

Eduskunnan vastaus EV 15/2025 vp — HE 57/2024 vp

Hallituksen esitys eduskunnalle kyberturvallisuudirektiivin (NIS 2 -direktiivi) täytäntöönpanoa koskevaksi lainsäädännöksi

Asia

Hallituksen esitys eduskunnalle kyberturvallisuudirektiivin (NIS 2 -direktiivi) täytäntöönpanoa koskevaksi lainsäädännöksi (HE 57/2024 vp).

Valiokuntakäsittely

Valiokunnan mietintö: Liikenne- ja viestintävaliokunta (LiVM 1/2025 vp).

Päätös

Eduskunta on hyväksynyt seuraavat lausumat:

1. Eduskunta edellyttää, että valtioneuvosto seuraa tarkoin lain tavoitteiden toteutumista ja sen soveltamista sekä ryhtyy tarvittaessa toimenpiteisiin havaitsemiensa epäkohtien korjaamiseksi.
2. Eduskunta edellyttää, että liikenne- ja viestintäministeriö antaa selvityksen lain tavoitteiden toteutumisesta ja sen soveltamisesta liikenne- ja viestintävaliokunnalle 31 päivään elokuuta 2026 mennessä.

Eduskunta on hyväksynyt seuraavat lait:

Kyberturvallisuuslaki

Eduskunnan päätöksen mukaisesti säädetään:

1 luku

Yleiset säännökset

1 §

Soveltamisala

Tässä laissa säädetään kyberturvallisuutta koskevien riskien hallinnasta.

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 annettu Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555 (*NIS 2 -direktiivi*).

NIS 2 -direktiivin täytäntöönpanosta mainitun direktiivin liitteen I kohdassa 10 tarkoitetulla julkishallinnon toimialalla säädetään julkisen hallinnon tiedonhallinnasta annetussa laissa (906/2019).

2 §

Määritelmät

Tässä laissa tarkoitetaan:

1) *aluetunnusrekisterin ylläpitäjällä* tahoja, jolle on myönnetty oikeus hallinnoida tiettyä aluetunnusta ja joka sitä hallinnoidessaan vastaa verkkotunnusten rekisteröinnistä sen alle sekä sen teknisestä toiminnasta;

2) *datakeskuspalvelulla* palvelua, joka käsittää rakenteita tai rakenteiden ryhmiä, jotka on tarkoitettu datan tallennus-, käsittely- ja siirtopalveluja tarjoavien tietoteknisten laitteiden ja verkkolaitteiden keskitettyyn ylläpitoon, yhteenliittämiseen ja ohjaukseen yhdessä kaikkien tarvittavien sähkönjakeluun ja toimintaolosuhteiden säätelyyn tarkoitettujen laitteiden ja infrastruktuurin kanssa;

3) *DNS-palveluntarjoajalla* toimijaa, joka tarjoaa yleisesti saatavilla olevia rekursiivisia verkkotunnusten selvityspalveluja internetin loppukäyttäjille tai auktoritatiivisia verkkotunnusten selvityspalveluja kolmansille osapuolille, lukuun ottamatta juurinimipalvelimia;

4) *haavoittuvuudella* tieto- ja viestintätekniikan tuotteiden tai -palvelujen heikkoutta, alttiutta tai vikaa, joka voi aiheuttaa kyberuhkan tai poikkeaman;

5) *hallintapalvelun tarjoajalla* toimijaa, joka tarjoaa 17 kohdassa tarkoitettujen TVT-tuotteiden, verkkojen, infrastruktuurin, sovellusten tai muiden viestintäverkkojen ja tietojärjestelmien asentamiseen, hallintaan, käyttöön tai ylläpitoon liittyviä palveluja joko asiakkaan tiloissa tai etäyhteyden välityksellä toteutettavan tuen tai aktiivisen ylläpidon muodossa;

6) *hyväksytyllä luottamuspalvelun tarjoajalla* sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoami-

Eduskunnan vastaus EV 15/2025 vp

sesta annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 (*eIDAS-asetus*) 3 artiklan 20 alakohdassa tarkoitettua hyväksyttyä luottamuspalvelun tarjoajaa;

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

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

9) *luottamuspalvelun tarjoajalla* eIDAS-asetuksen 3 artiklan 19 alakohdassa määriteltyä luottamuspalvelun tarjoajaa;

10) *pilvipalvelulla* digitaalista palvelua, joka tarjoaa laajaan etäkäyttöön skaalattavan ja joustavan joukon jaettavissa olevia ja tarveperusteisesti ohjattavia tietoteknisiä resursseja;

11) *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;

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

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

14) *sisällönjakeluverkolla* maantieteellisesti hajautettujen palvelimien verkkoa, jonka tarkoituksena on varmistaa digitaalisen sisällön ja digitaalisten palvelujen hyvä saatavuus, käytettävyys ja nopea jakelu internetin käyttäjille sisällön ja palvelujen tarjoajien puolesta;

15) *tietoturvapalveluntarjoajalla* hallintapalvelun tarjoajaa, joka toimii kyberturvallisuusriskien hallitsemiseksi tai antaa tukea sitä varten;

16) *TVT-palvelulla* Euroopan unionin kyberturvallisuusvirasto ENISA:sta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista sekä asetuksen (EU) N:o 526/2013 kumoamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/881 (*kyberturvallisuusasetus*) 2 artiklan 13 kohdassa tarkoitettua tieto- ja viestintätekniikan palvelua;

17) *TVT-tuotteella* kyberturvallisuusasetuksen 2 artiklan 12 kohdassa tarkoitettua tieto- ja viestintätekniikan tuotetta;

18) *valvovalla viranomaisella* 26 §:ssä mainittuja viranomaisia;

19) *verkkoyhteisöalustalla* alustaa, jonka avulla loppukäyttäjät voivat olla yhteydessä toisiinsa, jakaa sisältöä, hakea tietoa ja viestiä keskenään monenlaisilla päätelaitteilla;

20) *verkossa toimivalla hakukoneella* oikeudenmukaisuuden ja avoimuuden edistämisestä verkossa toimivien välityspalvelujen yrityskäyttäjää varten annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/1150 2 artiklan 5 kohdassa tarkoitettua verkossa toimivaa hakukonetta;

21) *verkossa toimivalla markkinapaikalla* kuluttajansuojalain (38/1978) 6 luvun 8 §:n 4 kohdassa tarkoitettua verkossa toimivaa markkinapaikkaa;

22) *viestintäverkolla ja tietojärjestelmällä*

a) eurooppalaisesta sähköisen viestinnän säännöstöstä annettua Euroopan parlamentin ja neuvoston direktiivin (EU) 2018/1972 (*teledirektiivi*) 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;

Eduskunnan vastaus EV 15/2025 vp

23) *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;

24) *yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajalla* sitä, joka tarjoaa sähköisen viestinnän palveluista annetun lain (917/2014) 3 §:n 37 kohdassa tarkoitettua viestintäpalvelua ennalta rajaamattomalle käyttäjäpiirille;

25) *yleisten sähköisten viestintäverkkojen tarjoajalla* sitä, joka tarjoaa sähköisen viestinnän palveluista annetun lain 3 §:n 34 kohdassa tarkoitettua verkkopalvelua.

3 §

Toimijat

Tätä lakia sovelletaan oikeushenkilöön ja luonnolliseen henkilöön (*toimija*), joka:

1) harjoittaa liitteessä I tai II tarkoitettua toimintaa tai on mainituissa liitteissä tarkoitettu toimija; ja

2) täyttää tai ylittää mikroyritysten sekä pienten ja keskisuurten yritysten määritelmästä annetun komission suosituksen 2003/361/EY liitteen 2 artiklan mukaiset keskisuuria yrityksiä koskevat edellytykset ja tarjoaa palvelujaan tai harjoittaa toimintaansa jossakin Euroopan unionin jäsenvaltiossa.

Tätä lakia sovelletaan myös toimijaan, joka koostaan riippumatta on:

1) yleisten sähköisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoaja;

2) luottamuspalvelun tarjoaja;

3) aluetunnusrekisterin ylläpitäjä; tai

4) DNS-palveluntarjoaja.

Lisäksi tätä lakia sovelletaan sellaiseen toimijaan sen koosta riippumatta, joka harjoittaa liitteessä I tai II tarkoitettua toimintaa tai on mainituissa liitteissä tarkoitettu toimija, jos:

1) se tarjoaa palvelua, joka on yhteiskunnan tai talouden kriittisten toimintojen ylläpitämisen kannalta keskeinen ja jota muut toimijat eivät tarjoa;

2) häiriö sen tarjoamassa palvelussa vaikuttaisi merkittävästi yleiseen järjestykseen, yleiseen turvallisuuteen tai kansanterveyteen;

3) häiriö sen tarjoamassa palvelussa voisi aiheuttaa merkittävän systeemisen riskin erityisesti aloilla, joilla tällaisella häiriöllä voisi olla rajat ylittäviä vaikutuksia; tai

4) se on kriittinen, koska sillä on erityisen suuri merkitys kansallisella tai alueellisella tasolla kyseisen toimialan tai palvelutyyppin tai jonkin Euroopan unionin jäsenvaltion muiden keskinäisriippuvaisten toimialojen kannalta.

Edellä 3 momentissa tarkoitetuista kriteereistä voidaan antaa tarkempia säännöksiä valtioneuvoston asetuksella.

Toimijaan ei sovelleta 1 momentin 2 kohdassa mainitun suosituksen liitteen 3 artiklan 4 kohtaa.

Eduskunnan vastaus EV 15/2025 vp

4 §

Soveltamisalan rajaukset

Tämän lain 2 lukua ei sovelleta toimintaan eikä palveluihin, joita tarjotaan maanpuolustuksen, kansallisen turvallisuuden, yleisen järjestyksen ja turvallisuuden taikka rikosten ennalta estämisen, rikostutkinnan ja syytetoimien toteuttamiseksi.

Tätä lakia ei sovelleta toimijaan, joka tarjoaa ainoastaan 1 momentissa tarkoitettua toimintaa tai palvelua.

Edellä 1 ja 2 momentista poiketen lakia sovelletaan toimijaan, joka on luottamuspalvelun tarjoaja.

Tätä lakia ei sovelleta toimijaan, johon finanssialan digitaalisesta häiriönsietokyvystä ja asetusten (EY) N:o 1060/2009, (EU) N:o 648/2012, (EU) N:o 600/2014, (EU) N:o 909/2014 ja (EU) 2016/1011 muuttamisesta annettua Euroopan parlamentin ja neuvoston asetusta (EU) 2022/2554 (*DORA-asetus*) ei sovelleta sen 2 artiklan 4 kohdan nojalla.

Tätä lakia ei sovelleta toimijaan, jonka harjoittama liitteessä I tai II tarkoitettu toiminta on satunnaista ja vähäistä.

Tätä lakia sovelletaan kuntalaissa (410/2015) tarkoitettuun kuntaan vain liitteessä I tai II tarkoitettujen toiminnan osalta.

Tämän lain säännöksiä, jotka velvoittavat antamaan tietoa, ei sovelleta, jos tiedon luovuttaminen vaarantaisi maanpuolustusta tai kansallista turvallisuutta taikka olisi vastoin siihen liittyvää tärkeää etua.

5 §

Suhde muuhun lainsäädäntöön

Jos muussa laissa tai sen nojalla annetuissa säännöksissä tai määräyksissä on tästä laista poikkeavia vaatimuksia kyberturvallisuusriskien hallinnasta tai merkittävistä poikkeamista ilmoittamisesta ja vaatimukset ovat vaikutuksiltaan vähintään tässä laissa säädettyjä velvoitteita vastaavia, niitä sovelletaan tämän lain vastaavien säännösten asemasta.

Jos Euroopan unionin asetuksessa tai NIS 2 -direktiivin nojalla säädettyssä komission asetuksessa edellytetään, että toimija ottaa käyttöön kyberturvallisuutta koskevien riskien hallitsemiseksi toimenpiteitä tai ilmoittaa merkittävistä poikkeamista, ja vaatimukset ovat vaikutuksiltaan vähintään tässä laissa säädettyjä velvoitteita vastaavia, säännöksiä sovelletaan tämän lain 2, 4 ja 5 luvun sekä 41 §:n asemasta.

