Laki

julkisen hallinnon tiedonhallinnasta annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan julkisen hallinnon tiedonhallinnasta annetun lain (906/2019) 2 §:n 16 kohta, 3 § ja 10 §:n 1 momentin 2 kohta, sellaisina kuin niistä ovat 2 §:n 16 kohta laissa 488/2023 ja 3 § osaksi laeissa 653/2021 ja 488/2023, sekä

lisätään 1 §:ään siitä lailla 710/2021 kumotun 2 momentin tilalle uusi 2 momentti ja 2 §:ään, sellaisena kuin se on osaksi laissa 488/2023, uusi 17—25 kohta sekä lakiin uusi 4 a luku seuraavasti:

1 §

Lain tarkoitus

— —

Tällä lailla pannaan täytäntöön toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta annetun Euroopan parlamentin ja neuvoston direktiivin (EU) 2022/2555 (*NIS 2 -direktiivi*) toimijaa koskevia velvoitteita, niiden noudattamisen valvontaa ja seuraamuksia koskevat säännökset NIS 2 -direktiivin liitteen I kohdassa 10 tarkoitetulla julkishallinnon toimialalla (*julkishallinnon toimiala*). NIS 2 -direktiivin täytäntöönpanosta muilta osin säädetään kyberturvallisuuslaissa (/).

2 §

Määritelmät

Tässä laissa tarkoitetaan:

— —

16) *käsittelysäännöillä* luonnollisen henkilön ennalta laatimia automaattisen tietojenkäsittelyn ohjaamiseen tarkoitettuja sääntöjä;

17) *viestintäverkolla ja tietojärjestelmällä*18) *viestintäverkon ja tietojärjestelmän turvallisuudella* viestintäverkon ja tietojärjestelmien kykyä suojautua tietyllä varmuudella tapahtumilta, jotka saattavat vaarantaa niissä tarjottavien tai niiden välityksellä saatavilla olevien tallennettujen, siirrettyjen tai käsiteltyjen tietojen taikka palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden;

a) eurooppalaisesta sähköisen viestinnän säännöstöstä annetun Euroopan parlamentin ja neuvoston direktiivin (EU) 2018/1972 2 artiklan 1 kohdassa tarkoitettua sähköistä viestintäverkkoa;

b) laitetta taikka yhteen kytkettyjen tai toisiinsa yhteydessä olevien laitteiden ryhmää, joista yksi tai useampi suorittaa ohjelman avulla digitaalisten tietojen automaattista käsittelyä; ja

c) digitaalisia tietoja, joita a ja b alakohdassa tarkoitetuissa järjestelmissä säilytetään, käsitellään, haetaan tai siirretään näiden järjestelmien toimintaa, käyttöä, suojausta tai ylläpitoa varten;

HE 57/2024 vp
LiVM 1/2025 vp
EV 15/2025 vp

19) *kyberturvallisuudella* toimia, joita tarvitaan viestintäverkkojen ja tietojärjestelmien, niiden käyttäjien ja muiden asianosaisten henkilöiden suojaamiseksi kyberuhilta;

20) *kyberuhkalla* tilannetta, tapahtumaa tai toimintaa, joka toteutuessaan voi vahingoittaa tai häiritä viestintäverkkoja ja tietojärjestelmiä, tällaisten järjestelmien käyttäjiä ja muita henkilöitä tai muulla tavoin vaikuttaa näihin haitallisesti;

21) *merkittävällä kyberuhkalla* kyberuhkaa, jonka voidaan sen teknisten ominaisuuksien perusteella olettaa vaikuttavan mahdollisesti vakavasti viranomaisen verkko- ja tietojärjestelmiin tai sen palvelujen käyttäjiin aiheuttamalla huomattavaa aineellista tai aineetonta vahinkoa;

22) *kyberriskillä* poikkeaman aiheuttamien menetysten tai häiriön mahdollisuutta, joka ilmaistaan menetyksen tai häiriön suuruuden ja poikkeaman toteutumisen todennäköisyyden yhdistelmänä;

23) *poikkeamalla* tapahtumaa, joka vaarantaa viestintäverkoissa ja tietojärjestelmissä tarjottavien tai niiden välityksellä saatavilla olevien tallennettujen, siirrettyjen tai käsiteltyjen tietojen taikka palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden;

24) *merkittävällä poikkeamalla* poikkeamaa, joka:

a) on aiheuttanut tai voi aiheuttaa vakavan palvelujen toimintahäiriön tai viranomaiselle huomattavia taloudellisia tappioita; tai

b) on vaikuttanut tai voi vaikuttaa luonnollisiin henkilöihin tai oikeushenkilöihin aiheuttamalla huomattavaa aineellista tai aineetonta vahinkoa;

25) *poikkeaman käsittelyllä* toimia ja menettelyjä, joilla pyritään ehkäisemään ja havaitsemaan poikkeama, analysoimaan, rajoittamaan tai hallitsemaan sitä ja palautumaan siitä.

