian kaupunki
NordLab
Nousiaisten kunta
Novia
Nurmeksen kaupunki
Nurmijärven kunta
Nykarleby stad - Uusikaarlepyyn kaupunki
Närpes stad - Närpiön kaupunki
Oikeusministeriö
Oikeusrekisterikeskus
Omnia
Onnettomuustutkintakeskus
Opetus- ja kulttuuriministeriö
Opetushallitus
Opintotuen muutoksenhakulautakunta
Oppimis- ja ohjauskeskus Valteri
Optima samkommun
Orimattilan kaupunki
Oripään kunta
Oriveden kaupunki
Oulaisten kaupunki
Oulun ammattikorkeakoulu
Oulun kaupunki
Oulun käräjäoikeus
Oulun poliisilaitoa
Oulun yliopisto
Oulunkaaren kuntayhtymä
Outokummun kaupunki
Padajoen kunta
Paimion kaupunki
Paltamon kunta
Pargas stad - Paraisten kaupunki
Parikkalan kunta
Parkanon kaupunki
Pedersöre kommun - Pedersören kunta
Pelastusopisto
Pelkosenniemen kunta
Pellon kunta
Perhon kunta
Peruspalvelukuntayhtymä Selänne
Petäjäveden kunta
Piceasoft Oy
Pieksämäen kaupunki
Pielaveden kunta
Pihtiputaan kunta
Pirkanmaan ELY-keskus
Pirkanmaan hyvinvointialue
Pirkanmaan käräjäoikeus

Pirkanmaan liitto
Pirkanmaan TE-toimisto
Pirkkalan kunta
Pohjanmaan ELY-keskus
Pohjanmaan hyvinvointialue
Pohjanmaan käräjäoikeus
Pohjanmaan liitto
Pohjanmaan poliisilaitos
Pohjanmaan TE-toimisto
Pohjoisen Keski-Suomen ammattiopisto
Pohjois-Karjalan ELY-keskus
Pohjois-Karjalan hyvinvointialue
Pohjois-Karjalan käräjäoikeus
Pohjois-Karjalan maakuntaliitto
Pohjois-Karjalan TE-toimisto
Pohjois-Pohjanmaan ELY-keskus
Pohjois-Pohjanmaan hyvinvointialue
Pohjois-Pohjanmaan liitto
Pohjois-Pohjanmaan TE-toimisto
Pohjois-Savon ELY-keskus
Pohjois-Savon hyvinvointialue
Pohjois-Savon hyvinvointialue
Pohjois-Savon käräjäoikeus
Pohjois-Savon TE-toimisto
Pohjois-Suomen aluehallintovirasto
Pohjois-Suomen hallinto-oikeus
Pohjois-Suomen oikeusapu
Poliisiammattikorkeakoulu
Poliisihallitus
Polvijärven kunta
Pomarkun kunta
Porin kaupunki
Pornaisten kunta
Porvoon kaupunki - Borgå stad
Posion kunta
PRH
Pudasjärven kaupunki
Pukkilan kunta
Punkalaitumen kunta
Puolangan kunta
Puolustusministeriö
Puolustusvoimat
Puumalan kunta
Pyhtään kunta - Pyttis kommun
Pyhäjoen kunta
Pyhäjärven kaupunki
Pyhännän kunta
Pyhärannan kunta
Päijät-Hämeen hyvinvointialue
Päijät-Hämeen käräjäoikeus
Päijät-Hämeen liitto

Pälkäneen kunta
Pöytyän kunta
Raahen kaupunki
Raahen sairaala
Rahoitusvakausvirasto
Raision kaupunki
Raision seudun koulutuskuntayhtymä
Rajavartiolaitos
Rantasalmen kunta
Ranuan kunta
Raseborg stad - Raaseporin kaupunki
Rauman kaupunki
Rautalammin kunta
Rautavaaran kunta
Rautjärven kunta
Reaktor Innovations Oy
Reisjärven kunta
Riihimäen kaupunki
Rikosseuraamusalan koulutuskeskus
Rikosseuraamuslaitos
Ristijärven kunta
Riveria
Rovaniemen hovioikeus
Rovaniemen kaupunki
Rovaniemen koulutuskuntayhtymä
Ruokolahden kunta
Ruoveden kunta
Ruskon kunta
Rääkkylän kunta
Saamelaisalueen koulutuskeskus
Saarijärven kaupunki
Saimaan ammattiopisto Sampo
Sallan kunta
Salon kaupunki
Salon seudun koulutuskuntayhtymä
Saltviks kommun
Samiedu
SASKY koulutuskuntayhtymä
Sastamalan kaupunki
Satakunnan ammattikorkeakoulu
Satakunnan ELY-keskus
Satakunnan hyvinvointialue
Satakunnan käräjäoikeus
Satakunnan TE-toimisto
Satakuntaliitto
Sauvon kunta
Savitaipaleen kunta
Savon koulutuskuntayhtymä
Savonia-ammattikorkeakoulu
Savonlinnan kaupunki
Savukosken kunta

Seinäjoen ammattikorkeakoulu
Seinäjoen kaupunki
Seinäjoen koulutuskuntayhtymä
Sievin kunta
Siikaisten kunta
Siikajoen kunta
Siikalatvan kunta
Siilinjärven kunta
Simon kunta
Sipoon kunta - Sibbo kommun
Sisäministeriö
Sisä-Suomen poliisilaitos
Siuntion kunta - Sjundeå kommun
Sodankylän kunta
Soinin kunta
Someron kaupunki
Sonkajärven kunta
Sosiaali- ja terveysministeriö
Sosiaaliturva-asioiden muutoksenhakulautakunta
Sotkamon kunta
Sottunga kommun
Sulkavan kunta
Sunds kommun
Suojelupoliisi
Suomalais-venäläinen kouku
Suomen Akatemia
Suomen riistakeskus
Suomen ympäristökeskus
Suomenlinna
Suomussalmen kunta
Suonenjoen kaupunki
Svenska Österbottens Förbund för Utbildning och Kultur
Sysmän kunta
Säkylän kunta
Säteilyturvakeskus
Taideyliopisto
Taipalsaaren kunta
Taiteen edistämiskeskus
Taivalkosken kunta
Taivassalon kunta
Tammelan kunta
Tampereen ammattikorkeakoulu
Tampereen kaupunki
Tampereen kaupunkiseudun kuntayhtymä
Tampereen yliopisto
Tasa-arvovaltuutettu
Tasavallan presidentin kanslia
Teknologiateollisuus ry
Terveyden ja hyvinvoinnin laitos
Tervolan kunta
Tervon kunta

Teuvan kunta
Tiedusteluvalvontavaltuutetun toimisto
Tietosuojavaltuutetun toimisto
Tilastokeskus
Tl. Kosken kunta
Tohmajärven kunta
Toholammin kunta
Toivakan kunta
Tornion kaupunki
Traficom
Tuki- ja osaamiskeskus Eskoo
Tulli
Tuomioistuinvirasto
Turun ammattikorkeakoulu
Turun hallinto-oikeus
Turun hovioikeus
Turun kaupunki - Åbo stad
Turun yliopisto
Tuusniemen kunta
Tuusulan kunta
Tyrnävän kunta
Työ- ja elinkeinoministeriö
Työterveyslaitos
Työtuomioistuin
Ulkoministeriö
Ulkopoliittinen instituutti
Ulosottolaitos
Ulosottolaitos
Ulvilan kaupunki
uokavirasto
Urjalan kunta
urvallisuus- ja kemikaalivirasto
Utajärven kunta
Utsjoen kunta
Uudenmaan ELY-keskus
Uudenmaan liitto
Uudenmaan tTE-toimisto
Uuraisten kunta
Uusikaupunki
Vaalan kunta
Vaalijalan kuntayhtymä
Vaasan ammattikorkeakoulu
Vaasan hallinto-oikeus
Vaasan hovioikeus
Vaasan kaupunki - Vasa stad
Vaasan yliopisto
Vakuutusoikeus
Valkeakosken kaupunki
Valtakunnansyyttäjä
Valtakunnanvoudin kanslia
Valtiokonttori

Valtion koulukodit
Valtion taloudellinen tutkimuskeskus
Valtion talous- ja henkilöstöhallinnon palvelukeskus
Valtion tieto- ja viestintätekniikkakeskus
Valtioneuvoston kanslia
Valtioneuvoston oikeuskansleri
Valtiontalouden tarkastusvirasto
Valtiovarainministeriö
Valvira
Vanhan Vaasan sairaala
Vanhusasiavaltuutetun toimisto
Vantaan ammattiopisto Varia
Vantaan ja Keravan hyvinvointialue
Vantaan kaupunki - Vanda stad
Varastokirjasto
Varkauden kaupunki
Varsinais-Suomen ELY-keskus
Varsinais-Suomen hyvinvointialue
Varsinais-Suomen hyvinvointialue
Varsinais-Suomen käräjäoikeus
Varsinais-Suomen liitto
Varsinais-Suomen TE-toimisto
Vehmaan kunta
Verohallinto
Vesannon kunta
Vesilahden kunta
Vetelin kunta
Vieremän kunta
Vihdin kunta
Viitasaaren kaupunki
Vimpelin kunta
Virolahden kunta
Virtain kaupunki
Vuoksi
Vårdö kommun
Väylävirasto
Vörå kommun - Vöyrin kunta
Yhdenvertaisuusvaltuutettu
Ylioppilastutkintolautakunta
Ylitornion kunta
Ylivieskan kaupunki
Ylä-Savon ammattiopisto
Ylöjärven kaupunki
Ympäristöministeriö
Ypäjän kunta
Åbo Akademi
Ähtärin kaupunki
Äänekosken kaupunki