Henkilötietojen käsittelyn tietoturvallisuudesta säädetään luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuojasetus) annetun Euroopan parlamentin ja neuvoston asetuksessa (EU) 2016/679, jäljempänä *yleinen tietosuojasetus*, ja tietosuojalaissa (1050/2018).

Sen lisäksi mitä tässä laissa säädetään valvovan viranomaisen toimivaltuuksista, luvan peruuttamiseen sovelletaan sähkö- ja maakaasumarkkinoiden valvonnasta annetun lain (590/2013) 23 §:n 6 kohdassa, vaarallisten kemikaalien ja räjähteiden käsittelyn turvallisuudesta annetun lain (390/2005) 109 a §:ssä sekä maa-asemista ja eräistä tutkista annetun lain (96/2023) 8 §:n 1 momentin 3 kohdassa säädettyä.

Eduskunnan vastaus EV 15/2025 vp

6 §

Lainkäyttövalta ja alueellisuus

Tätä lakia sovelletaan toimijaan, joka on sijoittautunut Suomeen, jollei laissa toisin säädetä tai Euroopan unionin lainsäädännöstä tai Suomea sitovasta kansainvälisestä velvoitteesta muuta johdu.

Riippumatta valtiosta, johon toimija on sijoittautunut, tätä lakia sovelletaan yleisen sähköisen viestintäverkon tarjoajaan ja yleisesti saatavilla olevan sähköisen viestintäpalvelun tarjoajaan silloin kun se tarjoaa palvelujaan Suomessa.

DNS-palveluntarjoaja, aluetunnusrekisterin ylläpitäjä, pilvipalvelujen tarjoaja, datakeskuspalvelujen tarjoaja, sisällönjakeluverkkojen tarjoaja, hallintapalvelun tarjoaja, tietoturvapalveluntarjoaja, verkossa toimivien markkinapaikkojen tarjoaja, verkossa toimivien hakukoneiden tarjoaja ja verkkoyhteisöalustojen tarjoaja kuuluvat tämän lain soveltamisalaan, jos sen NIS 2 -direktiivin 26 artiklan 2 kohdassa tarkoitettu päätoimipaikka tai 3 kohdassa tarkoitettu Euroopan unioniin nimetty edustaja sijaitsee Suomessa. Jos tällainen toimija ei ole sijoittautunut Euroopan unionin jäsenvaltioon ja se tarjoaa palvelujaan Suomessa tai muun Euroopan unionin jäsenvaltion alueella, sen on nimettävä NIS 2 -direktiivin 26 artiklan 3 kohdassa tarkoitettu edustaja Euroopan unionin jäsenvaltioiden aluetta varten. Jos toimija ei ole sijoittautunut Euroopan unionin jäsenvaltioon tai asettanut NIS 2 -direktiivin 26 artiklan 3 kohdassa tarkoitettua nimettyä edustajaa ja toimija tarjoaa palveluita Suomessa, toimija kuuluu tämän lain soveltamisalaan.

Valvova viranomainen voi suorittaa toiseen Euroopan unionin jäsenvaltioon sijoittautuneeseen toimijaan kohdistuvia valvonta- tai täytäntöönpanotoimia siten kuin tässä laissa säädetään, jos toisen jäsenvaltion toimivaltainen viranomainen sitä pyytää ja toimija tarjoaa palveluja Suomessa tai sillä on viestintäverkko tai tietojärjestelmä Suomen alueella. Edellytyksenä on lisäksi, että valvovalla viranomaisella olisi oikeus suorittaa vastaava valvonta- tai täytäntöönpanotoimi tämän lain nojalla, jos toimija olisi sijoittautunut Suomeen. Valvova viranomainen voi kieltäytyä pyynnöstä, jos sillä ei ole lain nojalla toimivaltaa antaa pyydettyä apua, pyydetty apu ei ole oikeassa suhteessa valvontatehtäviin tai pyyntö koskee sellaisia tietoja tai käsittää sellaisia toimintoja, joiden paljastaminen tai toteuttaminen olisi vastoin Suomen maapuolustukseen tai kansalliseen turvallisuuteen liittyviä etuja. Ennen pyynnöstä kieltäytymistä valvovan viranomaisen on kuultava muita asianomaisia toimivaltaisia viranomaisia sekä, jos jokin Euroopan unionin jäsenvaltio sitä pyytää, Euroopan komissiota ja Euroopan unionin kyberturvallisuusvirastoa.

2 luku

Riskienhallinta ja poikkeamista ilmoittaminen

7 §

Riskienhallinta

Toimijan on tunnistettava, arvioitava ja hallittava riskejä, joita kohdistuu sen toiminnoissa tai palveluntarjonnassa käytettävien viestintäverkkojen ja tietojärjestelmien turvallisuuteen. Kyber-

Eduskunnan vastaus EV 15/2025 vp

turvallisuutta koskevalla riskienhallinnalla tulee estää tai minimoida poikkeamien vaikutus toimintaan, toiminnan jatkuvuuteen, palvelujen vastaanottajiin ja muihin palveluihin.

Toimijan on toteutettava riskienhallintatoimenpiteet, jotka ovat ajantasaisia, oikeasuhtaisia ja riittäviä suhteessa toiminnassa käytettävälle viestintäverkoille ja tietojärjestelmille aiheutuviin riskeihin ja viestintäverkon tai tietojärjestelmän merkitykseen toimijan toiminnan ja palveluntarjonnan kannalta.

8 §

Kyberturvallisuutta koskeva riskienhallinnan toimintamalli

Toimijalla 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 9 §:n mukaiset toimenpiteet, joilla viestintäverkkoja ja tietojärjestelmiä ja niiden fyysistä ympäristöä suojataan kyberuhkilta ja poikkeamilta (*hallintatoimenpiteet*).

9 §

Toimenpiteet kyberturvallisuutta koskevien riskien hallinnassa

Toimijoiden on toteutettava kyberturvallisuutta koskevan riskienhallinnan toimintamallin mukaiset oikeasuhtaiset tekniset, operatiiviset tai organisatoriset hallintatoimenpiteet viestintäverkkojen ja tietojärjestelmien turvallisuuteen kohdistuvien riskien hallitsemiseksi ja haitallisten vaikutusten estämiseksi tai minimoimiseksi.

Toimintamallissa ja siihen perustuvissa hallintatoimenpiteissä on otettava huomioon ja pidettävä yllä ajantasaisesti ainakin:

- 1) kyberturvallisuutta koskevan riskienhallinnan toimintaperiaatteet ja hallintatoimenpiteiden 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 sisällytetty hallintatoimenpiteet sekä välittömien toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt;
- 5) omaisuudenhallinta ja sen turvallisuuden kannalta tärkeiden toimintojen tunnistaminen;
- 6) henkilöstöturvallisuus ja kyberturvallisuuskoulutus;
- 7) pääsynhallinnan ja todentamisen menettelyt;
- 8) salausten menetelmien käyttämisestä koskevat toimintaperiaatteet ja menettelyt sekä tarvittaessa toimenpiteet suojatun sähköisen viestinnän käyttämiseksi;
- 9) poikkeamien havainnointi ja käsittely turvallisuuden ja toimintavarmuuden palauttamiseksi ja ylläpitämiseksi;

Eduskunnan vastaus EV 15/2025 vp

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

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

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

Toimenpiteet on suhteutettava toiminnan laatuun ja laajuuteen, poikkeamasta kohtuudella ennakoitavissa oleviin välittömiin vaikutuksiin, toimijan viestintäverkkojen ja tietojärjestelmien riskialttiuteen, poikkeamien todennäköisyyteen ja vakavuuteen, toimenpiteistä aiheutuviin kustannuksiin sekä ajantasainen kehitys huomioon ottaen käytettävissä oleviin teknisiin mahdollisuuksiin torjua uhka.

Valvova viranomainen voi toimialallaan antaa riskienhallintavelvollisuuksia tarkentavia teknisiä määräyksiä:

1) toimialakohtaisista erityispiirteistä, jotka on otettava huomioon kyberturvallisuutta koskevassa riskienhallinnan toimintamallissa ja 2 momentissa tarkoitetuissa osa-alueissa sekä riskienhallinnan ja viestintäverkkojen ja tietojärjestelmien tietoturvallisuuden hallinnan menettelyissä;

2) kriittisiä toimitusketjuja koskevien unionin tason koordinoitujen riskinarviointien tuloksien huomioimisesta toimialakohtaisessa riskienhallinnassa.

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

10 §

Johdon vastuu

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

Johdolla tarkoitetaan toimijan hallitusta, hallintoneuvostoa ja toimitusjohtajaa sekä muussa niihin rinnastettavassa asemassa olevaa, joka tosiasiallisesti johtaa sen toimintaa.

11 §

Poikkeamailmoitukset viranomaiselle

Toimijan on viipymättä ilmoitettava valvovalle viranomaiselle merkittävästä poikkeamasta. Merkittävällä poikkeamalla tarkoitetaan poikkeamaa, joka on aiheuttanut tai voi aiheuttaa vakavan palvelujen toimintahäiriön tai huomattavia taloudellisia tappioita asianomaiselle toimijalle, sekä poikkeamaa, joka on vaikuttanut tai voi vaikuttaa muihin luonnollisiin henkilöihin tai oikeushenkilöihin aiheuttamalla huomattavaa aineellista tai aineetonta vahinkoa.

Ensi-ilmoitus on tehtävä 24 tunnin kuluessa merkittävän poikkeaman havaitsemisesta ja jatkoilmoitus 72 tunnin kuluessa merkittävän poikkeaman havaitsemisesta.

Ensi-ilmoituksessa on ilmoitettava:

1) merkittävän poikkeaman havaitsemisesta;

Eduskunnan vastaus EV 15/2025 vp

2) epäilläänkö merkittävän poikkeaman johtuvan rikoksesta tai muusta lainvastaisesta tai vihamielisestä teosta;

3) rajat ylittävien vaikutuksien mahdollisuus ja todennäköisyys sekä rajat ylittävien vaikutusten ennakkointiin liittyvät tiedot.

Jatkoilmoituksessa on ilmoitettava:

- 1) arvio merkittävän poikkeaman laadusta, vakavuudesta ja vaikutuksista;
- 2) tekniset vaarantumisindikaattorit, jos sellaisia on saatavilla;
- 3) mahdolliset päivitykset ensi-ilmoituksen tietoihin.

Valvova viranomainen voi toimialallaan antaa tarkempia teknisiä määräyksiä, joilla tarkennetaan 11—15 §:n nojalla tehtävän ilmoituksen, tiedotuksen tai raportin tietosisältöä, teknistä muotoa ja menettelyä.

Edellä 2 momentissa säädetystä poiketen luottamuspalvelun tarjoajan on tehtävä jatkoilmoitus 24 tunnin kuluessa merkittävän poikkeaman havaitsemisesta, jos merkittävä poikkeama vaikuttaa sen luottamuspalvelujen tarjontaan.

Edellä 1 momentissa tarkoitettuna lisäksi merkittävällä poikkeamalla tarkoitetaan NIS 2 -direktiivin 23 artiklan 11 kohdan nojalla annetussa Euroopan komission täytäntöönpanosäädöksessä täsmennettyä tilannetta, jossa poikkeama katsotaan merkittäväksi.

12 §

Poikkeamaa koskeva väliraportti

Toimijan on annettava valvovan viranomaisen pyynnöstä lisätietoja tai väliraportti merkittävää poikkeamaa koskevista tilannepäivityksistä ja käsittelyn edistymisestä.

Jos merkittävä poikkeama on pitkäkestoinen, toimijan on annettava väliraportti viimeistään kuukauden kuluttua jatkoilmoituksen antamisesta.

13 §

Poikkeamaa koskeva loppuraportti

Toimijan on annettava valvovalle viranomaiselle merkittävää poikkeamaa koskeva loppuraportti kuukauden kuluessa jatkoilmoituksen toimittamisesta tai, jos kyseessä on pitkäkestoinen poikkeama, kuukauden kuluessa sen käsittelyn päättymisestä.

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.

Eduskunnan vastaus EV 15/2025 vp

14 §

Poikkeamasta ja kyberuhkasta ilmoittaminen muulle kuin viranomaiselle

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

Toimijan on ilmoitettava viipymättä 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 toimijan tiedottamaan asiasta tai tiedottaa asiasta itse.