3 §

Lain soveltamisala ja sen rajaukset

Tätä lakia sovelletaan tiedonhallintaan ja tietojärjestelmien käyttöön, kun viranomaiset käsittelevät tietoaineistoja, jollei muualla laissa toisin säädetä. Tämän lain 6 a lukua sovelletaan *automaattisen ratkaisumenettelyn* käyttöönottoon ja käyttöön. Mitä tässä laissa säädetään viranomaisesta, sovelletaan myös yliopistolaissa (558/2009) tarkoitettuihin yliopistoihin ja ammattikorkeakoululaissa (932/2014) tarkoitettuihin ammattikorkeakouluihin.

Asiankäsittelyssä ja palvelujen tuottamisessa noudatettavista menettelyistä, salassapidosta ja tiedonsaantioikeudesta viranomaisten asiakirjoihin sekä asiakirjojen arkistoinnista säädetään erikseen. Tiedonhallinnasta ja tietojärjestelmien käytöstä Suomen evankelis-luterilaisessa kirkossa säädetään kirkkolaissa (652/2023).

Tämän lain 4 a lukua ei sovelleta seuraaviin viranomaisiin ja viranomaisen toimintaan:

1) tasavallan presidentin kanslia, eduskunnan virastot, Puolustusvoimat, poliisin hallinnosta annetussa laissa (110/1992) tarkoitetut poliisiyksiköt, Rajavartiolaitos, Syyttäjälaitos ja Tullin rikostorjunta;

2) tuomioistuimet ja valitusasioita käsittelemään perustetut lautakunnat;

3) Puolustuskiinteistöt;

4) kunnalliset viranomaiset lukuun ottamatta Helsingin kaupunkia, johon sovelletaan 4 a lukua sen hoitaessa hyvinvointialueiden järjestämisvastuulle lailla säädettyjä tehtäviä;

5) Suomen Pankki;

6) yliopistolaissa tarkoitetut yliopistot, ammattikorkeakoululaissa tarkoitetut ammattikorkeakoulut, Pelastusopisto sekä muut valtion opetus- ja koulutusalan laitokset;

7) julkisen hallinnon turvallisuusverkkotoiminnasta annetussa laissa (10/2015) tarkoitettu turvallisuusverkon palvelutuotanto ja turvallisuusverkon palvelujen käyttö;

8) viranomaiset, jotka on perustettu yhdessä Euroopan talousalueeseen kuulumattoman maan kanssa kansainvälisen sopimuksen mukaisesti ja näissä maissa sijaitsevat diplomaattiset edustustot ja konsuliedustustot sekä näiden verkko- ja tietojärjestelmät, siltä osin kuin tällaiset

järjestelmät sijaitsevat edustuston tiloissa tai niitä ylläpidetään näissä maissa olevia käyttäjiä varten.

Tämän lain 19, 20, 26 ja 27 §:ää ei sovelleta tuomioistuimien eikä valitusasioita käsittelemään perustettujen lautakuntien lainkäyttöön. Tämän lain 3 lukua ei sovelleta eduskunnan oikeusasiamiehen eikä valtioneuvoston oikeuskanslerin toimintaan, tuomioistuimien eikä valitusasioita käsittelemään perustettujen lautakuntien toimintaan, tasavallan presidentin kansliaan, eduskunnan virastoihin, Kansaneläkelaitokseen, Suomen Pankkiin, muihin itsenäisiin julkisoikeudellisiin laitoksiin, yliopistolaissa tarkoitettuihin yliopistoihin eikä ammattikorkeakoululaissa tarkoitettuihin ammattikorkeakouluihin. Tämän lain 3 lukua sovelletaan hyvinvointialueisiin, hyvinvointiyhtymiin, kuntiin ja kuntayhtymiin niiden hoitaessa laissa säädettyjä tehtäviä. Tämän lain 18 g §:n 3 momenttia ja 18 h—18 l §:ää ei sovelleta eduskunnan oikeusasiamiehen eikä valtioneuvoston oikeuskanslerin toimintaan.