Arviointilain muutokset/ Ändringarna i bedömningslagen

Huomiot ehdotetusta soveltamisalan laajenemisesta varautumisen arviointiin sekä muutoksen mahdollisista vaikutuksista/ Kommentarer om föreslaget att utvidga tillämpningsområdet så att det omfattar bedömningen av beredskapen och om ändringarnas konsekvenser:

Klikkaa ja lisää otsikko avoimelle kysymykselle

Huomiot ehdotetuista arviointimenettelyjä koskevista muutoksista sekä uusista viranomaisia koskevista arviointivelvollisuuksista ja niiden vaikutuksista organisaatiosi toimintaan (3–3 c §)/ Kommentarer om de föreslagna ändringarna i bedömningsförfarandena och om de nya bedömningsskyldigheterna för myndigheterna samt konsekvenserna av dessa för din organisation (3–3 c §):

Klikkaa ja lisää otsikko avoimelle kysymykselle

Huomiot ehdotetuista arviointiviranomaistehtävien ja tiedonsaanti- ja tarkastusoikeuksien muutoksista (3 d–6 §)/ Kommentarer om de föreslagna ändringarna i bedömningsmyndigheternas uppgifter och rätt att få information och utföra inspektioner (3 d–6 §):

Klikkaa ja lisää otsikko avoimelle kysymykselle

Huomiot ehdotetusta uudesta turvallisuuskriittisten ratkaisujen ja niiden valmistuksen arviointien kokonaisuudesta/ Kommentarer om de nya bestämmelserna om bedömningen av säkerhetskritiska lösningar och produktionen av dem:

Klikkaa ja lisää otsikko avoimelle kysymykselle

Huomiot ehdotetuista siirtymäsäännöksistä ja -ajoista/ Kommentarer om de föreslagna övergångsbestämmelserna och övergångstiderna:

Klikkaa ja lisää otsikko avoimelle kysymykselle

Muut arviointilakia koskevat huomiot, pyydämme yksilöimään pykälän/ Övriga kommentarer om bedömningslagen (specificera vilken paragraf som avses):

Klikkaa ja lisää otsikko avoimelle kysymykselle

Arviointilaitoslain muutokset/ Ändringarna i lagen om bedömningsorgan

Huomiot ehdotetusta tietoturvallisuuden arviointilaitosten luotettavuuden varmistamista koskevista muutoksista (4–5 §)/ Kommentarer om de föreslagna ändringarna angående säkerställandet av tillförlitligheten hos bedömningsorganen för informationssäkerhet (4–5 §):

Klikkaa ja lisää otsikko avoimelle kysymykselle

Huomiot ehdotetusta tietoturvallisuuden arviointilaitosten lisäpätevyyksien hyväksymisprosessista (5 § 3 mom)/ Kommentarer om processen för godkännande av bedömningsorganens specialbehörigheter (5 § 3 mom.):

Klikkaa ja lisää otsikko avoimelle kysymykselle

Muut arviointilaitoslakia koskevat huomiot, pyydämme yksilöimään pykälän/ Övriga kommentarer om lagen om bedömningsorgan (specificera vilken paragraf som avses):

Klikkaa ja lisää otsikko avoimelle kysymykselle

Huomiot esityksen vaikutusten arvioinnista/ Kommentarer om bedömningen av propositionens konsekvenser:

Klikkaa ja lisää otsikko avoimelle kysymykselle

Huotari Maarit
Valtiovarainministeriö

Kalliotie Marika
Valtiovarainministeriö

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

ESITYKSEN PÄÄASIALLINEN SISÄLTÖ

Esityksessä ehdotetaan muutettavaksi 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 ja 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. Muiden 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, ellei 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.

Lait on tarkoitettu tulemaan voimaan x.x.2026

SISÄLLYS

ESITYKSEN PÄÄASIALLINEN SISÄLTÖ 1
PERUSTELUT 3
1 Asian tausta ja valmistelu 3
1.1 Tausta 3
1.2 Valmistelu 3
2 Nykytila ja sen arviointi 4
2.1 Viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arviointi 4
2.2 Salaustuotteiden ja muiden turvallisuuskriittisten ratkaisujen arviointi 11
2.3 Tietoturvallisuuden arviointilaitokset 12
2.4 Euroopan unionin oikeus 14
3 Tavoitteet 16
4 Ehdotukset ja niiden vaikutukset 16
4.1 Keskeiset ehdotukset 16
4.2 Pääasialliset vaikutukset 18
4.2.1 Taloudelliset vaikutukset 18
4.2.1.1 Yritykset 18
4.2.2 Muut ihmisiin kohdistuvat ja yhteiskunnalliset vaikutukset 20
4.2.2.1 Viranomaiset 20
4.2.2.2 Kansallinen turvallisuus 24
4.2.2.3 Tietoyhteiskunta 25
5 Muut toteuttamisvaihtoehdot 25
5.1 Vaihtoehdot ja niiden vaikutukset 25
5.2 Ulkomaiden lainsäädäntö ja muut ulkomailla käytetyt keinot 27
6 Lausuntopalaute 29
7 Säännöskohtaiset perustelut 30
7.1 Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista 30
7.2 Laki tietoturvallisuuden arviointilaitoksista 49
7.3 Turvallisuusselvityslaki 56
8 Lakia alemman asteinen sääntely 57
9 Voimaantulo 57
10 Suhde perustuslakiin ja säätämisjärjestys 58
LAKIEHDOTUKSET 63
viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annetun lain muuttamisesta 63
tietoturvallisuuden arviointilaitoksista annetun lain muuttamisesta 71
turvallisuusselvityslain 18 ja 48 § muuttamisesta 76
LIITE 77
RINNAKKAISTEKSTIT 77
viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annetun lain muuttamisesta 77
tietoturvallisuuden arviointilaitoksista annetun lain muuttamisesta 91
turvallisuusselvityslain 18 ja 48 § muuttamisesta 99

PERUSTELUT

1 Asian tausta ja valmistelu

1.1 Tausta

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

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

Suomen 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 säädösvalmistekohteita. Tähän perustuen työryhmä valmisteli lainsäädännön muutosehdotukset hallituksen esityksen muotoon. Työryhmän hallituksen esityksen luonnos valmistui 23.9.2025. Esitykseen sisältyviä lainsäädännön muutosehdotuksia käsiteltiin työryhmän julkiselle hallinnolle 9.9.2025 ja yritysten edustajille 11.9.2025 järjestetyissä 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 xx.xx.xxxx – xx.xx.xxxx. Lausuntoa pyydettiin: [Täydennetään lausuntokierroksen jälkeen]

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 §:än, 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 ja muita kansainvälisiä tietoturvallisuusvelvoitteita koskee laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004) sekä Pohjois-Atlantin sopimuksen osapuolten välillä tehty sopimus tietoturvallisuudesta ja sen nojalla annetut turvallisuussäännöt (SopS 55–56/2023).

Muuttuneessa turvallisuustilanteessa voisi kuitenkin olla perusteltua, että sektorikohtaisen ja kansainvälisiin tietoturvallisuusvelvoitteisiin liittyvien arviointivelvollisuuksia 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 liittyy 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. 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 säädetyn tietoaineistojen ja tietojärjestelmien riskiarviointiin perustuvista velvollisuuksista 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 Valviran rekisteriin merkittyjä tietojärjestelmiä ja käyttöympäristöjä on 99. Vuonna 2023 Valviran 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 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

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

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 (706/2014) ja arviointilaissa. Arviointilain 3 § mukaan Liikenne- ja viestintävirasto on nykytilassa ainoa viranomainen, joka toteuttaa arviointilain mukaisia viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arviointeja. Liikenne- ja 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 (1190/2023).