15 §

Vapaaehtoinen ilmoittaminen

Toimijat voivat vapaaehtoisesti tehdä valvovalle viranomaiselle ilmoituksia muista kuin 11 §:ssä tarkoitetuista poikkeamista, kyberuhkista ja läheltä piti -tilanteista.

Valvovan viranomaisen on toimialallaan otettava vastaan vapaaehtoisia poikkeamailmoituksia merkittävistä poikkeamista, poikkeamista, kyberuhkista ja läheltä piti -tilanteista myös muilta kuin tässä laissa tarkoitetuilta toimijoilta.

Valvovan viranomaisen on toimitettava tieto tämän pykälän nojalla tehdyistä ilmoituksista 18 §:ssä tarkoitettulle keskitetylle yhteyspisteelle.

16 §

Poikkeamailmoituksen vastaanottaminen

Valvovan viranomaisen on vastattava poikkeamailmoituksen tehneelle taholle viivytyksettä. Vastauksessa on oltava alustava palaute merkittävästä poikkeamasta sekä ohjeet siitä ilmoittamisesta esitutkintaviranomaiselle, jos asiassa epäillään rikosta.

Valvova viranomainen voi asettaa etusijalle 11 §:ssä tarkoitettuihin ilmoituksiin vastaamisen ja niiden 17 §:n mukaisen käsittelyn vapaaehtoisiin ilmoituksiin nähden.

17 §

Poikkeamailmoitusten käsittely

Valvovan viranomaisen on toimitettava 11—13 ja 15 §:ssä tarkoitettut ilmoitukset ja raportit CSIRT-yksikölle välittömästi. CSIRT-yksikkö antaa toimijan pyynnöstä ohjeita ja operatiivisia neuvoja vaikutuksia lieventävistä toimenpiteistä.

Jos merkittävästä poikkeamasta on aiheutunut yleisen tietosuoja-asetuksen 33 artiklassa tarkoitettu henkilötietojen tietoturvaloukkaus, josta on ilmoitettava, valvovan viranomaisen on ilmoitettava poikkeaman havaitsemisesta tietosuojavaltuutetulle.

Eduskunnan vastaus EV 15/2025 vp

Jos merkittävässä poikkeamassa toimijan ilmoituksen perusteella voidaan olettaa tehdyksi rikos, josta säädetty enimmäisrangaistus on vähintään kolme vuotta vankeutta, valvovan viranomaisen on ilmoitettava merkittävän poikkeaman havaitsemisesta poliisille.

Jos merkittävällä poikkeamalla on vaikutuksia muihin Euroopan unionin jäsenvaltioihin tai muihin toimialoihin, valvovan viranomaisen on tiedotettava siitä 18 §:ssä tarkoitetulle keskitetylle yhteyspisteelle ja toimitettava sitä koskevat ilmoitukset, raportit ja muut tiedot yhteyspisteelle.

Jos merkittävä poikkeama vaikuttaa toiseen Euroopan unionin jäsenvaltioon, keskitetyn yhteyspisteen on ilmoitettava siitä ilman aiheutonta viivytystä Euroopan unionin kyberturvallisuusvirastolle ja niille jäsenvaltioille, joihin poikkeama vaikuttaa. Keskitetyn yhteyspisteen on pyynnöstä toimitettava myös 11—13 §:ssä tarkoitetut ilmoitukset ja raportit sen Euroopan unionin jäsenvaltion, johon poikkeama vaikuttaa, keskitetylle yhteyspisteelle. Keskitetty yhteyspiste saa luovuttaa tässä tarkoituksessa Euroopan unionin kyberturvallisuusvirastolle ja muiden Euroopan unionin jäsenvaltioiden keskitetyille yhteyspisteille tietoja merkittävästä poikkeamasta.

18 §

Keskitetty yhteyspiste

Liikenne- ja viestintäviraston Kyberturvallisuuskeskus toimii NIS 2 -direktiivin 8 artiklan 3 kohdassa tarkoitettuna keskitettynä yhteyspisteenä.

Keskitetyn yhteyspisteen tehtävänä on edistää valvovien viranomaisten välistä yhteistyötä ja koordinaatiota tämän lain mukaisten tehtävien toteuttamisessa.

Keskitetyn yhteyspisteen on toimitettava Euroopan unionin kyberturvallisuusvirastolle kolmen kuukauden välein yhteenvetoraportti, joka sisältää anonymisoidut koontitiedot 11—13 ja 15 §:n nojalla ilmoitetuista merkittävistä poikkeamista, poikkeamista, kyberuhkista ja läheltä piti-tilanteista. Keskitetyllä yhteyspisteellä on oikeus saada tätä tarkoitusta varten anonymisoidut koontitiedot valvovalta viranomaiselta.

3 luku

CSIRT-yksikkö

19 §

CSIRT-yksikkö

Liikenne- ja viestintävirastossa toimii tietoturvaloukkauksiin reagoiva ja niitä tutkiva NIS 2 -direktiivin 1 artiklan 2 kohdan a alakohdassa tarkoitettu CSIRT-yksikkö. Sen toiminta on järjestetty erilliseksi 26 §:n nojalla tehtävästä valvonnasta.

CSIRT-yksikön on täytettävä seuraavat vaatimukset:

1) sen on varmistettava viestintäkanaviensa kattava saatavuus välttämällä viestinnän täysin katkaisevia yksittäisiä vikaantumispisteitä ja ylläpidettävä useita viestintäkeinoja, joilla muut voivat ottaa siihen ja se voi ottaa muihin yhteyttä milloin tahansa;

2) sen toimitilat ja niiden toimia tukevat tietojärjestelmät on sijoitettava suojattuihin paikkoihin;

Eduskunnan vastaus EV 15/2025 vp

3) sillä on oltava tarkoituksenmukainen järjestelmä pyyntöjen hallintaa ja reititystä varten, erityisesti tapausten tuloksekkaan ja tehokkaan edelleen ohjauksen helpottamiseksi;

4) sen on varmistettava toimintojensa luottamuksellisuus ja luotettavuus;

5) sillä on oltava riittävä henkilöstö palvelujensa jatkuvan saatavuuden varmistamiseksi, ja sen on varmistettava henkilöstönsä asianmukainen koulutus;

6) sillä on oltava varautumisjärjestelyt palvelujensa jatkuvuuden varmistamiseksi.

CSIRT-yksikön on määritettävä selkeästi 2 momentin 1 kohdassa tarkoitettut viestintäkanavat ja tiedotettava niistä kohderyhmilleen ja yhteistyökumppaneilleen.

20 §

CSIRT-yksikön tehtävät

CSIRT-yksikön tehtävänä on:

1) seurata ja analysoida kyberuhkia, haavoittuvuuksia ja poikkeamia kansallisella tasolla sekä kerätä niitä koskevia tietoja ja antaa niitä koskevia ennakkovaroituksia, hälytyksiä, ilmoituksia ja tietoja;

2) avustaa pyynnöstä viestintäverkkojen ja tietojärjestelmien tietoturvallisuuden reaaliaikaisessa tai lähes reaaliaikaisessa seurannassa;

3) reagoida poikkeamailmoituksiin ja tarvittaessa avustaa poikkeamasta ilmoittanutta tahoa poikkeaman käsittelyssä;

4) kerätä ja analysoida uhkatietoja ja tietoturvaloukkausten tutkintaa koskevia tietoja;

5) laatia riski- ja poikkeama-analyysyjä ja tukea kyberturvallisuuden tilannekuvan ylläpitämistä;

6) osallistua NIS 2 -direktiivin 15 artiklassa tarkoitettuun CSIRT-verkostoon ja avustaa sen jäseniä niiden pyynnöstä;

7) nimetä asiantuntijoita NIS 2 -direktiivin 19 artiklassa tarkoitettuihin vertaisarviointeihin;

8) edistää tietoturvallisten tiedonjakovälineiden käyttöönottoa;

9) antaa ohjeita ja suosituksia poikkeamien käsittelemisestä, kyberturvallisuuden kriisinhallinnasta ja koordinoitusta haavoittuvuuksien julkistamisesta.

CSIRT-yksikkö voi asettaa tehtäviään riskiperusteisesti tärkeysjärjestykseen käytettävissään olevien voimavarojen mukaisesti.

CSIRT-yksikkö koordinoi 23 §:ssä tarkoitettuja kyberturvallisuustietojen vapaaehtoisia jakamisjärjestelyjä itsensä, tämän lain soveltamisalaan kuuluvien toimijoiden ja muiden yhteisöjen kesken.

CSIRT-yksikkö voi tuottaa 1 momentin 2 kohdassa tarkoitettua viestintäverkon ja tietojärjestelmien reaaliaikaista tai lähes reaaliaikaista tietoturvallisuuden seurantaa koskevaa palvelua viestintäverkkojen ja tietojärjestelmien tietoturvallisuuden varmistamiseksi, poikkeamien havaitsemiseksi ja selvittämiseksi sekä kyberuhkien ennalta estämiseksi (*tietoturvaloukkausten havainnointipalvelu*). CSIRT-yksikkö voi tarjota tietoturvaloukkausten havainnointipalvelua suoraan sitä pyytävälle toimijoille ja muille yhteisöille sekä sellaisille tietoturvapalveluntarjoajille, jotka tarjoavat tietoturvaloukkausten havainnointipalvelua toimijoille tai muille yhteisöille käytettäväksi (*palvelukeskus*).

CSIRT-yksikön 1 momentin 1 ja 2 kohdassa sekä 21 §:n 4 momentissa tarkoitettu palvelusta voidaan periä maksu siltä, joka palvelua pyytää. Viranomaisten suoritteiden maksullisuudesta ja

Eduskunnan vastaus EV 15/2025 vp

suoritteista perittävien maksujen suuruuden yleisistä perusteista sekä maksujen muista perusteista säädetään valtion maksuperustelaissa (150/1992).

21 §

Yleisten viestintäverkkojen ja tietojärjestelmien verkkopohjainen haavoittuvuuskartoitus

CSIRT-yksiköllä on oikeus ennakoivalla, muulla kuin intrusiivisella tavalla havainnoida ja kartoittaa tietoja yleiseen viestintäverkkoon liitetyistä viestintäverkoista ja tietojärjestelmistä haavoittuvuuksien, kyberuhkien ja turvattomasti määritettyjen viestintäverkkojen tai tietojärjestelmien asetuksien havaitsemiseksi (*haavoittuvuuskartoitus*). Haavoittuvuuskartoitus tehdään haavoittuvien tai turvattomasti määritettyjen viestintäverkkojen ja tietojärjestelmien asetuksien havaitsemiseksi ja havainnoista asianomaisille tahoille ilmoittamiseksi.

Haavoittuvuuskartoituksen toteuttamisessa CSIRT-yksiköllä on oikeus yleisen viestintäverkon välityksellä hankkia tietoja siihen kytkettyjen viestintäverkkolaitteiden, telepäätelaitteiden, muiden tietojärjestelmien ja niiden tietoliikennejärjestelyjen yksilöintitiedoista, käytetyistä ohjelmistoista ja niiden toiminnasta, teknisestä toteutuksesta ja niiden avulla tarjotuista palveluista. Haavoittuvuuskartoitus ei saa aiheuttaa haittaa kartoituksen kohteena olevan järjestelmän tai palvelun toiminnalle. Haavoittuvuuskartoituksella ei saa hankkia tietoa yleisessä viestintäverkossa tai yleisesti saatavilla olevassa viestintäpalvelussa välitettävänä olevasta viestinnästä.

Haavoittuvuuskartoituksessa havaittuja, kartoituksen kohteeseen yhdistettävissä olevia tietoja saa käyttää vain viestintäverkkoon tai tietojärjestelmään kohdistuvista haavoittuvuuksista ja riskeistä ilmoittamiseksi kartoituksen kohteelle. CSIRT-yksikkö voi käyttää haavoittuvuuskartoituksella hankittuja tietoja lisäksi 20 §:n 1 momentin 1, 4 ja 5 kohdassa tarkoitettujen tehtävien hoitamiseksi. Tarpeettomat tiedot on poistettava viipymättä.