Mitä 4 luvussa, 22—24 ja 25—27 §:ssä sekä 6 a luvussa säädetään tiedonhallintayksiköstä ja viranomaisesta, sovelletaan yksityisiin henkilöihin ja yhteisöihin sekä muihin kuin viranomaisena toimiviin julkisoikeudellisiin yhteisöihin siltä osin kuin ne hoitavat julkista hallintotehtävää. Yksityisiin henkilöihin ja yhteisöihin sekä muihin kuin viranomaisena toimiviin julkisoikeudellisiin yhteisöihin sovelletaan lisäksi, mitä 4 ja 28 §:ssä säädetään tiedonhallintayksiköstä, niiden käyttäessä julkista valtaa viranomaisten toiminnan julkisuudesta annetun lain 4 §:n 2 momentissa tarkoitetulla tavalla tai kun mainittu laki on säädetty erikseen sovellettavaksi niiden toiminnassa. Edelleen yksityisiin yhteisöihin ja muihin kuin viranomaisena toimiviin julkisoikeudellisiin yhteisöihin sovelletaan, mitä 19 §:n 2 momentissa sekä 24 a ja 24 b §:ssä säädetään viranomaisesta niiden käyttäessä julkista valtaa viranomaisten toiminnan julkisuudesta annetun lain 4 §:n 2 momentissa tarkoitetulla tavalla.

Tätä lakia ei sovelleta Ahvenanmaan maakunnassa toimiviin valtion viranomaisiin. Tämän lain 13 a §:ää ja 6 a lukua sovelletaan kuitenkin Ahvenanmaalla toimiviin valtion viranomaisiin niiden hoitaessa sellaisia valtakunnan lainsäädäntövaltaan kuuluvia viranomaistehtäviä, joissa tehdään hallintolain 53 e §:ssä tarkoitettuja asian automaattisia ratkaisuja. Myös 4 a lukua sovelletaan Ahvenanmaan maakunnassa toimiviin valtion viranomaisiin, jollei 3 momentista muuta johdu.

10 §

Julkisen hallinnon tiedonhallintalautakunta

Valtiovarainministeriön yhteydessä toimii julkisen hallinnon tiedonhallintalautakunta (*tiedonhallintalautakunta*), jonka tehtävänä on:

— —

2) edistää tässä laissa säädettyjen tiedonhallinnan ja tietoturvallisuuden menettelytapojen ja tämän lain vaatimusten toteuttamista, lukuun ottamatta 4 a luvussa säädettyä.

— —

4 a luku

Kyberturvallisuutta koskevat velvollisuudet ja niiden noudattamisen valvonta

18 a §

Toimijajaottelu ja toimintaa koskeva ilmoitus

Tämän luvun soveltamisalaan kuuluvat tiedonhallintayksiköt ovat julkishallinnon toimialan keskeisiä toimijoita. Hyvinvointialueet ja hyvinvointiyhtymät sekä Helsingin kaupunki ovat kuitenkin tärkeitä toimijoita.

Tiedonhallintayksikön on ilmoitettava valvovalle viranomaiselle:

1) nimensä;

2) osoitteensa, sähköpostiosoitteensa, puhelinnumeronsa ja muut ajantasaiset yhteystietonsa;

3) IP-osoitealueensa;

4) tieto siitä, onko se julkishallinnon toimialan keskeinen vai tärkeä toimija;

5) luettelo muista Euroopan unionin jäsenvaltioista, joissa se tarjoaa palvelujaan;

6) osallistumisestaan kyberturvallisuuslain 23 §:ssä tarkoitettuun kyberturvallisuustietojen vapaaehtoiseen jakamisjärjestelyyn.

Tiedonhallintayksikön on ilmoitettava kaikista 2 momentissa tarkoitettujen tietojen muutoksista viipymättä, viimeistään kahden viikon kuluttua muutoksesta.

18 b §

Velvollisuus hallita kyberturvallisuusriskejä ja riskienhallinnan toimintamalli

Tiedonhallintayksikön on tunnistettava, arvioitava ja hallittava kyberriskejä, joita kohdistuu sen toiminnoissa tai palveluntarjonnassa käytettävien viestintäverkkojen ja tietojärjestelmien turvallisuuteen. Kyberturvallisuutta koskevalla riskienhallinnalla tulee estää tai minimoida poikkeamien vaikutus toimintaan, toiminnan jatkuvuuteen, palvelujen vastaanottajiin ja muihin palveluihin. Tiedonhallintayksikön on toteutettava 18 c §:ssä tarkoitetut kyberturvallisuutta koskevat riskienhallintatoimenpiteet.