Arviointilain 4 §:n 3 momentin mukaan Liikenne- ja viestintävirasto suorittaa tehtävänsä käytettävissään olevien voimavarojen mukaisesti ottaen huomioon kansainvälisten tietoturvallisuusvelvoitteiden noudattamisen sekä pyydettyjen toimenpiteiden merkityksen viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden yleiseen parantamiseen. Nykytilassa Liikenne- ja viestintävirasto priorisoi viranomaisten kansainvälisiin tietoturvallisuusvelvoitteisiin liittyviä arviointipyyntöjä ja yritysturvallisuusselvityksiin liittyviä turvallisuusselvityslain mukaisia Suojelupoliisin tai Puolustusvoimien Pääesikunnan pyyntöjä sekä 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. Pääesikunta on myös sopinut Liikenne- ja viestintäviraston kanssa eräiden sellaisten salausteknisen materiaalin jakeluun ja hallintaan liittyvien tehtävien hoitamisesta, joiden hoitamiseen Puolustusvoimilla on toimivat menettelyt. 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 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. 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 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 kansallisesti 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 tai muutoin kansainvälisten velvoitteiden sitä edellyttäessä. 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 turvallisuussäännöissä 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. 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 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 ja hyväksytystä tuotteesta viraston verkkosivuilla ylläpidetylle listalle. Hyväksyttyjen tuotteiden 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 arviointeja voivat tietoturvallisuuden arviointilaitoksilta hankkia. 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 säädetä tietoturvallisuuden arviointilaitokseksi hakeutuvan yrityksen sijaintivaltiosta. Tietoturvallisuuden arviointilaitoksen henkilökunnan luotettavuudesta ei säädetä ja tietoturvallisuuden arviointilaitoksen mahdollisuus hankkia henkilöturvallisuusselvitys työntekijöistä on ollut tulkinnanvarainen tai se ei ole ollut mahdollista, jolloin jokainen arviointilaitoksen viranomaisasiakas on joutunut hankkimaan turvallisuusselvityksen tietojärjestelmiään tai tietoliikennejärjestelyjään arvioivista arviointilaitoksen työntekijöistä. 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.

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 on selvityksen perustana olleiden arviointiperusteiden mukainen. Todistuksessa tulee yksilöidä arvioinnissa käytetyt tietoturvallisuuden arviointiperusteet ja arvioinnin laajuus. Arviointiraportista ei säädetä erikseen, mutta arviointitoiminnan käytäntöihin ja akkreditoituun pätevyyteen kuuluu asianmukainen dokumentointi. Asiakastietolaissa ja toisiolaissa säädetään velvollisuudesta hankkia tietyille toiminnoille hyväksytyn tietoturvallisuuden arviointilaitoksen todistus. Näissä laeissa säädetään myös todistuksen voimassaolosta, ylläpidosta ja peruuttamisesta.

Arviointilaitoslain 13 §:ssä säädetään hyvää hallintoa koskevien säännösten, 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), Sosiaali- ja terveysalan lupa- ja valvontaviraston (Valvira), Sosiaali- ja terveysalan tietolupaviranomaisen (Findatan) 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 toimivallan jakautumista ja sitä koskevia 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) artiklan 1 mukaan asetuksen kohde on sisämarkkinoiden asianmukaisen toiminnan varmistaminen ja kyberturvallisuuden, kyberresilienssin ja luottamuksen korkea taso unionissa. Tässä tarkoituksessa asetuksessa vahvistetaan kehys kyberturvallisuuden sertifiointijärjestelmien perustamiselle tieto- ja viestintätekniikan tuotteille, palveluille ja prosesseille sekä tietoturvapalveluille. Kehyksillä vältetään sisämarkkinoiden hajautuminen kyberturvallisuuden sertifiointijärjestelmien osalta. Asetus ei 1 artiklan 2 alakohdan mukaan rajoita jäsenvaltioiden toimivaltaa yleisen turvallisuuden, puolustuksen ja kansallisen turvallisuuden alalla eikä yksittäistä valtiota koskevan rikosoikeuden toimissa.

Ensimmäisenä sertifiointijärjestelmänä on vastikään komission täytäntöönpanosäädöksellä (EU) 2024/482 annettu EU:n Common Criteria -skeema (EUCC). Skeema soveltuu esimerkiksi älykorttien ja tietoturvabokseilla varustettujen laitteiden, allekirjoituksen luontivälineiden,

sähköisesti luettavien matkustusasiakirjojen ja ajopiirtureiden sertifiointiin. Valmistelussa ovat muun ohessa pilvipalveluita (EUCS, European Union Cybersecurity Certification Scheme for Cloud Services) ja 5G-verkkoja koskevat sertifiointiskeemat. Mahdollisia tulevia työkohteita ovat komission työohjelman mukaan (Work Programme for European cybersecurity certification, SWD (2024) 7.2.2024) digitaalisen identiteetin lompakkosovellus, tietoturvallisuuden hallintapalvelut ja yleisesti 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.

Euroopan unionin sääntely mahdollistaa jäsenvaltioiden kansallisen 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 EU:n sisämarkkinoita koskeva sertifiointisääntely ei näyttäisi estävän vaatimusten ja arviointimenettelyjen asettamista näihin tarkoituksiin kansallisen sääntelyn mukaisesti ja kansainvälisten tietoturvallisuusvelvoitteiden mukaisesti.

3 Tavoitteet

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

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

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

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

4 Ehdotukset ja niiden vaikutukset

4.1 Keskeiset ehdotukset

Viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen arviointi laajennettaisiin koskemaan tietoturvallisuuden lisäksi varautumista 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. Puolustusvoimille 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 valtionhallinon 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, millä edellytyksillä tietoturvallisuuden arviointilaitos voisi käyttää arviointitehtäviensä suorittamisessa alihankkijaa. Julkiseen hallintotehtävään liittyvien hallinnon yleislakien luetteloa täydennettäisiin vastaamaan nykytilaa ja lakiin lisättäisiin säännös rikosoikeudellisesta virkavastuusta. Ehdotetaan myös, että arviointilaitoksen tulisi olla Suomeen sijoittautunut oikeushenkilö.

Tietoturvallisuuden arviointilaitoksen arviointipätevyyden osoittamisen menettelyjä joustavoitettaisiin. Pätevyysalue liittyisi aina arviointilaitoslain 10 §:ssä säädetyn arviointiperusteen kuten säädöksen, ohjeen tai standardin tuntemukseen. Ehdotetaan, 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.[1] Valtion tieto- ja viestintätekniikkakeskus Valtori käyttää turvallisuusverkkoasetuksen sekä valtiovarainministeriön määräyksen ja ohjeistuksen perusteella turvallisuusluokkiin IV ja III luokiteltuja tietoja käsittelevien tietojärjestelmien ja tietoliikennejärjestelyjen arviointeihin tieturvallisuuden 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 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

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

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.[2] Arviointien toteuttamisesta aiheutuvien kustannusten hillitsemiseksi valtionhallinnon 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[2].

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

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

tiedonhallinnan muutoksen lausuntomenettelyyn, mikä helpottaa tietoturvallisuuden arviointien toteuttamista.

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.

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 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.

Tietojärjestelmän tai tietoliikennejärjestelyn arvioinnin laajentamisella niihin kuuluvan turvallisuuskriittisen ratkaisun tietoturvallisuuden ja varautumisen arviointiin ei ole välitöntä resurssivaikutusta Liikenne- ja viestintävirastolle tai Puolustusvoimille. 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. 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 nykyisellääänkin vastuuhenkilöiden henkilöturvallisuusselvityksiä ja voi lausua toimitiloista, mutta tehtävä laajentuisi yrityksen luotettavuuteen ja seurantaan.

FINASin tehtäviin voisi vähäisessä määrin vaikuttaa se, että tietoturvallisuuden arviointilaitoksen lisäpätevyyden hakeminen ja myöntäminen tulisi arviointilaitoslaissa mahdolliseksi ilman FINASin akkreditointia. Mahdollisuus koskisi vain lisäpätevyyksiä ja tietoturvallisuuden arviointilaitoksen hyväksynnän edellytys olisi jatkossakin jokin soveltuva FINASin akkreditoima pätevyys, kuten pätevyys tietoturvallisuuden johtamisjärjestelmän sertifiointiin standardin ISO/IEC 27001 mukaan. Lisäpätevyyksien hyväksyntä Liikenne- ja viestintäviraston päätöksellä ilman FINASin akkreditointia ei vaikuttaisi FINASin tehtäviin tai vastuisiin, sillä näiden lisäpätevyyksien seuranta kuuluisi kokonaisuudessaan Liikenne- ja

viestintäviraston ohjaus- ja valvontatoiminnan vastuulle. Arviointilaissa ehdotettuun hajasäteilysuojaus- eli TEMPEST-yritysten hyväksyntään mahdollisesti sisällytettävä akkreditointi voisi tuoda FINASille vain vähäisiä lisätehtäviä ottaen huomioon TEMPEST-yritysten pieni lukumäärä.

Arviointilaitoslakiin ehdotettu Liikenne- ja viestintäviraston velvollisuus pyytää lausuntoa pätevyyden hyväksymisen kannalta keskeisiltä viranomainsilta 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 välttämään. Hyvä tietoturvallisuus ja häiriönsietokyky minimoivat tietovuotojen sekä aineellisten ja aineettomien omaisuuksien menetyksiä ja tietojärjestelmän käytön keskeytymisestä aiheutuvia haittoja. Tietojärjestelmien tietoturvallisuuden ja varautumisen arvioinnin parantuessa haitallisten vaikutusten aiheuttaminen viranomaisten toiminnan kannalta keskeisille palveluille vaikeutuu ja kallistuu.