CSIRT-yksiköllä on oikeus tehdä kartoituksen kohteen pyynnöstä haavoittuvuuskartoitus kartoituksen kohteen viestintäverkossa tai tietojärjestelmissä 1—3 momentissa säädetystä poikkeavalla tavalla sellaisen haavoittuvuuden, kyberuhkan tai turvattomasti määritettyjen asetuksien havaitsemiseksi, jolla voi olla merkittävä vaikutus viestintäverkkoon tai tietojärjestelmään tai niiden avulla tarjottaviin palveluihin (*kohdennettu haavoittuvuuskartoitus*).

Haavoittuvuuskartoituksessa ja kohdennetussa haavoittuvuuskartoituksessa ei saa käsitellä sähköisten viestien sisältöä eikä välitystietoa. CSIRT-yksikön on hävitettävä haavoittuvuuskartoituksessa tai kohdennetussa haavoittuvuuskartoituksessa saamansa tiedot, kun ne eivät ole enää tarpeen tässä pykälässä tarkoitettujen tehtävien hoitamiseksi.

22 §

Koordinoitu haavoittuvuuksien julkistaminen

CSIRT-yksikkö toimii NIS 2 -direktiivin 12 artiklassa tarkoitettuna koordinaattorina koordinoitua haavoittuvuuksien julkistamista varten. Tässä tehtävässä CSIRT-yksikkö ottaa vastaan ilmoituksia haavoittuvuuksista ja huolehtii niistä johtuvista tarpeellisista jatkotoimista. Ilmoituksen saa antaa nimettömänä.

Koordinaattorina CSIRT-yksikkö ottaa yhteyttä ja toimii tarvittaessa välittäjänä haavoittuvuudesta ilmoittavan tahon ja TVT-tuotteen tai -palvelun valmistajan tai tarjoajan välillä, avustaa haavoittuvuudesta ilmoittavia tahoja ja neuvottelee haavoittuvuuden julkistamisen aikataulusta

Eduskunnan vastaus EV 15/2025 vp

sekä koordinoi useisiin toimijoihin vaikuttavien haavoittuvuuksien hallintaa. Lisäksi CSIRT-yksikkö ohjaa ja neuvoa tietojen ilmoittamisessa Euroopan haavoittuvuustietokantaan ja tietojen hakemisessa siitä.

CSIRT-yksiköllä on oikeus ilmoittaa Euroopan haavoittuvuustietokantaan haavoittuvuuksista tiedot:

- 1) jotka sisältävät kuvauksen haavoittuvuudesta;
- 2) TVT-tuotteista tai -palveluista, joihin haavoittuvuus vaikuttaa, sekä haavoittuvuuden vakavuus niiden olosuhteiden perusteella, joissa haavoittuvuutta voidaan hyödyntää;
- 3) ohjelmistokorjausten saatavuudesta ja, jos niitä ei ole saatavilla, valvovan viranomaisen tai CSIRT-yksikön ohjeistuksesta haavoittuvien TVT-tuotteiden tai -palveluiden käyttäjille siitä, miten julkistetusta haavoittuvuudesta johtuvia riskejä voidaan vähentää.

Jos CSIRT-yksikkö saa tiedon sellaisesta haavoittuvuudesta, jolla voi olla merkittävä vaikutus muihin Euroopan unionin jäsenvaltioihin, sen on tehtävä yhteistyötä kyseisten valtioiden CSIRT-yksiköiden kanssa CSIRT-verkostossa.

23 §

Kyberturvallisuustietojen vapaaehtoiset jakamisjärjestelyt

CSIRT-yksikön, toimijoiden ja muiden kuin tämän lain soveltamisalaan kuuluvien yhteisöiden välillä voidaan muodostaa CSIRT-yksikön koordinoimia kyberturvallisuustietojen vapaaehtoisia jakamisjärjestelyitä niihin osallistuvien yhteisöjen sekä niiden asiakkaiden viestintäverkkoihin, tietojärjestelmiin tai palveluihin kohdistuvien kyberuhkien ehkäisemiseksi ja havaitsemiseksi, poikkeamien hallitsemiseksi ja niistä palautumiseksi ja niiden vaikutusten lieventämiseksi.

Kyberturvallisuustietojen vapaaehtoiseen jakamisjärjestelyyn osallistuvien kesken voidaan luovuttaa tietoja:

- 1) kyberuhkista;
- 2) poikkeamista ja läheltä piti -tilanteista;
- 3) haavoittuvuuksista;
- 4) taktiikoista, tekniikoista ja menettelyistä;
- 5) vaarantumisindikaattoreista;
- 6) yksittäisistä uhkatoimijoista;
- 7) kyberturvallisuushälytyksistä;
- 8) muista kuin 1—7 kohdassa tarkoitetuista kyberuhkien ja poikkeamien torjumiseksi tarpeellisista seikoista.

Sen lisäksi, mitä sähköisen viestinnän palveluista annetun lain 319 §:ssä säädetään tietojen luovuttamisesta, CSIRT-yksikkö voi luovuttaa jakamisjärjestelyyn osallistuvalla tämän lain mukaisia tehtäviä suorittaessaan saamansa tiedon kyberuhkaan tai poikkeamaan liittyvästä välitystiedosta tai haitallisen tietokoneohjelman tai käskyn sisältävästä viestistä.

Jakamisjärjestelyihin osallistuva toimija tai muu yhteisö saa sähköisen viestinnän palveluista annetun lain 136 §:n 4 momentin estämättä luovuttaa oma-aloitteisesti CSIRT-yksikölle ja toiselle tämän lain mukaiseen vapaaehtoiseen jakamisjärjestelyyn osallistuvalla tietoa kyberuhkaan tai poikkeamaan liittyvästä välitystiedosta tai haitallisen tietokoneohjelman tai käskyn sisältävästä viestistä.

Jakamisjärjestelyihin osallistuva saa käsitellä tämän pykälän nojalla saamaansa kyberuhkaan tai poikkeamaan liittyvää välitystietoa tai haitallisen tietokoneohjelman tai käskyn sisältävää

Eduskunnan vastaus EV 15/2025 vp

viestiä koskevaa tietoa vain 1 momentissa tarkoitettuihin tarkoituksiin. CSIRT-yksikkö voi lisäksi käsitellä tämän pykälän nojalla saamia tietoa 20 §:n 1 momentissa säädetyn tehtävänsä hoitamiseksi. Tiedon luovuttamisella ei saa rajoittaa luottamuksellisen viestin ja yksityisyyden suojaa enempää kuin on välttämätöntä 1 momentissa säädetyn tarkoituksen vuoksi.

24 §

Tietoturvaloukkausten havainnointipalveluun liittyvä tiedonkäsittely

Tietoturvaloukkausten havainnointipalvelua käyttävä toimija, muu yhteisö, palvelukeskus ja CSIRT-yksikkö saavat luovuttaa toisilleen viestintäverkkojen ja tietojärjestelmien tietoturvallisuuden seurannan kannalta tarpeellisia tietoja kyberuhkien ehkäisemiseksi ja havaitsemiseksi sekä poikkeamien hallitsemiseksi, niistä palautumiseksi ja niiden vaikutusten lieventämiseksi. Siinä määrin kuin tietoturvaloukkausten havainnointipalvelun toteuttamiseksi on välttämätöntä, luovutettavat tiedot saavat sisältää palvelua käyttävän toimijan tai muun yhteisön palvelussa käsiteltäväksi pyytämiä sellaisia sähköisiä viestejä tai niihin liittyviä välitystietoja, joita sillä on oikeus käsitellä sähköisen viestinnän palveluista annetun lain 272 §:n nojalla.

Välitystietojen ja sähköisten viestien käsittelyyn tietoturvaloukkausten havainnointipalvelussa CSIRT-yksikössä ja palvelukeskuksessa sovelletaan, mitä sähköisen viestinnän palveluista annetun lain 136—138, 145 ja 272 §:ssä säädetään. CSIRT-yksikkö saa lisäksi käyttää palvelun tuottamisen yhteydessä saamia välitystietoja ja muita tietoja kansallisen kyberturvallisuuden tilannekuvan ylläpitämisen tukemiseksi.

Mitä sähköisen viestinnän palveluista annetun lain 316 §:n 4 momentissa säädetään merkittävien tietoturvaloukkausten tai -uhkien selvittämistä koskevien tietojen hävittämisestä ja 319 §:n 1 momentissa salassapitovelvollisuudesta, koskee myös CSIRT-yksikölle tietoturvaloukkausten havainnointipalvelun toteuttamiseksi luovutettuja viestejä ja välitystietoja.

25 §

CSIRT-yksikölle vapaaehtoisesti luovutettu tieto

Siitä riippumatta, mitä viranomaisten tiedonsaantioikeuksista muualla laissa säädetään, CSIRT-yksikölle tämän lain mukaisten tehtävien hoitamiseksi vapaaehtoisesti luovutettua tietoa ei saa ilman tiedon luovuttaneen suostumusta käyttää tiedon luovuttajaan kohdistuvassa rikostutkinnassa eikä hallinnollisessa tai muussa tiedon luovuttajaan kohdistuvassa päätöksenteossa.

Eduskunnan vastaus EV 15/2025 vp

4 luku

Valvonta

26 §

Valvovat viranomaiset

Tämän lain, sen nojalla annettujen määräysten ja NIS 2 -direktiivin nojalla annettujen säännösten noudattamista valvoo:

1) Liikenne- ja viestintävirasto siltä osin kuin kyse on liitteen I kohdissa 1—7 ja liitteen II kohdissa 1—5 tarkoitetuista toimijoista;

2) Energiavirasto siltä osin kuin kyse on liitteen I kohdissa 8 ja 9 sekä kohdan 10 alakohdissa a—c ja kohdan 12 alakohdassa b tarkoitetuista toimijoista;

3) Turvallisuus- ja kemikaalivirasto siltä osin kuin kyse on liitteen I kohdan 10 alakohdissa d—g, kohdassa 11, kohdan 12 alakohdassa a sekä liitteen II kohdissa 6 ja 11—13 tarkoitetuista toimijoista;

4) Sosiaali- ja terveystieteiden lupa- ja valvontavirasto siltä osin kuin kyse on liitteen I kohdan 13 alakohdissa a ja b tarkoitetuista toimijoista;

5) Etelä-Savon elinkeino-, liikenne- ja ympäristökeskus siltä osin kuin kyse on liitteen I kohdissa 14—15 sekä liitteen II kohdassa 8 tarkoitetuista toimijoista;

6) Ruokavirasto siltä osin kuin kyse on liitteen II kohdassa 7 tarkoitetuista toimijoista;

7) Lääkealan turvallisuus- ja kehittämiskeskus siltä osin kuin kyse on liitteen I kohdan 13 alakohdissa c—f ja liitteen II kohdissa 9 ja 10 tarkoitetuista toimijoista.

Valvovien viranomaisten on tehtävä yhteistyötä valvonnan toteuttamisessa.

27 §

Valvonnan kohdistaminen

Valvonta on kohdistettava keskeisiin toimijoihin. Valvova viranomainen voi kuitenkin kohdistaa valvontaa myös muuhun kuin keskeiseen toimijaan, jos on perusteltu syy epäillä, että tämä ei ole noudattanut tätä lakia, sen nojalla annettuja määräyksiä tai NIS 2 -direktiivin nojalla annettuja säännöksiä.

Keskeisellä toimijalla tarkoitetaan:

1) liitteessä I tarkoitettua toimijaa, joka ylittää mikroyritysten sekä pienten ja keskisuurten yritysten määritelmästä annetun komission suosituksen 2003/361/EY liitteen 2 artiklan mukaiset keskisuuria yrityksiä koskevat edellytykset;

2) hyväksytyjä luottamuspalvelun tarjoajia, aluetunnusrekisterin ylläpitäjiä sekä DNS-palveluntarjoajia;

3) yleisten sähköisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajia, jotka täyttävät tai ylittävät mikroyritysten sekä pienten ja keskisuurten yritysten määritelmästä annetun komission suosituksen 2003/361/EY liitteen 2 artiklan mukaiset keskisuuria yrityksiä koskevat edellytykset; sekä

4) 3 §:n 3 momentissa tarkoitettua toimijaa.