Tiedonhallintayksiköllä on oltava käytössä ajantasainen kyberturvallisuutta koskeva riskienhallinnan toimintamalli viestintäverkkojen ja tietojärjestelmien ja niiden fyysisen ympäristön suojaamiseksi poikkeamilta ja niiden vaikutuksilta. Kyberturvallisuutta koskevassa riskienhallinnan toimintamallissa on tunnistettava viestintäverkkoihin ja tietojärjestelmiin ja niiden fyysiseen ympäristöön kohdistuvat riskit ottaen huomioon kaikki vaaratekijät huomioiva lähestymistapa. Toimintamallissa on määritettävä ja kuvattava kyberturvallisuutta koskevan riskienhallinnan tavoitteet, menettelyt ja vastuut sekä 18 c §:n mukaiset toimenpiteet, joilla viestintäverkkoja ja tietojärjestelmiä ja niiden fyysistä ympäristöä suojataan kyberuhkilta ja poikkeamilta.

Tiedonhallintayksikön johto vastaa kyberturvallisuutta koskevan riskienhallinnan toteuttamisen ja valvonnan järjestämisestä sekä hyväksyy riskienhallinnan toimintamallin ja valvoo sen toteuttamista. Tiedonhallintayksikön johdolla tulee olla riittävä perehtyneisyys kyberturvallisuutta koskevaan riskienhallintaan.

18 c §

Toimenpiteet kyberturvallisuutta koskevien riskien hallinnassa

Tiedonhallintayksikön on toteuttava oikeasuhtaiset tekniset, operatiiviset ja organisatoriset kyberturvallisuutta koskevat riskienhallintatoimenpiteet käyttämiensä viestintäverkkojen ja tietojärjestelmien turvallisuuteen kohdistuvien kyberriskien hallitsemiseksi ja haitallisten vaikutusten estämiseksi tai minimoimiseksi. Kyberturvallisuutta koskevassa riskienhallinnan toimintamallissa ja siihen perustuvissa kyberturvallisuuden riskienhallintatoimenpiteissä on otettava huomioon ja pidettävä yllä ajantasaisesti ainakin:

1) kyberturvallisuutta koskevan riskienhallinnan toimintaperiaatteet ja kyberturvallisuuden riskienhallintatoimenpiteiden vaikuttavuuden arviointi;

2) viestintäverkkojen ja tietojärjestelmien turvallisuutta koskevat toimintaperiaatteet;

3) viestintäverkkojen ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuus sekä tarvittavat menettelyt haavoittuvuuksien käsittelemiseksi ja julkistamiseksi;

4) toimitusketjun välittömien toimittajien tuotteiden ja palveluntarjoajien palvelujen yleinen laatu ja häiriönsietokyky, niihin sisällytetyt kyberturvallisuutta koskevat riskienhallintatoimenpiteet ja välittömien toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt sekä NIS 2 -direktiivin 22 artiklan 1 kohdassa tarkoitetut kriittisiä toimitusketjuja koskevien koordinoitujen riskinarviointien tulokset;

5) omaisuudenhallinta ja sen turvallisuuden kannalta tärkeiden toimintojen tunnistaminen;

6) henkilöstöturvallisuus ja kyberturvallisuuskoulutus;

7) pääsynhallinnan ja todentamisen menettelyt;

8) salausmenetelmien käyttämistä koskevat toimintaperiaatteet ja menettelyt sekä tarvittaessa toimenpiteet suojatun sähköisen viestinnän käyttämiseksi;

9) poikkeamien havainnointi ja käsittely turvallisuuden ja toimintavarmuuden ylläpitämiseksi ja palauttamiseksi;

10) varmuuskopiointi, palautumissuunnittelu, kriisinhallinta ja muu toiminnan jatkuvuuden hallinta sekä tarvittaessa suojattujen varaviestintäjärjestelmien käyttö;

11) perustason tietoturvakäytännöt toiminnan, tietoliikenneturvallisuuden, laitteisto- ja ohjelmistoturvallisuuden ja tietoaineistoturvallisuuden varmistamiseksi;

12) toimenpiteet viestintäverkkojen ja tietojärjestelmien fyysisen ympäristön suojaamiseksi sekä tilaturvallisuuden ja välttämättömien resurssien varmistamiseksi.