4.2.2.2 Kansallinen turvallisuus

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

Tietoturvallisuuden ja varautumisen arviointi parantaa yleisesti tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuutta ja 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.

Puolustushallinnon 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.

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.

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 15 §:n mukaisesti lähtökohtana on, että selvitystä voi hakea se, jonka suojattavasta edusta on kysymys. Vain taho, jonka etua suojataan, voi arvioida mahdollisten ilmoitettavien tietojen merkityksen suhteessa tehtävässä suojattavaan etuun. Vaikka tietoturvallisuuden arviointilaitoksille annettaisiin turvallisuusselvityslain systematiikasta 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 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

[täydennetään lausuntokierroksen jälkeen]

7 Säännöskohtaiset perustelut

7.1 Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista

1 § *Soveltamisala.* Lain soveltamisalaa laajennettaisiin siten, että lain *1 momenttiin* lisättäisiin varautumisen arviointi sekä turvallisuuskriittisen ratkaisujen 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 muuten voimassa olevaa 2 momenttia, mutta toimivaltaisen viranomaisen nimeksi muutettaisiin Liikenne- ja viestintävirasto. Kyse on teknisluonteisesta muutoksesta. Liikenne- ja viestintäministeriön hallinnonalalla tehdyn virastouudistuksen myötä Viestintävirasto lakkasi olemasta 1.1.2019 alkaen, ja uutena viestintähallinnon viranomaisena toimii Liikenne- ja viestintävirasto.

2 § *Määritelmät.* Pykälässä säädetään laissa käytetyistä määritelmistä. Pykälää muutettaisiin siten, että sen 2 ja 3 kohdan määritelmät 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.

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. 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. Kyseisessä asetuksessa, eli asiakirjojen turvallisuusluokittelusta valtionhallinnossa annetun valtioneuvoston asetuksen (1101/2019), jäljempänä *turvallisuusluokitteluasetus,* 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.

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 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. Ohjeena voitaisiin esimerkiksi käyttää Tiedonhallintalautakunnan suositusta tietoturvallisuudesta hankinnoissa (2023:57). 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 valtiohallinnon viranomaisille velvollisuus arvioida tietojärjestelmiensä ja tietoliikennejärjestelyjensä tietoturvallisuutta ja varautumista käyttäen 3 §:ssä säädettyjä menettelyjä. Käytettävä menettely tulisi valita riskiarvion perusteella.

Valtionhallinnon viranomainen valitsisi riskiarvioinnin perusteella millä menettelyllä tietojärjestelmien ja tietoliikennejärjestelyjen turvallisuutta ja varautumista arvioidaan, kuka on arvioinnin toteuttaja, mitä vaatimuksia ja kriteerejä arvioinnissa käytetään, ja miten arvioinneista huolehditaan tietojärjestelmän ja tietoliikennejärjestelyn elinkaaren ajan. Tietojärjestelmän tai tietoliikennejärjestelyn eri osiin tai osa-alueisiin voitaisiin valita erilainen arviointimenettely. Arviointimenettelyä valittaessa voitaisiin huomioida arvioinnin taloudellinen ja tehokas toteuttaminen, arvioitavassa tietojärjestelmässä tai tietoliikennejärjestelyssä käsiteltävien tietojen luottamuksellisuus-, eheys-, saatavuus- ja jatkuvuudenhallintavaatimukset sekä salassapitovaatimukset ja turvallisuusluokat, arvioitavan järjestelmän tarkoituksenmukaiseen tuotantotapaan kohdistuvat vaatimukset ja tekninen laajuus, toteutustapa ja liitynnät muihin järjestelmiin sekä ulkopuolisen erityisosaamisen tarve suhteessa viranomaisen käytettävissä oleviin resursseihin. Arviointimenettelyn valintaa rajoittaisivat kuitenkin ehdotetun 3 §:n 2 ja 3 momenteissa säädettäväksi ehdotettujen rajoitteiden lisäksi tämän pykälän 1 ja 2 kohdassa ehdotetut arviointivelvollisuudet.

Pykälän *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.

Pykälän *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 hankittamatta tietoturvallisuuden arviointilaitoksen arviointia, tulisi päätös tehdä viranomaisen sisäisen ratkaisuvallan mukaisesti, mikä usein edellyttää johdon hyväksyntää.

Pykälän *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.

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 tietoturvallisuuden arviointia.

Pykälän *1 momentissa* säädettäisiin muille kuin valtionhallinnon viranomaiselle ehdotetun 3 a §:n 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 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 *1 kohdan* mukaan kansainvälisistä tietoturvallisuusvelvoitteista annetun lain tarkoittamissa tilanteissa tai pykälän *2 kohdan* mukaan jos muutoin kansainvälinen yhteistyö sitä edellyttää taikka pykälän *3 kohdan* mukaan jos vaatimustenmukaisuuden osoittamisesta erikseen säädetään.

Hyväksynnän tarve ja oikeus hakea hyväksyntää liittyisi kansainvälisistä tietoturvallisuusvelvoitteista tai kansainvälisestä yhteistyöstä johtuvaan tai säädettyyn velvollisuuteen osoittaa tietoturvallisuusvaatimusten täyttyminen riippumattoman arviointielimen toimesta kolmannelle tai kolmansille osapuolille. Esimerkiksi EU:n ja Naton turvallisuusluokitellun tiedon käsittelyyn käytettävät tietojärjestelmät on turvallisuusääntöjen mukaan etukäteen akkreditoitava, ja myös tietyt osa-alueet tai elementit on etukäteen arvioitava ja hyväksyttävä. 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.

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

Pykälän *1 momentissa* säädettäisiin arviointiviranomaisista, joita olisivat Liikenne- ja viestintävirasto ja Pääesikunnan määrätty turvallisuusviranomainen (DSA Designated Security Authority). Liikenne- ja viestintävirasto hoitaa arviointitehtäviä jo voimassa olevan lain nojalla, mutta Pääesikunnan määrätylle turvallisuusviranomaiselle tehtävä olisi uusi. Pääesikunnan määrätyn turvallisuusviranomaisen arviointitehtäviä voisi myös hoitaa sen nimeämä Puolustusvoimien palkattuun henkilöstöön kuuluvaa henkilö. Nimetyt henkilöt olisivat tehtäviä hoitaessaan Pääesikunnan määrätyn turvallisuusviranomaisen ohjauksessa ja valvonnassa. Puolustusvoimien arviointitehtävä on tarpeen säätää nimenomaisesti Pääesikunnan määrätylle turvallisuusviranomaiselle toiminnan riippumattomuuden varmistamiseksi. Pääesikunnan määrätyn turvallisuusviranomaisen tehtävistä säädetään kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa.

Pykälän *2 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 2 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.

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

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

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

Pykälän *1 momenttia* muutettaisiin siten, että siinä säädettäisiin 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 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 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. Momentin *8 kohdan* mukaan huomioon tulisi myös ottaa Liikenne- ja viestintäviraston käytettävissä oleva voimavarat, mikä vastaisi voimassa olevan momentin priorisointiperusteita.

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, 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 työt, 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 3 ja 4 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.

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, mutta myös varmistaa, että Puolustusvoimien erityiset toiminnalliset vaatimukset tulevat tarkoituksenmukaisesti huomioiduiksi.

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 tarkastusoikeus, tiedonsaantioikeus ja 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 koskiviat 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 tai sitä avustavan asiantuntijan tarkastusoikeudesta hajasäteilysuojausratkaisuja tarjoavan valmistajan ehdotetun 4 § 2 momentin 3 kohdassa tarkoitetussa valvonnassa. 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 toiminalle on asetettu tietoturvallisuusvaatimusten rinnalle myös kyberturvallisuusvaatimuksia, jotka olisi tarkoituksenmukaista huomioida osana tietojärjestelmien ja tietoliikennejärjestelyjen arviointeja.

Tiettyjen viranomaisten, kuten valtiovarainministeriön ja kansallisen turvallisuusviranomaisen ohjeiden mainitsemisen sijaan yleisesti viranomaisen ohjeet säädösten soveltamisesta olisi riittävä ja yleispätevämpi määrittely. Viranomaisten tulisi varmistua ohjeistuksen yhdenmukaisuudesta ja yhtenäisyydestä. Näin ollen 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 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 ulkomaisen vaikutuksen riskit.

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

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

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

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

Pykälässä säädettäisiin, että hyväksyttyään turvallisuuskriittisen ratkaisun 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 turvallisuusluokka, jonka mukaisen tiedon suojaamiseen ratkaisu on todettu riittäväksi. Luetteloon merkittäisiin tieto kansallisen turvallisuusluokan perusteella ja tarvittaessa EU:n tai Naton turvallisuusluokan perusteella tehdystä arvioinnista.