Eduskunnan vastaus EV 15/2025 vp

Valvova viranomainen voi asettaa sille tässä laissa säädetty tehtävät tärkeysjärjestykseen riskiperusteisesti. Valvovan viranomaisen on otettava valvonnan kohdistamisessa ja 29—34 §:ssä tarkoitettujen toimien käyttämisestä päättäessään huomioon:

- 1) liitteessä I tai II tarkoitettun toiminnan laatu ja laajuus;
- 2) tietojärjestelmän tai viestintäverkon merkitys liitteessä I tai II tarkoitettulle toiminnalle; ja
- 3) 37 §:ssä tarkoitettut seikat.

28 §

Tiedonsaantioikeus

Valvovalla viranomaisella on salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus saada toimijalta 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.

Valvovalla viranomaisella on salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus saada toimijalta 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.

Valvovan viranomaisen on tietopyynnössä ilmoitettava pyynnön tarkoitus sekä täsmennettävät pyydetyt tiedot. Tiedot on luovutettava viipymättä, viranomaisen pyytämässä muodossa ja maksutta.

Valvovalla viranomaisella on salassapitosäännösten, 2 momentissa säädetyn salassapitovelvollisuuden ja muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus luovuttaa tässä laissa säädettyjen tehtäviensä hoitamisen yhteydessä saamansa tai laatimansa asiakirja sekä ilmaista salassa pidettävä tieto toiselle valvovalle viranomaiselle ja CSIRT-yksikölle, jos se on välttämätöntä viranomaiselle tässä laissa säädettyä tehtävää varten. Tiedonsaantioikeuden käytämisellä tai tietojen luovuttamisella ei saa rajoittaa luottamuksellisen viestin ja yksityisyyden suojaa enempää kuin on välttämätöntä.

Valvovan viranomaisen tiedonsaantioikeus ei koske CSIRT-yksikön tämän lain nojalla tuottamia palveluita eikä tietoja toimijassa.

Tässä pykälässä tarkoitettu tiedonsaantioikeus ei koske salassa pidettäviä tietoja julkisen hallinnon turvallisuusverkko-toiminnasta annetussa laissa (10/2015) tarkoitettua turvallisuusverkon palvelutuotannosta tai palvelujen käytöstä eikä tietoja, joiden luovuttaminen vaarantaisi maanpuolustusta tai kansallista turvallisuutta taikka olisi vastoin niihin liittyvää tärkeää etua.

29 §

Tarkastusoikeus

Valvovalla viranomaisella on oikeus tehdä toimijaa koskeva tarkastus. Tarkastus tehdään tässä laissa tai sen nojalla annetussa määräyksessä taikka NIS 2 -direktiivin nojalla annetuissa sään-

Eduskunnan vastaus EV 15/2025 vp

nöksissä säädettyjen velvollisuuksien noudattamisen valvomiseksi siinä laajuudessa kuin se on tarpeen.

Jos se on tarkastuksen laadun tai siihen liittyvien teknisten syiden vuoksi tarpeellista, valvova viranomainen voi pyytää tarkastuksen suorittajaksi toisen valvovan viranomaisen tai käyttää tarkastuksessa apuna toista valvovaa viranomaista, tietoturvallisuuden arviointilaitosta ja ulkopuolista tietotekniikan asiantuntijaa. Tarkastuksen suorittajalla ja siihen osallistuvalla on oltava sellainen koulutus ja kokemus kuin tarkastuksen suorittamiseksi on tarpeen. Ulkopuoliseen asiantuntijaan sovelletaan rikosoikeudellista virkavastuuta koskevia säännöksiä hänen hoitaessaan tämän pykälän mukaisia tehtäviä. Vahingonkorvausvastuusta säädetään vahingonkorvauslaissa (412/1974).

Toimijoiden on tarkastusta varten päästettävä tarkastusta suorittava tarkastuksen edellyttämässä laajuudessa tarkastuksen kohteena olevaan viestintäverkkoon tai tietojärjestelmään ja muihin kuin pysyväisluonteiseen asumiseen tarkoitettuihin tiloihin. Tarkastuksen suorittamiseksi valvovalla viranomaisella, tarkastusta suorittavalla toisella viranomaisella, tietoturvallisuuden arviointilaitoksella ja ulkopuolisella asiantuntijalla 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 toimijan toteuttamat turvallisuusjärjestelyt. Tarkastuksen suorittajan tarkastus- ja tiedonsaantioikeuteen sovelletaan mitä 28 §:n 6 momentissa säädetään tiedonsaantioikeuden rajoituksista.

Tarkastuksessa noudatettavaan menettelyyn sovelletaan, mitä hallintolain (434/2003) 39 §:ssä säädetään tarkastuksesta.

30 §

Turvallisuusauditointi

Valvovalla viranomaisella on oikeus velvoittaa toimija teettämään kyberturvallisuuden riskienhallintaan kohdistuva turvallisuusauditointi, jos:

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

2) toimija on olennaisesti ja vakavasti laiminlyönyt toteuttaa 8 §:ssä tarkoitetun kyberturvallisuutta koskevan riskienhallinnan toimintamallin tai siinä edellytetyjä hallintatoimenpiteitä taikka muutoin olennaisesti ja vakavasti toiminut tässä laissa tai sen nojalla taikka NIS 2 -direktiivin nojalla säädetyn velvollisuuden vastaisesti.

Valvovalla viranomaisella on oikeus saada tieto teetetyn turvallisuusauditoinnin tuloksista sekä velvoittaa toimija toteuttamaan turvallisuusauditoinnin suosittelemat kohtuulliset ja oikeasuhtaiset toimenpiteet kyberturvallisuutta koskevan riskienhallinnan kehittämiseksi.

31 §

Valvontapäätös ja varoitus

Valvova viranomainen voi velvoittaa toimijan määräajassa korjaamaan puutteet tässä laissa tai sen nojalla annetuissa määräyksissä taikka NIS 2 -direktiivin nojalla annetuissa säännöksissä säädettyjen velvollisuuksien noudattamisessa. Valvova viranomainen voi päätöksellä velvoittaa toi-

Eduskunnan vastaus EV 15/2025 vp

mijan julkistamaan kyseiset puutteet tai muut seikat, jotka liittyvät tämän lain, sen nojalla annettujen määräysten tai NIS 2 -direktiivin nojalla annettujen säännösten rikkomiseen.

Valvova viranomainen voi antaa toimijalle varoituksen, jos tämä ei ole noudattanut tätä lakia, sen nojalla annettuja määräyksiä tai NIS 2 -direktiivin nojalla annettuja säännöksiä. Varoituksessa on yksilöitävä puute tai laiminlyönti, jota se koskee. Varoitus on annettava kirjallisena.

32 §

Johdon toiminnan rajoittaminen

Valvova viranomainen voi kieltää määrääjäksi henkilöä toimimasta keskeisen toimijan hallituksen jäsenenä tai varajäsenenä, hallintoneuvoston jäsenenä tai varajäsenenä, toimitusjohtajana tai muussa siihen rinnastettavassa asemassa, jos tämä on toistuvasti ja vakavasti rikkonut 10 §:ssä säädettyjä velvollisuuksia. Valvovan viranomaisen on ennen päätöksen tekemistä annettava keskeiselle toimijalle varoitus, jossa yksilöidään puute tai laiminlyönti, jonka korjaamatta jättäminen voi johtaa päätökseen johdon toiminnan rajoittamisesta, sekä varattava toimijalle kohtuullinen määräaika puutteen tai laiminlyönnin korjaamiseksi. Päätös saa olla voimassa enintään niin kauan, kuin sen perusteena oleva puute tai laiminlyönti on korjaamatta, kuitenkin enintään viisi vuotta.

Edellä 1 momentissa säädetystä poiketen johdon toimintaa ei saa rajoittaa, jos kyse on yksityisestä elinkeinonharjoittajasta, avoimesta yhtiöstä, kommandiittiyhtiöstä, valtion viranomaisesta, valtion liikelaitoksesta, hyvinvointialueesta tai -yhtymästä, kunnallisesta viranomaisesta, itsenäisestä julkisoikeudellisesta laitoksesta, eduskunnan virastosta, tasavallan presidentin kansliasta, Suomen evankelis-luterilaisesta kirkosta, Suomen ortodoksisesta kirkosta tai niiden seurakunnista, seurakuntayhtymistä taikka muista elimistä.

33 §

Ilmoitus tietosuojavaltuutetulle

Jos valvova viranomainen saa tässä laissa tarkoitettujen tehtävien hoitamisen yhteydessä tietoonsa, että 2 luvussa säädettyjen velvollisuuksien laiminlyönti voi johtaa tai on johtanut yleisessä tietosuojasetuksessa tarkoitettuun henkilötietojen tietoturvaloukkaukseen, josta on mainitun asetuksen 33 artiklan nojalla ilmoitettava asetuksessa tarkoitettulle valvontaviranomaiselle, valvovan viranomaisen on ilmoitettava asiasta tietosuojavaltuutetulle.

Valvovan viranomaisen on tehtävä 1 momentissa tarkoitettu ilmoitus tietosuojavaltuutetulle myös, jos yleisen tietosuojasetuksen nojalla toimivaltainen valvontaviranomainen on sijoittunut toiseen jäsenvaltioon.

34 §

Uhkasakko, teettämisuhka ja keskeyttämisuhka

Valvova viranomainen voi asettaa tämän lain nojalla antamansa päätöksen tehosteeksi uhkasakon, teettämisuhan tai keskeyttämisuhan.

Eduskunnan vastaus EV 15/2025 vp

5 luku

Seuraamusmaksu

35 §

Hallinnollinen seuraamusmaksu

Toimijalle voidaan määrätä hallinnollinen seuraamusmaksu, jos se tahallaan tai törkeästä huolimattomuudesta laiminlyö:

1) 7 §:ssä tarkoitetun velvollisuuden hallita riskejä, 8 §:ssä tarkoitetun kyberturvallisuutta koskevan riskienhallinnan toimintamallin laatimisen tai 9 §:n 1 momentissa tarkoitettujen osa-alueiden huomioimisen osana kyberturvallisuuden riskienhallinnan toimintamallia;

2) toteuttaa 9 §:n 2 momentissa tarkoitetut toimenpiteet;

3) antaa 11 §:ssä tarkoitetun poikkeamailmoituksen, 12 §:ssä tarkoitetun väliraportin tai 13 §:ssä tarkoitetun loppuraportin valvovalle viranomaiselle;

4) antaa 41 §:ssä tarkoitetut tiedot valvovalle viranomaiselle.

Seuraamusmaksua ei voi määrätä valtion viranomaisille, valtion liikelaitoksille, hyvinvointialueille eikä -yhtymille, kunnallisille viranomaisille, itsenäisille julkisoikeudellisille laitoksille, eduskunnan virastoille, tasavallan presidentin kanslialle eikä Suomen evankelis-luterilaiselle kirkolle ja Suomen ortodoksiselle kirkolle eikä niiden seurakunnille, seurakuntayhtymille ja muille elimille.

36 §

Seuraamusmaksulautakunta

Liikenne- ja viestintäviraston yhteydessä toimii seuraamusmaksulautakunta. Lautakunta määrää hallinnollisen seuraamusmaksun valvovan viranomaisen esityksestä. Hallinnollinen seuraamusmaksu määrätään maksettavaksi valtiolle.

Liikenne- ja viestintävirasto nimeää lautakunnan puheenjohtajan ja varapuheenjohtajan. Kunkin valvova viranomainen nimeää lautakuntaan jäsenen ja tälle henkilökohtaisen varajäsenen. Lautakunnan jäseneltä ja varajäseneltä edellytetään perehtyneisyyttä kyberturvallisuutta koskevien riskien hallintaan sekä NIS 2 -direktiiviin ja sitä täytäntöönpanevassa sääntelyssä asetettuihin velvollisuuksiin nimeävän viranomaisen valvontatoimialalla. Lautakunnan puheenjohtajalla ja varapuheenjohtajalla tulee olla tehtävän edellyttämä riittävä oikeudellinen asiantuntemus. Lautakunnan jäsenet nimetään kolmen vuoden määräajaksi. Lautakunnan jäsen toimii tehtävässään riippumattomasti ja puolueettomasti.