Toimenpiteiden on oltava ajantasaiset, asianmukaiset ja oikeasuhtaiset suhteessa tiedonhallintayksikön käyttämien viestintäverkkojen ja tietojärjestelmien riskialttiuteen, viestintäverkon tai tietojärjestelmän merkitykseen tiedonhallintayksikön toiminnalle sekä niissä ilmenevän poikkeaman kohtuudella ennakoitavissa oleviin välittömiin vaikutuksiin. Lisäksi toimenpiteiden mitoittamisessa on otettava huomioon tiedonhallintayksikön koko, sen toiminnan laatu, poikkeaman todennäköisyys ja vakavuus, toimenpiteistä aiheutuvat kustannukset sekä ajantasainen kehitys huomioon ottaen käytettävissä olevat tekniset mahdollisuudet torjua kyberuhka.

Riskienhallinnassa, riskienhallinnan toimintamallissa ja riskienhallintatoimenpiteitä toteutettaessa on noudatettava lisäksi NIS 2 -direktiivin 21 artiklan 5 kohdan nojalla mahdollisesti annettavia Euroopan komission täytäntöönpanosäädöksiä.

18 d §

Ilmoitusvelvollisuus merkittävästä poikkeamasta

Viranomaisen on viipymättä, viimeistään 24 tunnin kuluttua merkittävän poikkeaman havaitsemisesta, toimitettava valvovalle viranomaiselle poikkeamaa koskeva ensi-ilmoitus, jossa on ilmoitettava, epäilläänkö poikkeaman johtuvan rikoksesta taikka muusta lainvastaisesta tai vihamielisestä teosta ja voiko poikkeamalla olla rajat ylittäviä vaikutuksia sekä näiden vaikutusten todennäköisyys.

Viranomaisen on viipymättä, viimeistään 72 tunnin kuluttua merkittävän poikkeaman havaitsemisesta, toimitettava valvovalle viranomaiselle poikkeamaa koskeva jatkoilmoitus, jossa on saatettava ajan tasalle 1 momentissa tarkoitetut tiedot ja esitettävä ensimmäinen arvio merkittävän poikkeaman laadusta, vakavuudesta ja vaikutuksista sekä vaarantumisindikaattorit, jos sellaisia on saatavilla.

Viranomaisen on annettava valvovalle viranomaiselle merkittävää poikkeamaa koskeva loppuraportti kuukauden kuluessa jatkoilmoituksen toimittamisesta. Loppuraportin on sisällettävä:

1) yksityiskohtainen kuvaus poikkeamasta, sen vakavuudesta ja vaikutuksista;

2) selvitys poikkeaman todennäköisesti aiheuttaneen uhkan tai juurisyyn tyypistä;

3) selvitys toteutetuista ja meneillään olevista toimenpiteistä poikkeaman vaikutusten lieventämiseksi; ja

4) selvitys mahdollisista rajat ylittävistä vaikutuksista.

Jos poikkeama edelleen jatkuu, kun 3 momentissa tarkoitettu loppuraportti pitäisi toimittaa, on loppuraportin sijaan toimitettava väliraportti poikkeaman käsittelyn edistymisestä. Loppuraportti on tällöin toimitettava kuukauden kuluessa siitä, kun viranomainen on käsitellyt poikkeaman. Valvovalla viranomaisella on oikeus poikkeaman kestäessä saada viranomaiselta lisätietoja tai väliraportti.

Merkittävän poikkeaman ilmoittamisessa on noudatettava lisäksi NIS 2 -direktiivin 23 artiklan 11 kohdan nojalla mahdollisesti annettavia Euroopan komission täytäntöönpanosäädöksiä ilmoituksen tietosisällöstä, muodosta ja ilmoitusmenettelystä sekä merkittävän poikkeaman tarkemmasta määrittelystä.

18 e §

Poikkeamailmoituksen vastaanottaminen

Valvovan viranomaisen on viipymättä, mahdollisuuksien mukaan 24 tunnin kuluessa 18 d §:n 1 momentissa tarkoitetun ensi-ilmoituksen vastaanottamisesta annettava viranomaiselle vastaus. Vastauksessa on oltava alustava palaute merkittävästä poikkeamasta, viranomaisen pyynnöstä poikkeaman käsittelyä koskevia ohjeita tai operatiivisia neuvoja sekä ohjeet merkittävän poikkeaman ilmoittamisesta esitutkintaviranomaiselle, jos asiassa epäillään rikosta.