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.

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 perumisesta. Lisäksi Viestintävirasto korvattaisiin arviointiviranomaisella, jolloin Liikenne- ja viestintäviraston lisäksi myös Pääesikunnan määrätyllä turvallisuusviranomaisella olisi mahdollisuus peruuttaa tai kumota antamansa hyväksyntäpäätös tai perua antamansa lausunto.

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 Liikenne- ja viestintäviraston sähköiseen viestintään liittyvistä suoritteista perittävistä maksuista annetun asetuksen (1190/2023) 3 §:n kanssa, jonka mukaan Liikenne- ja viestintävirasto perii omakustannusarvon mukaisen maksun muun muassa salaustuotteiden, muiden tietoturvatuotteiden ja tietoliikenneyhteyksiä hyödyntävien tuotteiden turvallisuuden tason arvioinnista, viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista ja siihen liittyvän toimitilojen tietoturvallisuuden arvioinnista sekä todistuksen antamisesta, valtiovarainministeriön pyytämästä tietojärjestelmien tai tietoliikennejärjestelyjen turvallisuutta koskevasta selvityksestä, sähkömagneettiseen hajasäteilyyn liittyvästä arvioinnista sekä luokiteltua tietoa käsittelevien tietojärjestelmien suunnitteluun liittyvästä neuvontapalvelusta.

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

Pykälän 1 momenttiin myös lisättäisiin yhdenmukaisesti arviointilakiin ehdotetun kanssa, että 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* muutettaisiin 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 4 kohtaan* lisättäisiin tietoturvallisuuden arviointilaitoksen hyväksymisen edellytykseksi se, että laitoksen yritysturvallisuusselvityksestä ei ole ilmennyt mitään estettä, mikä kokonaisharkinnan perusteella vaarantaisi yrityksen tai vastuuhenkilöiden luotettavuuden tai sitoumustenhoitokyvyn arviointitehtävässä. Lisäksi 1 momentin 4 kohtaan lisättäisiin edellytys siitä, että laitoksella on luotettavaksi arvioitu ja valvottu menetelmä, jolla henkilökunnan luotettavuus varmistetaan. Arviointilaitoksella tulisi olla prosessit ja ohjeistus henkilöstöturvallisuudesta huolehtimiseksi. Henkilöstöturvallisuudella tarkoitetaan menettelyjä, joilla varmistetaan henkilöiden tietoturvavastuut ja velvollisuudet, tietoturvaosaaminen ja taustatarkastukset sekä avainhenkilöriskien hallinta. Lisäksi nämä

menettelyt kattavat väärinkäytösten estämistä, kuten vaarallisten työyhdistelmien tunnistamista ja välttämistä, työtehtäväkiertoa, sekä työsuhteen tai sopimuksen päättymisen. 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 *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 (920/2005) 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. 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.

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 koskisi Liikenne- ja viestintäviraston lisäksi, sen toimeksiannosta toimivan asiantuntijan sijaan, sitä avustavaa asiantuntijaa. Muutos vastaisi 4 §:n 2 momenttiin ehdotettavaa mahdollisuutta antaa vain avustavia tehtäviä ulkopuoliselle asiantuntijalle. Avustavassa tehtävässä toimivaa ulkopuolista asiantuntijaa voitaisiin käyttää tietoturvallisuuden arviointilaitoksen 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 arviointiperustetta ohjaavalta tai valvovalta viranomaiselta, arviointilaitokselta

tai sen asiakkaalta saatavia tietoja, jotka voivat olla salassa pidettäviä esimerkiksi liikesalaisuutena tai arviointilaitoksen asiakkaana olevien viranomaisten turvallisuusjärjestelyjä tai varautumista koskevina tietoina.

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

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

Alihankintana voitaisiin teettää vain sellaisia toimia, joissa hyväksytyllä 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.

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

Momentin *2 kohta* vastaisi nykyistä 3 kohtaa, mutta siihen lisättäisiin Suomen Nato-jäsenyyden myötä Euroopan unionin lisäksi Pohjois-Atlantin liitto säännösten tai ohjeiden mahdollisena antajana. Momentin 1 kohdan tavoin myös 2 kohtaan lisättäisiin tietoturvallisuuden lisäksi kyberturvallisuus ja varautuminen. Vaikka arviointiperusteina säädetään kansainvälisistä lähteistä, 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 Liikenne- ja viestintäviraston sähköiseen viestintään liittyvistä suoritteista perittävistä maksuista annetun asetuksen (1190/2023) 5 §:n kanssa, jonka mukaan Liikenne- ja viestintävirasto voi periä maksun jälkikäteisvalvontaan liittyvästä olennaisesta suoritteesta, tietoturvallisuuden arviointilaitosten hyväksyntään liittyvien toimenpiteiden lisäksi. Lisäksi pykälään tehtäisiin tekninen muutos, jossa Viestintävirasto muutettaisiin Liikenne- ja viestintävirastoksi.

12 § *Muutoksenhaku.* Pykälästä poistettaisiin viittaus kumottuun hallintolainkäyttölakiin (586/1996) ja lisättäisiin viittaus oikeudenkäynnistä hallintoasioissa annettuun lakiin (808/2019). 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). Voimassa olevan lain ja sen perustelujen mukaisesti (HE 45/2011 vp) hallinnon yleislakien soveltamista ei ole sidottu julkisen hallintotehtävän hoitamiseen, vaan niitä sovelletaan kaikkiin arviointilain mukaisten hyväksytyn tietoturvallisuuden arviointilaitosten tehtävien hoitamiseen.

Pykälään lisättäisiin uusi *2 momentti*, jossa säädettäisiin tietoturvallisuuden arviointilaitosten vastuuhenkilöiden ja palveluksessa olevien henkilöiden sekä alihankkijoiden palveluksessa olevaan 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

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

9 Voimaantulo

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

Arviointilakia koskevat muutokset sisältäisivät siirtymäsäännöksiä, koska lain voimaantullessa kaikilla viranomaisilla ei ole valmiuksia tai mahdollisuuksia välittömästi soveltaa uutta lakia ja noudattaa sen säännöksiä. Viranomaisilla on käytössä huomattava määrä eri aikoina käyttöönotettuja tietojärjestelmiä ja tietoliikennejärjestelyitä, joiden tietoturvallisuuden arviointimenettelyjen saattamisen 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 tämän lain 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 mitään estettä, mikä 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.

Julkinen hallintotehtävä

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

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

mukaisesti arviointitehtäviä ulkoistettaisiin Teknologian tutkimuskeskus VTT Oy:lle käytännössä silloin, kun arviointi vaatisi sellaista teknistä erityisosaamista ja -resursseja, joihin arviointiviranomaisen ei ole mahdollista tai tarkoituksenmukaista resursoida.

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

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

Elinkeinovapaus

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

Arviointilain 3 a §:ssä säädettäisiin uudistetuista arviointimenettelyistä, joihin lisättäisiin arviointimenettelyiksi viranomaisen toteuttama itsearviointi ja viranomaisen toimeksiannosta palveluntarjoajan toteuttama arviointi voimassa olevan lain mukaisten arviointimenettelyiden, eli tietoturvallisuuden arviointilaitoksen ja arviointiviranomaisen tekemän arvioinnin lisäksi. Esityksen tarkoituksena on parantaa arviointien sujuvuutta ja saatavuutta avaamalla arviointitoiminta tietyiltä osin myös yksityisille palveluntarjoajille. Viranomaisen toimeksiannosta toimivan palveluntarjoajan kannalta sääntely on merkityksellinen myös perustuslain 18 §:n 1 momentissa säädetyn elinkeinovapauden näkökulmasta. Arviointilain ehdotettu muutos mahdollistaisi uutta liiketoimintaa arviointipalveluita tarjoaville yrityksille. Toisaalta palveluntarjoajien toteuttamat arvioinnit rajattaisiin tietojärjestelmiin, joissa käsitellään julkisia, salassa pidettäviä ja korkeintaan turvallisuusluokkaan IV luokiteltuja tietoja. Rajoitus perustuisi siihen, että turvallisuusluokitellun tiedon käsittelyyn liittyvät korkeammat tiedon suojaamisvaatimukset, rajatummat käyttöoikeudet sekä suuremmat riskit, jos tieto oikeudettomasti paljastauisi. Palveluntarjoajien on lisäksi mahdollista hakea tietoturvallisuuden arviointilaitoksiksi, jos ne haluaisivat arvioida turvallisuusluokkaan III luokiteltuja tietoja käsitteleviä tietojärjestelmiä ja tietoliikennejärjestelyjä.