Seuraamusmaksulautakunnan päätös tehdään esittelystä. Esittelijänä toimii sen valvovan viranomaisen virkamies, jonka valvontatoimivaltaan kohdistuva asia on ratkaistavana. Lautakunta on päätösvaltainen, kun paikalla on puheenjohtaja tai varapuheenjohtaja ja vähintään kaksi muuta jäsentä tai varajäsentä. Päätökseksi tulee se kanta, jota enemmistö on kannattanut. Äänten mennessä tasan päätökseksi tulee se kanta, joka on lievempi sille, johon seuraamus kohdistuu.

Seuraamusmaksulautakunnalla on oikeus salassapitosäännösten estämättä saada maksutta seuraamusmaksun määräämiseksi välttämättömät 28 §:ssä tarkoitetut tiedot sekä muut tiedot, jotka ovat välttämättömiä seuraamusmaksun määräämiseksi tai sen määrän arvioimiseksi.

Eduskunnan vastaus EV 15/2025 vp

37 §

Seuraamusmaksun määrääminen

Hallinnollisen seuraamusmaksun määrä perustuu kokonaisarviointiin, jossa otetaan huomioon tapauksen olosuhteet sekä ainakin seuraavat seikat:

1) rikkomisen vakavuus ja rikottujen säännösten tärkeys siten, että rikkomisen vakavuutta osoittaa

- a) väärinkäytösten toistuvuus;
- b) merkittävien poikkeamien jättäminen ilmoittamatta tai korjaamatta;
- c) havaittujen puutteiden jättäminen korjaamatta valvovan viranomaisen päätöksistä tai varoituksista huolimatta;
- d) valvovan viranomaisen tarkastuksen estäminen tai määrätyn auditoinnin teettämättä jättäminen;
- e) riskienhallinnasta tai merkittävistä poikkeamista viranomaiselle liittyvien väärin tai harhaanjohtavien tietojen antaminen;

- 2) rikkomisen kesto;
- 3) toimijan mahdolliset vastaavat aiemmat rikkomiset;
- 4) aiheutunut vahinko, mukaan lukien rahoitukseen liittyvät tai taloudelliset tappiot, vaikutukset muihin palveluihin sekä niiden käyttäjien lukumäärä, joihin rikkominen vaikuttaa;
- 5) tahallisuuden aste;
- 6) toimenpiteet, jotka toimija on toteuttanut vahingon ehkäisemiseksi tai lieventämiseksi;
- 7) hyväksytyjen käytäntöjen tai hyväksytyjen sertifiointimekanismien noudattaminen;
- 8) toimijan halukkuus tehdä yhteistyötä valvovan viranomaisen kanssa.

38 §

Seuraamusmaksun enimmäismäärä

Keskeiselle toimijalle määrättävän hallinnollisen seuraamusmaksun enimmäismäärä on 10 000 000 euroa tai kaksi prosenttia toimijan edellisen tilikauden maailmanlaajuisesta vuotuisesta kokonaisliikevaihdosta sen mukaan, kumpi näistä määristä on suurempi.

Muulle kuin keskeiselle toimijalle määrättävän hallinnollisen seuraamusmaksun enimmäismäärä on 7 000 000 euroa tai 1,4 prosenttia toimijan edellisen tilikauden maailmanlaajuisesta vuotuisesta kokonaisliikevaihdosta sen mukaan, kumpi näistä määristä on suurempi.

39 §

Seuraamusmaksun määräämättä jättäminen

Seuraamusmaksu jätetään määräämättä, jos:

1) toimija on oma-aloitteisesti ryhtynyt riittäviin toimenpiteisiin rikkomuksen tai laiminlyönnin korjaamiseksi välittömästi sen havaitsemisen jälkeen ja ilmoittanut siitä viivytyksettä valvovalle viranomaiselle sekä toiminut yhteistyössä valvovan viranomaisen kanssa eikä rikkominen tai laiminlyönti ole vakava tai toistuva;

2) rikkomusta tai laiminlyöntiä on pidettävä vähäisenä; tai

Eduskunnan vastaus EV 15/2025 vp

3) seuraamusmaksun määräämistä on pidettävä ilmeisen kohtuuttomana muutoin kuin 1 tai 2 kohdassa tarkoitetulla perusteella.

Seuraamusmaksua ei saa määrätä, jos on kulunut yli viisi vuotta siitä, kun rikkomus tai laiminlyönti on tapahtunut. Jos rikkomus tai laiminlyönti on ollut luonteeltaan jatkuvaa, määräaika lasketaan siitä, kun rikkomus tai laiminlyönti on päättynyt.

Seuraamusmaksua ei saa määrätä sille, jota epäillään samasta teosta esitutkinnassa, syyteharkinnassa tai tuomioistuimessa vireillä olevassa rikosasiassa. Seuraamusmaksua ei saa määrätä myöskään sille, jolle on samasta teosta annettu lainvoimainen tuomio.

Seuraamusmaksua ei saa määrätä sille, jolle on määrätty samasta teosta yleisen tietosuoja-asetuksen 83 artiklassa tarkoitettu seuraamusmaksu.

40 §

Seuraamusmaksun täytäntöönpano

Seuraamusmaksun täytäntöönpanosta säädetään sakon täytäntöönpanosta annetussa laissa (672/2002). Seuraamusmaksu vanhenee viiden vuoden kuluttua lainvoiman saaneen päätöksen antamispäivästä. Seuraamusmaksu raukeaa, kun maksuvelvollinen luonnollinen henkilö kuolee.

6 luku

Muut säännökset

41 §

Toimijaluettelo

Valvova viranomainen ylläpitää valvontatoimialansa osalta toimijaluetteloa.

Toimijoiden on ilmoitettava valvovalle viranomaiselle:

- 1) toimijan nimi;
- 2) osoitteensa, sähköpostiosoitteensa, puhelinnumeron ja muut ajantasaiset yhteystietonsa;
- 3) IP-osoitealueensa;
- 4) NIS 2 -direktiivin liitteessä I tai II tarkoitettu asiaankuuluva toimialansa ja sen osa;
- 5) tieto siitä, onko se keskeinen toimija;
- 6) luettelo niistä Euroopan unionin jäsenvaltioista, joissa se tarjoaa NIS 2 -direktiivin soveltamisalaan kuuluvia palveluja; ja
- 7) osallistumisesta 23 §:ssä tarkoitettuun kyberturvallisuustietojen vapaaehtoiseen jakamisjärjestelyyn.

DNS-palveluntarjoajien, aluetunnusrekisterin ylläpitäjien, pilvipalvelujen tarjoajien, datakeskuspalvelujen tarjoajien, sisällönjakeluverkkojen tarjoajien, hallintapalvelun tarjoajien, tietoturvapalveluntarjoajien, verkossa toimivien markkinapaikkojen tarjoajien, verkossa toimivien hakukoneiden tarjoajien ja verkkoyhteisöalustojen tarjoajien on ilmoitettava valvovalle viranomaiselle 2 momentissa tarkoitettujen tietojen lisäksi:

- 1) NIS 2 -direktiivin liitteessä I tai II tarkoitettu toimijatyyppinsä;

Eduskunnan vastaus EV 15/2025 vp

2) päätoimipaikkansa ja muiden Euroopan unionin jäsenvaltiossa sijaitsevien laillisten toimipaikkojensa osoite tai, jos toimija ei ole sijoittautunut Euroopan unioniin, sen Euroopan unioniin nimetyn edustajan osoite, sähköpostiosoite, puhelinnumero ja muut ajantasaiset yhteystiedot; ja

3) luettelo Euroopan unionin jäsenvaltioista, joissa toimija tarjoaa palveluita.

Toimijoiden on ilmoitettava muutoksista tässä pykälässä tarkoitettuihin tietoihin viipymättä. Muutoksesta 2 momentissa tarkoitettuihin tietoihin on ilmoitettava valvovalle viranomaiselle kahden viikon kuluessa ja 3 momentissa tarkoitettuihin tietoihin kolmen kuukauden kuluessa muutoshetkestä. Valvova viranomainen voi antaa tarkempia teknisiä määräyksiä tietojen ilmoittamisesta.

Valvovan viranomaisen on toimitettava keskitetylle yhteyspisteelle NIS 2 -direktiivin 3 artiklan 5 kohdassa ja 27 artiklan 4 kohdassa tarkoitettujen ilmoituksien tekemiseksi tarpeelliset tiedot toimijaluettelosta. Keskitetty yhteyspiste vastaa mainituissa kohdissa tarkoitettujen ilmoituksien tekemisestä Euroopan komissiolle, NIS-yhteistyöryhmälle ja Euroopan unionin kyberturvallisuusvirastolle. CSIRT-yksiköllä on oikeus saada valvovalta viranomaiselta tietoja toimijaluettelosta.

42 §

Kansallinen kyberturvallisuusstrategia

Valtioneuvosto hyväksyy kansallisen kyberturvallisuusstrategian ja vastaa sen päivittämisestä säännöllisesti vähintään viiden vuoden välein.

Kansalliseen kyberturvallisuusstrategiaan on sisällytettävä vähintään NIS 2 -direktiivin 7 artiklan 1 kohdassa tarkoitettut osa-alueet ja 2 kohdassa tarkoitettut toimintaperiaatteet.

Valtioneuvosto antaa kansallisen kyberturvallisuusstrategian tiedoksi Euroopan komissiolle kolmen kuukauden kuluessa sen hyväksymisestä. Kyberturvallisuusstrategiasta voidaan jättää antamatta tietoja, joiden luovuttaminen vaarantaisi maanpuolustusta tai kansallista turvallisuutta taiikka olisi vastoin niihin liittyvää tärkeää etua.

43 §

Laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien hallintasuunnitelma

Kyberturvallisuutta koskevissa kriisitilanteissa käytettävissä olevien valmiuksien, voimavarojen ja menettelyiden yksilöimiseksi laaditaan laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien hallintasuunnitelma. Liikenne- ja viestintävirasto vastaa suunnitelman laatimisesta yhteistoiminnassa 26 §:ssä tarkoitettujen valvovien viranomaisten, poliisin, suojelupoliisin, Puolustusvoimien ja Huoltovarmuuskeskuksen kanssa.

Suunnitelman tulee sisältää laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien hallitsemiseksi tarpeelliset tiedot:

- 1) kansallisten varautumiskeinojen ja -toimien tavoitteista;
- 2) viranomaisten tehtävistä ja vastuista;
- 3) kriisinhallintaa koskevista toimintatavoista ja niiden sisällyttämisestä yleiseen kansalliseen kriisinhallintakehykseen sekä tiedonvaihtokanavista viranomaisten välillä;
- 4) kansallisista varautumiskeinoista, joihin kuuluvat myös harjoitukset ja koulutustoimenpiteet;

Eduskunnan vastaus EV 15/2025 vp

- 5) keskeisistä julkisista ja yksityisistä sidosryhmistä ja keskeisestä infrastruktuurista;
6) viranomaisten välisestä menettelystä osallistuttaessa laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien koordinoituun hallintaan Euroopan unionin tasolla.

Edellä 2 momentissa tarkoitettut tiedot on annettava tiedoksi Euroopan komissiolle ja NIS 2 -direktiivin 16 artiklassa tarkoitettulle Euroopan kyberkriisien yhteysorganisaatioiden verkostolle kolmen kuukauden kuluessa suunnitelman hyväksymisestä. Tietoja voidaan jättää antamatta siltä osin, jos niiden luovuttaminen vaarantaisi maanpuolustusta tai kansallista turvallisuutta taikka olisi vastoin niihin liittyvää tärkeää etua.

44 §

Kyberkriisinhallintaviranomainen

NIS 2 -direktiivin 9 artiklan 1 kohdan kohdassa tarkoitettuna kyberkriisinhallintaviranomaisena toimii kukin 43 §:n 1 momentissa tarkoitettu viranomainen sille laissa säädettyjen tehtävien mukaisesti. Liikenne- ja viestintäviraston Kyberturvallisuuskeskus toimii koordinaattorina laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien hallinnassa.

45 §

Viranomaisten yhteistyö

Valvovien viranomaisten, CSIRT-yksikön ja keskitetyn yhteyspisteen on toimittava yhteistyössä tässä laissa ja NIS 2 -direktiivin nojalla säädettyjen tehtävien hoitamiseksi.