Valvova viranomainen tekee 1 momentissa tarkoitettujen ohjeiden ja operatiivisten neuvojen antamisessa yhteistyötä kyberturvallisuuslaissa tarkoitetun CSIRT-yksikön kanssa. Ohjeet ja operatiiviset neuvot voi valvovan viranomaisen sijaan antaa CSIRT-yksikkö.

18 f §

Vapaaehtoinen ilmoittaminen

Viranomainen voi ilmoittaa valvovalle viranomaiselle myös muista kuin merkittävistä poikkeamista sekä kyberuhkista ja läheltä piti -tilanteista. Myös ne 3 §:ssä tarkoitetut, joihin tätä lukua ei sovelleta, voivat tehdä tällaisen ilmoituksen.

Valvovan viranomaisen on käsiteltävä 1 momentissa tarkoitetut vapaaehtoiset ilmoitukset 18 e §:ssä säädettyä menettelyä noudattaen. Valvova viranomainen voi asettaa 18 d §:ssä tarkoitettujen ilmoitusten käsittelyn etusijalle vapaaehtoisten ilmoitusten käsittelyyn nähden.

Viranomainen ja muut 3 §:ssä tarkoitetut voivat vapaaehtoisen ilmoituksen yhteydessä luovuttaa valvovalle viranomaiselle tietoja, jotka valvovalla viranomaisella on oikeus saada 18 i §:n nojalla.

Vapaaehtoisessa ilmoittamisessa on noudatettava lisäksi NIS 2 -direktiivin 23 artiklan 11 kohdan nojalla mahdollisesti annettavia Euroopan komission täytäntöönpanosäädöksiä ilmoituksen tietosisällöstä, muodosta ja ilmoitusmenettelystä.

18 g §

Tiedotusvelvollisuus merkittävästä kyberuhkasta ja poikkeamasta

Viranomaisen on viipymättä ilmoitettava merkittävästä poikkeamasta palvelujensa vastaanottajille, jos merkittävä poikkeama todennäköisesti haittaa sen palvelujen tarjoamista.

Viranomaisen on viipymättä ilmoitettava merkittävästä kyberuhkasta sekä kyberuhkan hallitsemiseksi käytettävissä olevista toimenpiteistä niille palvelujensa vastaanottajille, joihin merkittävä kyberuhka saattaa vaikuttaa.

Jos merkittävästä poikkeamasta tiedottaminen on yleisen edun mukaista, valvova viranomainen voi velvoittaa viranomaisen tiedottamaan merkittävästä poikkeamasta tai tiedottaa asiasta itse.

Edellä 1 ja 2 momentissa tarkoitetussa tiedottamisessa on noudatettava lisäksi NIS 2 -direktiivin 23 artiklan 11 kohdan nojalla mahdollisesti annettavia Euroopan komission täytäntöönpanosäädöksiä ilmoituksen tietosisällöstä, muodosta ja ilmoitusmenettelystä sekä merkittävän poikkeaman tarkemmasta määrittelystä.

18 h §

Valvova viranomainen

Tässä luvussa tarkoitettu valvova viranomainen ja NIS 2 -direktiivin 8 artiklan 1 kohdassa tarkoitettu toimivaltainen viranomainen julkishallinnon toimialalla on Liikenne- ja viestintävirasto. Valvovan viranomaisen tehtävänä on sen lisäksi mitä tässä luvussa säädetään, valvoa tässä luvussa ja NIS 2 -direktiivin nojalla annetuissa säännöksissä säädettyjen velvollisuuksien noudattamista julkishallinnon toimialalla sekä ylläpitää julkishallinnon toimialan toimijaluetteloa 18 a §:n nojalla toimitetuista tiedoista. Liikenne- ja viestintävirasto on valvovan viranomaisen toiminnassaan itsenäinen ja riippumaton.

Valvova viranomainen voi asettaa tässä laissa säädetyt valvontatehtävänsä tärkeysjärjestykseen riskiperusteisesti. Valvovan viranomaisen on valvonnan kohdistamisessa ja 18 l §:ssä tarkoitettua valvontapäätöstä tehdessään otettava huomioon kyberturvallisuuslain 27 §:n 3 momentissa ja 37 §:ssä tarkoitetut seikat. Valvova viranomainen voi kohdistaa valvontaa hyvinvointialueeseen, hyvinvointiyhtymään tai Helsingin kaupunkiin vain, jos on perusteltu syy epäillä, että mainittu ei ole noudattanut tässä luvussa tai NIS 2 -direktiivin nojalla annetuissa säädöksissä säädettyä.