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

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

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

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

Tiedonsaantioikeudet

Perustuslakivaliokunta on käytännössään katsonut, että salassapitosäännösten edelle menevässä tietojensaantioikeudessa on viime kädessä kysymys siitä, että tietoihin oikeutettu viranomainen omine tarpeineen syrjäyttää ne perusteet ja intressit, joita tietoja hallussaan pitävään

viranomaiseen kohdistuvalla salassapitovelvollisuudella suojataan. Perustuslakivaliokunta on lisäksi tietojen saamista ja luovuttamista koskevaa sääntelyä perustuslain 10 §:n 1 momentissa säädetyn yksityiselämän ja henkilötietojen suojan kannalta arvioidessaan kiinnittänyt huomiota muun muassa siihen, mihin ja ketä koskeviin tietoihin tiedonsaantioikeus ulottuu ja miten tietojensaantioikeus sidotaan tietojen välttämättömyyteen. Tällöin tietojensaanti- ja luovuttamismahdollisuus on voinut liittyä jonkin tarkoituksen kannalta ”tarpeellisiin tietoihin”, jos tarkoitetut tietosisällöt on pyritty luettelemaan laissa tyhjentävästi. Jos taas tietosisältöjä ei ole samalla tavoin luetteloitu, sääntelyyn on pitänyt sisällyttää vaatimus ”tietojen välttämättömyydestä” jonkin tarkoituksen kannalta (mm. PeVL 10/2014 vp, s. 6/II, PeVL 19/2012 vp, s. 3—4 ja PeVL 62/2010 vp, s. 4/I).

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

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

Kotirauha

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

Omaisuudensuoja

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

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

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

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

Ponsi

Edellä esitetyn perusteella annetaan eduskunnan hyväksyttäviksi seuraavat lakiehdotukset:

1.

Laki

viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti

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

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

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

1 §

Lain soveltamisala

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

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

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

2 §

Määritelmät

Tässä laissa tarkoitetaan:

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

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

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

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

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

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

7) *tietoturvallisuuden arviointilaitoksella* tietoturvallisuuden arviointilaitoksista annetussa laissa (1405/2011) tarkoitettua yritystä, yhteisöä tai viranomaista, jonka Liikenne- ja viestintävirasto on mainitun lain mukaisesti hyväksynyt;

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

9) *turvallisuuskriittisellä ratkaisulla* salausratkaisua, hajasäteilysuojausratkaisua 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) arviointiviranomaisen toteuttama arviointi.

Viranomainen voi toteuttaa arvioinnin 1 momentin 2 kohdan mukaisella menettelyllä vain, kun 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, kun 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 §:ssä 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, ellei se päätä arvioinnin pyytämisen tai hankkimisen olevan tietojärjestelmän tai tietoliikennejärjestelyn riskiarvioinnin perusteella tarpeetonta; ja

3) toteutettava aina vähintään itsearviointi.

3 b §

Muiden kuin valtionhallinnon viranomaisten arviointivelvollisuudet

Muun kuin 3 a §:ssä tarkoitetun viranomaisen on arvioitava tietojärjestelmänsä tai tietoliikennejärjestelynsä, jossa käsitellään turvallisuusluokkaan I tai II luokiteltuja tietoja 3 a §:n 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 kohdassa tarkoitetulla tavalla, ellei 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 annetun lain tai mainitun lain tarkoittaman kansainvälisen tietoturvallisuusvelvoitteen tarkoittamassa tilanteessa;

2) jos muutoin kansainvälinen yhteistyö sitä edellyttää; tai

3) jos vaatimustenmukaisuuden osoittamisesta erikseen säädetään.

3 d §

Arviointiviranomaiset

Arviointiviranomaisia ovat Liikenne- ja viestintävirasto ja 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.

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

Arvioinnin tekeminen kuuluu Pääesikunnan määrätyn turvallisuusviranomaisen toimivaltaan, jos arviointi koskee Puolustusvoimien tietojärjestelmien tai tietoliikennejärjestelyjen taikka niihin kuuluvien turvallisuuskriittisten ratkaisujen tietoturvallisuutta ja varautumista.

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

3) tiedon turvallisuusluokka;

4) muun riippumattoman arvioinnin saatavuus;

5) suomalaisten turvallisuuskriittisten ratkaisujen tarjonnan edistäminen;

6) arvioinnin pyytäjien ja hakijoiden yhdenvertainen kohtelu;

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

8) Liikenne- ja viestintäviraston käytettävissä oleva voimavarat.

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 3 ja 4 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 ja 4 a §:ssä tarkoitetulla sitä avustavalla ulkopuolisella asiantuntijalla on oikeus tehdä hajasäteilysuojausratkaisun valmistajan ja sen alihankkijan tiloissa tarkastus sen selvittämiseksi, noudattavatko valmistaja ja sen alihankkija tämän lain nojalla annettuja päätöksiä. Liikenne- ja viestintäviraston ja sitä avustavan ulkopuolisen asiantuntijan oikeuteen päästä tiloihin ja saada tutkittavakseen välttämättömät tiedot sekä suorittaa arviointitoimenpiteitä sovelletaan, mitä 1 momentissa säädetään. Tässä momentissa tarkoitetusta tarkastuksesta säädetään hallintolain (434/2003) 39 §:ssä.

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

7 §

Tietoturvallisuuden ja varautumisen arviointiperusteet

Tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden ja varautumisen 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 ja ohjeita sekä viranomaisten ohjeita niiden soveltamisesta;

3) julkaistuja ja yleisesti tai alueellisesti sovellettuja tietototurvallisuutta, 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 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 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 §:n mukaisesta pyynnöstä hyväksyntäpäätöksen tai -lausunnon, kun 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 c §

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) turvallisuusluokka, jonka mukaisen tiedon 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 ratkaisun tekemistä kuultava päätöksen tai lausunnon saanutta sekä varattava tälle tilaisuus korjata puute.

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

11 §

Muutoksenhaku

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

12 §

Maksut

Arviointiviranomaisen arvioinnista 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 x 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 3 a §:n 1 kohdassa säädettyä kahden vuoden kuluessa lain voimaantulosta ja 3 a §:n 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 3 b §:n 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 §, 5 §:n 1, 3 ja 4 momentti, 6–8 §, 3 luvun otsikko, 9–13 § ja 13 a §, sellaisena kuin niistä on 4 § osaksi laissa 727/2014 ja 13 a § laissa 727/2014, sekä

lisätään 3 lukuun uusi 9 a § ja 5 §:n uusi 5 momentti seuraavasti:

1 Luku

Yleiset säännökset

1 §

Lain tarkoitus

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

2 §

Lain soveltamisala

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

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

2 Luku

Arviointilaitoksen hyväksyminen ja valvonta

3 §

Arviointilaitoksen hyväksymistä koskeva hakemus

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

— —

4 §

Hakemuksen käsittely

Liikenne- ja viestintäviraston on ennen tietoturvallisuuden arviointilaitoksen hyväksymistä varattava suojelupoliisille tilaisuus lausua arviointilaitoksen vastuuhenkilöiden luotettavuudesta ja sen toimitilojen turvallisuudesta. Jos hakemus koskee turvallisuusluokitellun tiedon käsittelyn arvioinnin pätevyysaluetta, Liikenne- ja viestintäviraston tulee yrityksen ja sen vastuuhenkilöiden luotettavuuden ja sitoumustenhoitokyvyn varmistamiseksi hakea yrityksestä 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:

— —

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;

— —

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

Liikenne- ja viestintävirasto hyväksyy saamiensa ja laatimiensa selvitysten sekä suorittamiensa tarkastusten perusteella vaatimukset täyttävän laitoksen hyväksytyksi tietoturvallisuuden arviointilaitokseksi. Tällainen laitos voi markkinoinnissaan ja muussa viestinnässään käyttää Liikenne- ja viestintäviraston hyväksymistä koskevaa ilmaisua edellyttäen, ettei hyväksymisen voimassaoloa koskeva määräaika ole päättynyt tai Liikenne- ja viestintävirasto ole päättänyt peruuttaa 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 ja sitä avustavalla asiantuntijalla on oikeus tarkastaa hyväksyntää hakevan ja hyväksytyn tietoturvallisuuden arviointilaitoksen ja sen 9 a §:ssä tarkoitetun alihankkijan tilat sekä sen käytössä olevat menetelmät. 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 käytetyistä arviointiperusteista, arvioinnin laajuudesta ja havainnoista.

Hyväksytty tietoturvallisuuden arviointilaitos voi pyynnöstä, tai jos niin erikseen säädetään antaa selvitysten ja tarkastuksen perusteella todistuksen, jos arvioitava kohde on selvityksen

perustana olleiden arviointiperusteiden mukainen. Todistuksessa tulee yksilöidä arvioinnissa käytetyt tietoturvallisuuden ja varautumisen arviointiperusteet ja arvioinnin laajuus sekä voimassaoloaika.

9 a §

Alihankinta

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

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

10 §

Tietoturvallisuuden ja varautumisen arviointiperusteet

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

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

2) Euroopan unionin, Pohjois-Atlantin liiton tai muun kansainvälisen toimielimen antamia tietoturvallisuutta, kyberturvallisuutta tai varautumista koskevia säännöksiä ja ohjeita 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.