Valvovien viranomaisten, CSIRT-yksikön ja keskitetyn yhteyspisteen on toimittava tarvittaessa yhteistyössä poliisin tai muun esitutkintaviranomaisen, tietosuojavaltuutetun, Liikenne- ja viestintäviraston sille ilmailulaissa (864/2014), sähköisen viestinnän palveluista annetussa laissa ja eIDAS-asetuksessa säädettyjen tehtävien osalta ja Finanssivalvonnan kanssa.

Valvovien viranomaisten on ilmoitettava DORA-asetuksen 32 artiklan 1 kohdan nojalla perustetulle valvontafoorumille, kun ne käyttävät valvonta- ja täytäntöönpanovaltuuksiaan toimijaan, joka on nimetty kriittiseksi TVT-palveluntarjoajana olevaksi kolmanneksi osapuoleksi DORA-asetuksen 31 artiklan nojalla.

Valvovien viranomaisten, Liikenne- ja viestintäviraston ja Finanssivalvonnan on vaihdettava keskenään säännöllisesti tietoja merkittävistä poikkeamista ja kyberuhkista.

46 §

Muutoksenhaku

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

Valvovan viranomaisen tekemää päätöstä on noudatettava muutoksenhausta huolimatta, ellei muutoksenhakuviranomainen toisin määrää. Muutoksenhausta uhkasakon asettamista ja maksettavaksi tuomitsemista sekä teettämis- tai keskeyttämisuhan asettamista ja täytäntöönpantavaksi määräämistä koskevaan päätökseen sovelletaan kuitenkin, mitä uhkasakkolaissa (1113/1990) säädetään.

Eduskunnan vastaus EV 15/2025 vp

47 §

Voimaantulo

Tämä laki tulee voimaan päivänä kuuta 20 .

Tämän lain 41 §:ssä tarkoitettu ilmoitus on tehtävä viimeistään kuukauden kuluessa lain voimaantulosta tai siitä, kun 3 §:n mukaiset toimijan kriteerit täyttyvät.

Tämän lain 8 §:ssä tarkoitettu riskienhallinnan toimintamalli on laadittava kolmen kuukauden kuluessa lain voimaantulosta tai siitä, kun 3 §:n mukaiset toimijan kriteerit täyttyvät.

Toimijat, jotka harjoittavat seuraavaa toimintaa tai ovat seuraavaa toimijatyyppejä:

1. Ilmaliikenne:

- a) Yhteisistä siviili-ilmailun turvaamista koskevista säännöistä ja asetuksen (EY) N:o 2320/2002 kumoamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 300/2008 3 artiklan 4 alakohdassa määritelty lentoliikenteen harjoittajat, joiden toiminta on kaupallista
- b) Lentoasemaverkoista ja -maksuista annetun lain (210/2011) 3 §:n 1 momentin 2 kohdassa tarkoitetut lentoaseman pitäjät
- c) Yhtenäisen eurooppalaisen ilmatilan toteuttamisen puitteista annetun Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 549/2004 2 artiklan 1 alakohdassa määriteltyä lennonjohtopalvelua tarjoavat lennonjohtopalvelun tarjoajat

2. Raideliikenne:

- a) Raideliikennelain (1302/2018) 4 §:n 1 momentin 29 kohdassa tarkoitetut rataverkon haltijat ja liikenteenohjauspalvelua tarjoavat yhtiöt
- b) Raideliikennelain 4 §:n 1 momentin 34 kohdassa tarkoitetut rautatieyritykset
- c) Raideliikennelain 4 §:n 1 momentin 23 kohdassa tarkoitetut palvelupaikan ylläpitäjät

3. Vesiliikenne:

- a) Alusten ja satamarakenteiden turvatoimien parantamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 725/2004 liitteessä I merenkulun osalta määritelty sisävesillä, merillä ja rannikoilla matkustaja- ja rahtiliikennettä hoitavat yhtiöt, lukuun ottamatta tällaisten yhtiöiden liikennöimiä yksittäisiä aluksia
- b) Eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annetun lain (485/2004) 2 §:n 2 kohdassa tarkoitetut satamanpitäjät sekä toimijat, jotka huolehtivat rakenteista ja varusteista sataman alueella
- c) Alusliikennepalvelulain (623/2005) 2 §:n 1 momentin 5 kohdassa tarkoitetut VTS-palvelun tarjoajat

4. Tieliikenne:

- a) Liikenteen palveluista annetun lain (320/2017) 15 luvussa tarkoitetun tieliikenteen ohjaus- ja hallintapalvelun tarjoaja
- b) Liikenteen palveluista annetun lain 160 §:ssä tarkoitettujen älykkäiden liikennejärjestelmien ylläpitäjät

5. Maa-asemista ja eräistä tutkista annetun lain (96/2023) 2 §:n 1 momentin 5 kohdassa tarkoitetut toiminnanharjoittajat; tai muut avaruuspohjaisten palvelujen tarjoamista tukevan, jäsenvaltioiden tai yksityisten tahojen omistaman, hallinnoiman ja operoiman maassa sijaitsevan infrastruktuurin ylläpitäjät, lukuun ottamatta yleisten sähköisten viestintäverkkojen tarjoajia

Eduskunnan vastaus EV 15/2025 vp

6. Digitaalinen infrastruktuuri:

a) Internetin yhdysliikennepisteiden, eli sellaisen verkkoinfrastruktuurin osan, joka mahdollistaa useamman kuin kahden riippumattoman verkon (*autonomisen järjestelmän*) yhdistämisen pääasiassa internetliikenteen välittämisen helpottamiseksi, joka tarjoaa yhteenliittantaa ainoastaan autonomisille järjestelmille ja joka ei edellytä minkään yhteenliittämänsä kahden autonomisen järjestelmän väliseltä internetliikenteeltä kulkemista minkään kolmannen autonomisen järjestelmän kautta eikä muokkaa tällaista liikennettä tai muutoin puutu siihen, ylläpitäjät

- b) DNS-palveluntarjoajat
- c) Aluetunnusrekisterin ylläpitäjät
- d) Pilvipalvelun tarjoajat
- e) Datakeskuspalvelun tarjoajat
- f) Sisällönjakeluverkon tarjoajat
- g) Luottamuspalvelun tarjoajat
- h) Yleisten sähköisten viestintäverkkojen tarjoajat
- i) Yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajat

7. TVT-palvelujen hallinta:

- a) Hallintapalvelun tarjoajat
- b) Tietoturvapalveluntarjoajat

8. Sähkö:

- a) Sähkömarkkinalain (588/2013) 3 §:n 1 momentin 21 kohdassa tarkoitetut sähköalan yritykset, jotka harjoittavat momentin 11 kohdassa tarkoitettua sähköntoimitusta
- b) Sähkömarkkinalain 3 §:n 1 momentin 10 kohdassa tarkoitetut jakeluverkonhaltijat
- c) Sähkömarkkinalain 7 §:n mukaiset kantaverkonhaltijat
- d) Sähkömarkkinalain 3 §:n 1 momentin 15 kohdassa tarkoitetut tuottajat
- e) Sähkön sisämarkkinoista annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/943 2 artiklan 8 alakohdassa määritellyt nimitetyt sähkömarkkinaoperaattorit
- f) Sähkömarkkinalain 3 §:n 1 momentin 37 kohdassa tarkoitetut sähkömarkkinoiden osapuolet, jotka tarjoavat sähkömarkkinalain 3 §:n 1 momentin 21 a kohdassa tarkoitettua aggregointia, 30 a kohdassa tarkoitettua kulutusjoustoja tai 21 c kohdassa tarkoitettua energian varastointia
- g) Latauspisteiden operaattorit, jotka vastaavat latauspalvelua loppukäyttäjille tarjoavan latauspisteen hallinnoinnista ja toiminnasta, myös liikennepalvelun tarjoajan nimissä ja puolesta

9. Uusiutuvista lähteistä peräisin olevan energian käytön edistämisestä annetun Euroopan parlamentin ja neuvoston direktiivin (EU) 2018/2001 2 kohdan 19 alakohdassa määritellyn kaukolämmityksen tai kaukojäähdytyksen haltijat

10. Kaasu:

- a) Maakaasumarkkinalain (587/2017) 3 §:n 1 momentin 10 kohdassa tarkoitetut jakeluverkonhaltijat
- b) Maakaasumarkkinalain 3 §:n 1 momentin 9 kohdassa tarkoitetut siirtoverkonhaltijat
- c) Maakaasumarkkinalain 3 §:n 1 momentin 14 kohdassa tarkoitetut maakaasun toimittajat
- d) Maakaasumarkkinalain 3 §:n 1 momentin 20 kohdassa tarkoitetut varastointilaitteiston haltijat

Eduskunnan vastaus EV 15/2025 vp

e) Maakaasumarkkinalain 3 §:n 1 momentin 22 kohdassa tarkoitettut nesteytetyn maakaasun käsittelylaitteiston haltijat

f) Maakaasumarkkinalain 3 §:n 1 momentin 18 kohdassa tarkoitettut maakaasualan yritykset

g) Maakaasun jalostus- ja käsittelylaitteistojen haltijat

11. Öljy:

a) Öljynsiirtoputkistojen haltijat

b) Öljyn tuotanto-, jalostus- ja käsittelylaitteistojen haltijat sekä öljyn varastointia ja siirtoa hoitavat operaattorit

c) Jäsenvaltioiden velvollisuudesta ylläpitää raakaöljy- ja/tai öljytuotevarastojen vähimmäistasoa annetun Neuvoston direktiivin 2009/119/EY 2 kohdan f alakohdassa määritellyt keskusvarastointiyksiköt

12. Vety:

a) Vedyn tuotantoa ja varastointia harjoittavat toimijat

b) Vedyn siirtoa harjoittavat toimijat

13. Terveys:

a) Sosiaali- ja terveydenhuollon valvonnasta annetun lain (741/2023) 4 §:n 2 kohdassa tarkoitettut palveluntuottajat, jotka tuottavat mainitun pykälän 4 kohdassa tarkoitettua terveyspalvelua

b) Rajatylittävistä vakavista terveysuhkista ja päätöksen N:o 1082/2013/EU kumoamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2022/2371 15 artiklassa tarkoitettut EU:n vertailulaboratoriot

c) Ihmisille tarkoitettuja lääkkeitä koskevista yhteisön säännöistä annetun Euroopan parlamentin ja neuvoston direktiivin 2001/83/EY 1 artiklan 2 alakohdassa määriteltyjen lääkkeiden tutkimusta ja kehitystä harjoittavat toimijat

d) NACE Rev. 2 -luokituksen C jakson kaksinumerotasossa 21 tarkoitettua lääkeaineiden ja lääkkeiden valmistusta harjoittavat toimijat

e) Euroopan lääkeviraston roolin vahvistamisesta kriisivalmiudessa ja -hallinnassa lääkkeiden ja lääkinnällisten laitteiden osalta annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2022/123 22 artiklassa tarkoitettuja vakavan kansanterveysuhan aikana kriittisiksi katsottuja lääkinnällisiä laitteita (kansanterveysuhan aikana kriittisten lääkinnällisten laitteiden luettelo) valmistavat toimijat

f) Veripalvelulain (197/2005) mukaiset veripalvelulaitokset, apteekit ja potilaiden oikeuksien soveltamisesta rajat ylittävässä terveydenhuollossa annetun Euroopan parlamentin ja neuvoston direktiivin 2011/24/EU mukaiset lääkkeitä ja lääkinnällisiä laitteita toimittavat ja tarjoavat toimijat

14. Ihmisten käyttöön tarkoitettun veden laadusta annetun Euroopan parlamentin ja neuvoston direktiivin (EU) 2020/2184 2 artiklan 1 alakohdan a alakohdassa määritellyn ihmisten käyttöön tarkoitettun veden toimittajat ja jakelijat, lukuun ottamatta jakelijoita, joille ihmisten käyttöön tarkoitettun veden jakelu ei ole keskeinen osa niiden yleistä toimintaa, joka muodostuu muiden hyödykkeiden ja tavaroiden jakelusta

Eduskunnan vastaus EV 15/2025 vp

15. Yhdyskuntajätevesien käsittelystä annetun Neuvoston direktiivin 91/271/ETY 2 artiklan 1, 2 ja 3 alakohdassa määriteltyä yhdyskuntajätevettä, talousjätevettä tai teollisuusjätevettä keräävät, hävittävät tai käsittelevät yritykset, lukuun ottamatta yrityksiä, joille yhdyskuntajäteveden, talousjäteveden tai teollisuusjäteveden kerääminen, hävittäminen tai käsittely ei ole keskeinen osa niiden yleistä toimintaa