Ellei tässä luvussa toisin säädetä, valvovan viranomaisen on 18 a §:ssä tarkoitettujen toimintaa koskevien ilmoitusten, 18 d ja 18 f §:ssä tarkoitettujen poikkeamailmoitusten ja muiden valvontatehtävässä saatujen tietojen käsittelyssä sekä yhteistyössä muiden viranomaisten, Euroopan unionin toimielinten, erillisvirastojen ja yhteistyöelinten kanssa sekä tietojen luovuttamisessa niille noudatettava mitä kyberturvallisuuslain 6 §:n 4 momentissa, 15 §:n 3 momentissa, 17 §:ssä, 18 §:n 3 momentissa, 26 §:n 2 momentissa, 28 §:n 4 ja 5 momentissa, 33 §:ssä, 41 §:n 5 momentissa sekä 45 §:ssä säädetään tietojen käsittelystä valvovassa viranomaisessa sekä valvovan viranomaisen yhteistyöstä muiden viranomaisten, Euroopan unionin toimielinten, erillisvirastojen ja yhteistyöelinten kanssa sekä tietojen luovuttamisesta niille.

Liikenne- ja viestintäviraston tehtävistä NIS 2 -direktiivissä tarkoitettuna keskitettynä yhteyspisteenä ja CSIRT-yksikkönä säädetään kyberturvallisuuslaissa.

18 i §

Valvovan viranomaisen tiedonsaantioikeus

Valvovalla viranomaisella on tämän luvun mukaisia tehtäviä suorittaessaan salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus saada kyberturvallisuutta koskevien riskien hallintaa, riskienhallinnan toimintamallia, hallintatoimenpiteitä ja merkittävää poikkeamaa koskevat tiedot sekä muut edellä mainittuihin tietoihin välittömästi liittyvät tiedot, jotka ovat välttämättömiä kyberturvallisuutta koskevan riskienhallintavelvoitteen noudattamisen ja merkittävistä poikkeamista ilmoittamisen ja raportoinnin valvontaa varten. Viranomaisen on luovutettava tiedot viipymättä ja maksutta.

Valvovalla viranomaisella on salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus saada viranomaiselta välitystieto, sijaintitieto sekä tieto

haitallisen tietokoneohjelman tai käskyn sisältävästä viestistä, jos se on välttämätöntä kyberturvallisuutta koskevan riskienhallintavelvoitteen noudattamisen tai merkittävistä poikkeamista ilmoittamisen ja raportoinnin valvomista varten. Valvovan viranomaisen tämän momentin nojalla saamat tiedot on pidettävä salassa.

Tässä pykälässä tarkoitettu tiedonsaantioikeus ei koske salassa pidettäviä tietoja julkisen hallinnon turvallisuusverkkotoiminnasta annetussa laissa tarkoitetusta turvallisuusverkon palvelutuotannosta tai palvelujen käytöstä eikä tietoja, joiden luovuttaminen vaarantaisi maanpuolustusta tai kansallista turvallisuutta taikka olisi vastoin niihin liittyvää tärkeää etua.

Erityissuojattavan tietoaineiston käsittelyä koskevista velvollisuuksista säädetään kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa.

18 j §

Valvovan viranomaisen oikeus tehdä tarkastuksia

Valvovalla viranomaisella on siinä laajuudessa kuin se on tarpeen, oikeus tehdä tässä luvussa tai NIS 2 -direktiivin nojalla annetuissa säännöksissä säädettyjen velvollisuuksien noudattamisen valvomiseksi viranomaiseen kohdistuva tarkastus.

Tarkastuksen suorittajalla on oltava tarkastuksen laatuun ja laajuuteen nähden riittävä koulutus ja kokemus.