4 Luku

Erinäiset säännökset

11 §

Maksut

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

12 §

Muutoksenhaku

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

13 §

Virkavastuuta ja hyvää hallintoa koskevien säännösten soveltaminen

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

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. Hyväksynnän 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 x 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:

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 x päivänä -kuuta 2026.

_____

Helsingissä x.x.20xx

Pääministeri

Etunimi Sukunimi

..ministeri Etunimi Sukunimi

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 a ja 8 b §, sellaisina kuin ne ovat laissa 728/2014,
muutetaan 1–8 ja 9–12 §, sellaisena kuin niistä 1 § on osaksi laissa 728/2014, sekä
lisätään lakiin uusi 3 a–3 d, 4 a, 4 b, 7 a ja 8 c § 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 annetun lain (588/2004) mukaisen kansainvälisen tietoturvallisuusvelvoitteen edellyttämään erityissuojattavan tietoaineiston käsittelyyn tarkoitetun tietojärjestelmän, tietoliikennejärjestelyn ja turvallisuuskriittisen ratkaisun ja sen valmistuksen tietoturvallisuuden arviointiin, jollei kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa toisin säädetä tai mainitun lain mukaisesta kansainvälisestä tietoturvallisuusvelvoitteesta muuta johdu.* *Liikenne- ja viestintäviraston* tehtävistä yritysturvallisuusselvitystä laadittaessa säädetään turvallisuusselvityslaissa (726/2014).
2 §	2 §
Määritelmät	*Määritelmät*
Tässä laissa tarkoitetaan:	Tässä laissa tarkoitetaan:

Voimassa oleva laki

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

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 pykälän 4 momentin nojalla annetussa valtioneuvoston asetuksessa tarkoitettua turvallisuusluokkaa;

9) turvallisuuskriittisellä ratkaisulla salausratkaisua, hajasäteilysuojausratkaisua 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.

Voimassa oleva laki

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.

Ehdotus

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) arviointiviranomaisen toteuttama arviointi.

Viranomainen voi toteuttaa arvioinnin 1 momentin 2 kohdan mukaisella menettelyllä vain, kun 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, kun 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 §:ssä tarkoitettuja menettelyjä. Valtionhallinnon viranomaisen on valittava arviointimenettely tietojärjestelmän tai tietoliikennejärjestelyn riskiarvioinnin perusteella, kuitenkin siten, että sen on:

1) pyydettävä arviointiviranomaisen arviointi tietojärjestelmälleen tai

Voimassa oleva laki | *Ehdotus*

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, ellei se päätä arvioinnin pyytämisen tai hankkimisen olevan tietojärjestelmän tai tietoliikennejärjestelyn riskiarvioinnin perusteella tarpeetonta; ja

3) toteutettava aina vähintään itsearviointi.

3 b §

Muiden kuin valtionhallinnon viranomaisten arviointivelvollisuudet

Muun kuin 3 a §:ssä tarkoitetun viranomaisen on arvioitava tietojärjestelmänsä tai tietoliikennejärjestelynsä, jossa käsitellään turvallisuusluokkaan I tai II luokiteltuja tietoja 3 a §:n 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 kohdassa tarkoitetulla tavalla, ellei 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 annetun lain tai mainitun lain tarkoittaman kansainvälisen

Voimassa oleva laki

Ehdotus

tietoturvallisuusvelvoitteen tarkoittamassa tilanteessa;

2) jos muutoin kansainvälinen yhteistyö sitä edellyttää; tai

3) jos vaatimustenmukaisuuden osoittamisesta erikseen säädetään.

3 d §

Arviointiviranomaiset

Arviointiviranomaisia ovat Liikenne- ja viestintävirasto ja 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.

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

Arvioinnin tekeminen kuuluu Pääesikunnan määrätyn turvallisuusviranomaisen toimivaltaan, jos arviointi koskee Puolustusvoimien tietojärjestelmien tai tietoliikennejärjestelyjen taikka niihin kuuluvien turvallisuuskriittisten ratkaisujen tietoturvallisuutta ja varautumista.

4 §

Viestintäviraston tehtävät

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

4 §

***Arviointiviranomaisen** tehtävät*

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

Voimassa oleva laki

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

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

3) tiedon turvallisuusluokka;

4) muun riippumattoman arvioinnin saatavuus;

5) suomalaisten turvallisuuskriittisten ratkaisujen tarjonnan edistäminen;

6) arvioinnin pyytäjien ja hakijoiden yhdenvertainen kohtelu;

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

8) Liikenne- ja viestintäviraston käytettävissä oleva voimavarat.

Edellä 1 momentissa tarkoitetun pyynnön Liikenne- ja viestintävirastolle voi viranomaisen toimeksiannosta tehdä myös se, joka tekee viranomaisen lukuun hankintoja taikka tuottaa tietojenkäsittely- tai

Voimassa oleva laki | *Ehdotus*

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 3 ja 4 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

Voimassa oleva laki

5 §

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.

6 §

Viestintäviraston tiedonsaantioikeus ja 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 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.

Ehdotus

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

Voimassa oleva laki

7 §

Tietoturvallisuuden arviointiperusteet

Viestintävirasto voi käyttää viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arviointiperusteina:

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

Ehdotus

hallinnollisia ja teknisiä arviointitoimenpiteitä.

Liikenne- ja viestintävirastolla ja 4 a §:ssä tarkoitetulla sitä avustavalla ulkopuolisella asiantuntijalla on oikeus tehdä hajasäteilysuojausratkaisun valmistajan ja sen alihankkijan tiloissa tarkastus sen selvittämiseksi, noudattavatko valmistaja ja sen alihankkija tämän lain nojalla annettuja päätöksiä. Liikenne- ja viestintäviraston ja sitä avustavan ulkopuolisen asiantuntijan oikeuteen päästä tiloihin ja saada tutkittavakseen välttämättömät tiedot sekä suorittaa arviointitoimenpiteitä sovelletaan, mitä 1 momentissa säädetään. Tässä momentissa tarkoitetusta tarkastuksesta säädetään hallintolain (434/2003) 39 §:ssä.

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

7 §

Tietoturvallisuuden ja varautumisen arviointiperusteet

Tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden *ja varautumisen 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 ja ohjeita sekä viranomaisten ohjeita niiden soveltamisesta;*

3) julkaistuja ja yleisesti tai alueellisesti sovellettuja tietototurvallisuutta, kyberturvallisuutta tai varautumista koskevia säännöksiä, määräyksiä tai ohjeita;

4) vahvistettuun standardiin sisältyviä tietoturvallisuutta, kyberturvallisuutta tai varautumista koskevia vaatimuksia.

Voimassa oleva laki	*Ehdotus*
tietoturvallisuutta koskevat vaatimukset, jotka on otettu arviointiperusteeksi. Arviointi voidaan tehdä myös osittaisena.	
	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 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 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 §	8 §

Voimassa oleva laki

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 a §

Viranomaisen velvollisuus hankkia todistus

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.

8 b §

Ehdotus

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 §:n mukaisesta pyynnöstä hyväksyntäpäätöksen tai -lausunnon, kun 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.

(kumotaan)

Voimassa oleva laki	*Ehdotus*
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)
	8 c § *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) turvallisuusluokka, jonka mukaisen tiedon 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 **tason** 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, sekä sallittava Viestintävirastolle pääsy tietojärjestelmiin ja tietoliikennejärjestelyihin	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.*

Voimassa oleva laki	*Ehdotus*
sen selvittämiseksi, täyttävätkö ne edelleen todistuksen mukaiset vaatimukset.	
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. Viestintäviraston on ennen 1 momentissa tarkoitetun ratkaisun tekemistä kuultava todistuksen 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 peruuttaa 8 §:ssä tarkoitetun lausunnon tai päätöksen kokonaan tai osittain, jos arvioinnin kohteena ollut tietojärjestelmä, tietoliikennejärjestely tai turvallisuuskriittinen ratkaisu taikka turvallisuuskriittisen ratkaisun* valmistaja ei enää täytä niitä vaatimuksia, jotka ovat olleet edellytyksenä päätöksen tai lausunnon antamiselle. *Arviointiviranomaisen* on ennen 1 momentissa tarkoitetun ratkaisun tekemistä kuultava *päätöksen tai lausunnon saanutta* sekä varattava tälle tilaisuus korjata puute. *Arviointiviranomainen* voi 1 momentissa tarkoitetussa päätöksessään määrätä, että päätöstä on noudatettava muutoksenhausta huolimatta, jollei muutoksenhakuviranomainen toisin määrää.
11 §	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.*
	_____
	Tämä laki tulee voimaan x päivänä -kuuta 2026. *Valtionhallinnon viranomaisen on saatettava tietojärjestelmiensä ja*

Voimassa oleva laki	*Ehdotus*
	tietoliikennejärjestelyjensä tietoturvallisuuden ja varautumisen arviointi vastaamaan 3 a §:ssä säädettyä viiden vuoden kuluessa tämän lain voimaatulosta, kuitenkin siten, että arviointi on saatettava vastaamaan 3 a §:n 1 kohdassa säädettyä kahden vuoden kuluessa lain voimaantulosta ja 3 a §:n 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 3 b §:n 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 §, 5 §:n 1, 3 ja 4 momentti, 6–8 §, 3 luvun otsikko, 9–13 § ja 13 a §, sellaisena kuin niistä on 4 § osaksi laissa 727/2014 ja 13 a § laissa 727/2014, sekä

lisätään 3 lukuun uusi 9 a § ja 5 §:n uusi 5 momentti 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 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 *Suomeen sijoittautuneisiin* elinkeinonharjoittajiin ja palvelutehtäviä julkishallinnolle tarjoaviin yksiköihin, jotka toimeksiannosta arvioivat *tietoturvallisuuden tason taikka tietojärjestelmän tai tietoliikennejärjestelyn varautumisen tasoa* (***tietoturvallisuuden arviointilaitos***) ja jotka haluavat toiminnalleen *Liikenne- ja viestintäviraston* hyväksynnän. Lisäksi tätä lakia sovelletaan hyväksymismenettelyyn. *Arviointiviranomaisten* tehtävistä viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden *ja varautumisen* arvioinnissa sekä yritysturvallisuusselvitysten laadinnassa säädetään erikseen.

Voimassa oleva laki

2 Luku

Arviointilaitoksen hyväksyminen ja valvonta

3 §

Arviointilaitoksen hyväksymistä koskeva hakemus

Tietoturvallisuuden arviointilaitos voi hakea Viestintäviraston hyväksyntää toimintaansa varten.

— — — — — — — — — — — — — — —

4 §

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.

5 §

Ehdotus

2 Luku

Arviointilaitoksen hyväksyminen ja valvonta

3 §

Arviointilaitoksen hyväksymistä koskeva hakemus

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

— — — — — — — — — — — — — — —

4 §

Hakemuksen käsittely

Liikenne- ja viestintäviraston on ennen tietoturvallisuuden arviointilaitoksen hyväksymistä varattava suojelupoliisille tilaisuus lausua arviointilaitoksen vastuuhenkilöiden luotettavuudesta ja sen toimitilojen turvallisuudesta. *Jos hakemus koskee turvallisuusluokitellun tiedon käsittelyn arvioinnin pätevyysaluetta, Liikenne- ja viestintäviraston tulee yrityksen ja sen vastuuhenkilöiden luotettavuuden ja sitoumustenhoitokyvyn varmistamiseksi hakea yrityksestä 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 §

Voimassa oleva laki	*Ehdotus*
Arviointilaitoksen hyväksyminen	*Arviointilaitoksen hyväksyminen*
Tietoturvallisuuden arviointilaitoksen hyväksymisen edellytyksenä on, että:	Tietoturvallisuuden arviointilaitoksen hyväksymisen edellytyksenä on, että:
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
4)laitoksen vastuuhenkilöiden luotettavuus on varmistettu ja laitoksella on luotettavaksi arvioitu ja valvottu menetelmä, jonka avulla laitoksen toimitilojen ja tietojenkäsittelyn turvallisuus varmistetaan;	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;
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
	Sen estämättä mitä 2 momentissa säädetään, hyväksytyn arviointilaitoksen hakiessa hyväksyntää uudelle pätevyysalueelle voi Liikenne- ja viestintävirasto päättää vaatimusten täyttymisestä kuultuaan pätevyyden hyväksymisen kannalta keskeisiä viranomaisia.
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.	*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.	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 §	6 §

Voimassa oleva laki

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.

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.

8 §

Arviointilaitoksen tiedonanto- ja ilmoitusvelvollisuus

Ehdotus

Arviointilaitoksen hyväksymisen peruuttaminen

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

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

7 §

Liikenne- ja viestintäviraston tiedonsaanti ja tarkastusoikeus

Liikenne- ja viestintävirastolla ja sitä avustavalla asiantuntijalla on oikeus tarkastaa hyväksyntää *hakevan ja* hyväksytyn tietoturvallisuuden arviointilaitoksen *ja sen 9 a §:ssä tarkoitetun alihankkijan* tilat sekä sen käytössä olevat menetelmät. 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***

Voimassa oleva laki	*Ehdotus*
Hyväksytyn tietoturvallisuuden arviointilaitoksen on ilmoitettava Viestintävirastolle sellaisesta toimintaansa koskevasta muutoksesta, jolla on merkitystä laitosta koskevien velvoitteiden kannalta.	Hyväksytyn tietoturvallisuuden arviointilaitoksen on *ilmoitettava Liikenne- ja 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.	
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:	Hyväksytyn tietoturvallisuuden arviointilaitoksen on saamaansa tietoturvallisuuden *ja varautumisen* arviointitehtävää suorittaessaan noudatettava huolellisuutta ja pidettävä huolta siitä, että arvioinnin aikana:
1)tarkastetaan arvioinnin kohteen toimitilat;	1) tarkastetaan *tarvittaessa* 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).	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.	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 laadittava arviointiraportti, johon merkitään tiedot käytetyistä arviointiperusteista, arvioinnin laajuudesta ja havainnoista.* *Hyväksytty tietoturvallisuuden arviointilaitos voi pyynnöstä, tai jos niin erikseen säädetään* antaa selvitysten ja tarkastuksen perusteella todistuksen, jos arvioitava *kohde on selvityksen perustana olleiden arviointiperusteiden mukainen. Todistuksessa tulee yksilöidä arvioinnissa käytetyt tietoturvallisuuden ja varautumisen*

Voimassa oleva laki

Ehdotus

arviointiperusteet ja arvioinnin laajuus sekä voimassaoloaika.

9 a §

Alihankinta

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

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

10 §

Tietoturvallisuuden 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;

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;

10 §

Tietoturvallisuuden ja varautumisen arviointiperusteet

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

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

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

3) *julkaistuja ja yleisesti tai alueellisesti sovellettuja tietoturvallisuutta, kyberturvallisuutta tai varautumista koskevia säännöksiä, määräyksiä tai ohjeita;*

Voimassa oleva laki	*Ehdotus*
5)vahvistettuun standardiin sisältyviä tietoturvallisuutta koskevia vaatimuksia.	4) *vahvistettuun standardiin sisältyviä tietoturvallisuutta, kyberturvallisuutta tai varautumista koskevia vaatimuksia.*
4 luku	4 Luku
Erinäiset säännökset	**Erinäiset säännökset**
11 §	11 §
Maksut	*Maksut*
Tietoturvallisuuden arviointilaitoksen hyväksymistä koskevan asian käsittelystä Viestintävirastossa perittävästä maksusta säädetään valtion maksuperustelaissa (150/1992) ja sen nojalla.	Tietoturvallisuuden arviointilaitoksen hyväksymistä *ja valvontaa* koskevan asian käsittelystä *Liikenne- ja viestintävirastossa peritään maksu noudattaen, mitä valtion maksuperustelaissa (150/1992) säädetään*.
12 §	12 §
Muutoksenhaku	*Muutoksenhaku*
Muutoksenhausta Viestintäviraston tämän lain nojalla tekemään päätökseen säädetään hallintolainkäyttölaissa (586/1996).	Muutoksenhausta *Liikenne- ja viestintäviraston* tämän lain nojalla tekemään päätökseen säädetään *oikeudenkäynnistä hallintoasioissa annetussa laissa (808/2019).*
13 §	13 §
Hyvää hallintoa koskevien säännösten soveltaminen	*Virkavastuuta ja hyvää hallintoa koskevien säännösten soveltaminen*
Hyväksytyn tietoturvallisuuden arviointilaitoksen on tässä laissa tarkoitettuja tehtäviä hoitaessaan noudatettava hallintolakia (434/2003), viranomaisten toiminnan julkisuudesta annettua lakia (621/1999) *sekä* kielilakia (423/2003).	Hyväksytyn tietoturvallisuuden arviointilaitoksen on tässä laissa tarkoitettuja tehtäviä hoitaessaan noudatettava hallintolakia (434/2003), viranomaisten toiminnan julkisuudesta annettua lakia (621/1999), kielilakia (423/2003*), saamen kielilakia (1086/2003), tietosuojalakia (1050/2018) sekä sähköisestä asioinnista viranomaistoiminnassa annettua lakia (13/2003).* *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.*

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

13 a §

Turvallisuusselvitysrekisteriin merkittävät tiedot

Liikenne- ja viestintävirasto merkitsee turvallisuusselvityslaissa tarkoitettuun turvallisuusselvitysrekisteriin tiedot hyväksytyistä *tietoturvallisuuden* arviointilaitoksista samoin kuin arviointilaitokselle annettuun todistukseen merkityt tiedot. Hyväksynnän 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 x 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 .