Viranomaisen on tarkastusta varten päästettävä tarkastuksen suorittaja tarkastuksen edellyttämässä laajuudessa tarkastuksen kohteena olevaan viestintäverkkoon tai tietojärjestelmään ja muihin kuin pysyväisluonteiseen asumiseen tarkoitettuihin tiloihin. Tarkastuksen suorittamiseksi tarkastuksen suorittajalla on salassapitosäännösten tai muiden tiedon luovuttamista koskevien rajoitusten estämättä oikeus saada tutkittavakseen valvontatehtävän kannalta välttämättömät tiedot, asiakirjat, laitteet ja ohjelmistot, suorittaa tarvittavia testejä ja mittauksia sekä tarkastaa viranomaisen toteuttamat turvallisuusjärjestelyt. Tarkastuksen suorittajan tarkastus- ja tiedonsaantioikeuteen sovelletaan mitä 18 i §:n 3 momentissa säädetään tiedonsaantioikeuden rajoituksista.

Tarkastuksessa noudatettavaan menettelyyn sovelletaan, mitä hallintolain 39 §:ssä säädetään tarkastuksesta.

18 k §

Avustavan tehtävän antaminen tietoturvallisuuden arviointilaitokselle ja arvioinnin teettäminen

Valvova viranomainen voi antaa 18 j §:ssä tarkoitettuun tarkastustehtävään liittyvän avustavan tehtävän tietoturvallisuuden arviointilaitoksista annetussa laissa (1405/2011) tarkoitetulle hyväksytylle tietoturvallisuuden arviointilaitokselle.

Valvova viranomainen voi valvonnan toteuttamiseksi velvoittaa viranomaisen teettämään tietoturvallisuuden arviointilaitoksella kyberturvallisuuteen kohdistuvan riskienhallinnan arvioinnin, jos:

1) viranomaiseen on kohdistunut merkittävä poikkeama, joka on aiheuttanut palvelujen vakavan toimintahäiriön tai huomattavaa aineellista tai aineetonta vahinkoa; tai

2) viranomainen on olennaisesti ja vakavasti laiminlyönyt 18 b tai 18 c §:ssä tarkoitettujen kyberturvallisuuteen kohdistuvien riskienhallintavelvollisuuksien noudattamisen.

Tietoturvallisuuden arviointilaitoksen palveluksessa olevaan tarkastuksessa avustavaan henkilöön ja arvioinnin suorittajaan sovelletaan, mitä 18 j §:n 2—4 momentissa säädetään tarkastuksen suorittajan kokemuksesta ja koulutuksesta sekä tarkastuksen suorittajan oikeuksista. Ellei tässä luvussa toisin säädetä, tietoturvallisuuden arviointilaitokseen sovelletaan tietoturvallisuuden arviointilaitoksista annettua lakia. Tietoturvallisuuden arviointilaitoksen

palveluksessa olevaan henkilöön sovelletaan hänen tässä pykälässä tarkoitettuja tehtäviä hoitaessaan virkamiehen rikosoikeudellista virkavastuuta koskevia säännöksiä, viraltapanoseuraamusta lukuun ottamatta. Vahingonkorvausvastuusta säädetään vahingonkorvauslaissa.

18 l §

Seuraamukset

Valvova viranomainen voi velvoittaa viranomaisen määräajassa korjaamaan puutteet tässä luvussa tai NIS 2 -direktiivin nojalla annetuissa säännöksissä säädettyjen velvollisuuksien noudattamisessa. Valvova viranomainen voi velvoittaa viranomaisen julkistamaan kyseiset puutteet tai muut seikat, jotka liittyvät mainittujen velvollisuuksien rikkomiseen.

Valvova viranomainen voi antaa viranomaiselle varoituksen, jos tämä ei ole noudattanut tässä luvussa tai NIS 2 -direktiivin nojalla annetuissa säännöksissä säädettyjä velvollisuuksia. Varoituksessa on yksilöitävä puute tai laiminlyönti, jota varoitus koskee. Varoitus on annettava kirjallisena.

Valvova viranomainen voi asettaa uhkasakon 1 momentissa tarkoitetun päätöksen noudattamisen tehosteeksi.

18 m §

Muutoksenhaku

Muutoksenhausta hallintotuomioistuimeen säädetään oikeudenkäynnistä hallintoasioissa annetussa laissa (808/2019).

Muutoksenhausta uhkasakon asettamista ja maksettavaksi tuomitsemista koskevaan päätökseen säädetään uhkasakkolaissa (1113/1990).

Tämä laki tulee voimaan 8 päivänä huhtikuuta 2025.

Tämän lain 18 a §:n 2 momentissa tarkoitettu ilmoitus on tehtävä viimeistään kuukauden kuluessa lain voimaantulosta.

Helsingissä 4.4.2025

Tasavallan Presidentti

Alexander Stubb

Liikenne- ja viestintäministeri Lulu Ranne