Toimijat, jotka harjoittavat seuraavaa toimintaa tai ovat seuraavaa toimijatyyppejä:

1. Kuriiripalvelun tarjoajat ja yhteisön postipalvelujen sisämarkkinoiden kehittämistä ja palvelun laadun parantamista koskevista yhteisistä säännöistä annetun Euroopan parlamentin ja neuvoston direktiivin 97/67/EY 2 artiklan 1 a alakohdassa tarkoitettua postipalvelun tarjoajat

2. Digitaalisen palvelun tarjoajat:

- a) Verkossa toimivien markkinapaikkojen tarjoajat
- b) Verkossa toimivien hakukoneiden tarjoajat
- c) Verkkoyhteisöalustojen tarjoajat

3. NACE Rev. 2 -luokituksen C jakson kaksinumerotasossa 29 tarkoitettua moottoriajoneuvojen, perävaunujen ja puoliperävaunujen valmistusta harjoittavat toimijat

4. NACE Rev. 2 -luokituksen C jakson kaksinumerotasossa 30 tarkoitettua muiden kulkuneuvojen valmistusta harjoittavat toimijat

5. Tutkimusorganisaatiot, joiden ensisijaisena tavoitteena on harjoittaa soveltavaa tutkimusta tai kokeellista kehitystyötä kyseisen tutkimuksen tulosten hyödyntämiseksi kaupallisiin tarkoituksiin mutta jotka eivät ole korkeakouluja tai muita opetus- ja koulutusalan laitoksia

6. Kemikaalien rekisteröinnistä, arvioinnista, lupamenettelyistä ja rajoituksista (REACH), Euroopan kemikaaliviraston perustamisesta, direktiivin 1999/45/EY muuttamisesta sekä neuvoston asetuksen (ETY) N:o 793/93, komission asetuksen (EY) N:o 1488/94, neuvoston direktiivin 76/769/ETY ja komission direktiivien 91/155/ETY, 93/67/ETY, 93/105/EY ja 2000/21/EY kumoamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 1907/2006 3 artiklan 9 alakohdassa tarkoitettua aineiden valmistusta ja 14 alakohdassa tarkoitettua aineiden tai seosten jakelua harjoittavat yritykset sekä yritykset, jotka tuottavat mainitun asetuksen 3 artiklan 3 alakohdassa määritellyjä esineitä aineista tai seoksista silloin, kun aine on rekisteröitävä ja toiminta edellyttää vaarallisten kemikaalien ja räjähteiden käsittelyn turvallisuudesta annetun lain (390/2005) 23 §:ssä tarkoitettua lupaa tai 24 §:ssä tarkoitettua ilmoitusta

7. Elintarvikelainsäädäntöä koskevista yleisistä periaatteista ja vaatimuksista, Euroopan elintarviketurvallisuusviranomaisen perustamisesta sekä elintarvikkeiden turvallisuuteen liittyvistä menettelyistä annetun Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 178/2002 3 artiklan 2 alakohdassa määritellyt elintarvikeyritykset, jotka harjoittavat tukkukauppaa, teollista tuotantoa tai jalostusta

8. Jätteistä ja tiettyjen direktiivien kumoamisesta annetun Euroopan parlamentin ja neuvoston direktiivin 2008/98/EY 3 artiklan 9 alakohdassa määritellyä jätehuoltoa harjoittavat yritykset, lukuun ottamatta yrityksiä, joille jätehuolto ei ole niiden pääasiallista taloudellista toimintaa

Eduskunnan vastaus EV 15/2025 vp

9. Lääkinnällisistä laitteista, direktiivin 2001/83/EY, asetuksen (EY) N:o 178/2002 ja asetuksen (EY) N:o 1223/2009 muuttamisesta sekä neuvoston direktiivien 90/385/ETY ja 93/42/ETY kumoamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2017/745 2 artiklan 1 alakohdassa määriteltäviä lääkitä laitteita valmistavat toimijat

10. In vitro -diagnostiikkaan tarkoitettuja lääkitä laitteista sekä direktiivin 98/79/EY ja komission päätöksen 2010/227/EU kumoamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2017/746 2 artiklan 2 alakohdassa määriteltäviä in vitro -diagnostiikkaan tarkoitettuja lääkitä laitteita valmistavat toimijat, lukuun ottamatta tämän lain liitteessä I olevan 13 kohdan e-alakohdassa tarkoitettuja toimijoita

11. NACE Rev. 2 -luokituksen C jakson kaksinumeroitasossa 26 tarkoitettua tietokoneiden sekä elektronisten ja optisten tuotteiden valmistusta harjoittavat yritykset

12. NACE Rev. 2 -luokituksen C jakson kaksinumeroitasossa 27 tarkoitettua sähkölaitteiden valmistusta harjoittavat yritykset

13. NACE Rev. 2 -luokituksen C jakson kaksinumeroitasossa 28 tarkoitettua muiden koneiden ja laitteiden valmistusta harjoittavat yritykset

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 koh-

Eduskunnan vastaus EV 15/2025 vp

dassa 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*

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;

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;

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) *merkittäväällä 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) *merkittäväällä 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 tietoaaineistoja, 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) tarkoitettut 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 tarkoitettut yliopistot, ammattikorkeakoululaissa tarkoitettut ammattikorkeakoulut, Pelastusopisto sekä muut valtion opetus- ja koulutusalan laitokset;

7) julkisen hallinnon turvallisuusverkko-toiminnasta 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 tuomioistuinten eikä valitusasioita käsittelemään perustettujen lautakuntien lainkäyttöön. Tämän lain 3 lukua ei sovelleta eduskunnan oikeusasiamiehen eikä valtioneuvoston oikeuskanslerin toimintaan, tuomioistuinten 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, hyvinvointiyhtiöihin, kuntiin ja kuntayhtiöihin 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

Eduskunnan vastaus EV 15/2025 vp

tarkoitettulla 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 tarkoitettulla 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, puhelinnumeron 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;

Eduskunnan vastaus EV 15/2025 vp

8) salausten menetelmien 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 oikeasuhteiset suhteessa tiedonhallintayksikön käyttämien viestintäverkkojen ja tietojärjestelmien riskialttiuteen, viestintäverkon tai tietojärjestelmän merkitykseen tiedonhallintayksikön toiminnalle sekä niissä ilmenevän poikkeaman kohtuudella ennakoitavissa oleviin välittömiin vaikutuksiin. Lisäksi toimenpiteiden mitoitamisessa 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 juurisyn 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 viranomaisen on käsitelty poikkeaman.

Eduskunnan vastaus EV 15/2025 vp

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.

Eduskunnan vastaus EV 15/2025 vp

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

Edellä 1 ja 2 momentissa tarkoitettussa 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 säädetty 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 tarkoitettut 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 sääöksissä 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 yhteyspisteinä 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 liit-

Eduskunnan vastaus EV 15/2025 vp

tyvät 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 turvallisuusverkko toiminnasta annetussa laissa tarkoitettua turvallisuusverkon palvelutuotannosta tai palvelujen käytöstä eikä tietoja, joiden luovuttaminen vaarantaisi maanpuolustusta tai kansallista turvallisuutta taikka olisi vastoin niihin liittyvää tärkeää etua.

Eryityssuojattavan tietoa-aineiston 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) tarkoitettulle hyväksytylle tietoturvallisuuden arviointilaitokselle.

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

Eduskunnan vastaus EV 15/2025 vp

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 määräjassa 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 päivänä kuuta 20 .

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

Laki

sähköisen viestinnän palveluista annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti

kumotaan sähköisen viestinnän palveluista annetun lain (917/2014) 2 §:n 2 momentti ja 247 a §, sellaisina kuin ne ovat, 2 §:n 2 momentti laissa 1207/2020 ja 247 a § laissa 281/2018, *muutetaan* 165 §:n 1 momentti, 167, 170 ja 275 §, 308 §:n 3 momentti, 313 §:n 2 momentin 2 kohta, 318 §:n 4 momentti ja 342 §:n 2 momentti,

sellaisina kuin ne ovat, 165 §:n 1 momentti, 170 §, 308 §:n 3 momentti sekä 313 §:n 2 momentin 2 kohta laissa 1003/2018, 167 § laeissa 1003/2018 ja 1207/2020 sekä 275 § ja 318 §:n 4 momentti laissa 1207/2020 sekä 342 §:n 2 momentti laissa 1182/2023, ja

lisätään 165 §:ään, sellaisena kuin se on laissa 1003/2018, uusi 4 momentti ja 247 §:ään, sellaisena kuin se on laissa 1003/2018, uusi 5 momentti seuraavasti:

165 §

Verkkotunnusvälittäjän ilmoitusvelvollisuudet

Verkkotunnusvälittäjän on ennen toimintansa aloittamista tehtävä ilmoitus verkkotunnusrekisteriä hallinnoivalle viranomaiselle. Ilmoituksessa on oltava seuraavat tiedot:

1) verkkotunnusvälittäjän nimi, y-tunnus tai sellaisen puuttuessa muu yksilöivä tieto sekä kuulemiseen ja tiedoksiantoihin käytettävä sähköpostiosoite;

2) verkkotunnusvälittäjän päätoimipaikan ja muiden Euroopan unionissa sijaitsevien laillisten toimipaikkojen osoite ja ajantasaiset yhteystiedot tai, jos verkkotunnusvälittäjä ei ole sijoittautunut Euroopan unioniin, sen Euroopan unioniin nimetyn edustajan osoite, sähköpostiosoitteet, puhelinnumerot ja muut ajantasaiset yhteystiedot;

3) verkkotunnusvälittäjän IP-osoitealueet;

4) luettelo niistä Euroopan unionin jäsenvaltioista, joissa verkkotunnusvälittäjä tarjoaa palveluja; ja

5) muut kuin 1—4 kohdassa tarkoitetut valvonnan kannalta tarpeelliset tiedot.

Liikenne- ja viestintäviraston on toimitettava 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*) 27 artiklan 4 kohdassa tarkoitetun ilmoituksen tekemiseksi tarpeelliset tiedot verkkotunnusvälittäjien ilmoituksista kyberturvallisuuslain (/) 18 §:ssä tarkoitetulle keskitetylle yhteyspisteelle.

167 §

Tietojen merkitseminen verkkotunnusrekisteriin ja tietojen julkaiseminen

Verkkotunnus on merkittävä verkkotunnuksen käyttäjän nimiin. Verkkotunnuksen käyttäjän on ilmoitettava verkkotunnusvälittäjälle oikeat, ajantasaiset ja yksilöivät käyttäjä- ja yhteystiedot sekä niissä tapahtuvat muutokset. Verkkotunnusvälittäjän tai sen puolesta toimivan on merkittä-

Eduskunnan vastaus EV 15/2025 vp

vä verkkotunnusrekisteriin verkkotunnuksen käyttäjää ja rekisteröityä verkkotunnusta koskevat oikeat, ajantasaiset ja yksilöivät tiedot sekä kuulemisiin ja tiedoksiantoihin käytettävä sähköpostiosoite.

Liikenne- ja viestintävirasto voi estää verkkotunnuksen rekisteröinnin verkkotunnusrekisteriin, jos se epäilee 1 momentissa tarkoitettujen tietojen olevan puutteellisia tai virheellisiä eikä verkkotunnusvälittäjä kehotuksesta huolimatta todenna tietoja oikeiksi määräajassa. Liikenne- ja viestintävirasto asettaa julkisesti saataville käytössään olevat käyttäjätietojen oikeellisuuden varmistamista koskevat toimintaperiaatteet ja menettelyt.

Liikenne- ja viestintävirasto julkaisee ilman aiheutonta viivytystä internet-sivuillaan tai muussa sähköisessä palvelussa verkkotunnusrekisterin tiedot. Henkilötietojen suojasta säädetään luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta annetussa Euroopan parlamentin ja neuvoston asetuksessa (EU) 2016/679 (yleinen tietosuoja-asetus) ja sitä täydentävässä tietosuojalaissa. Liikenne- ja viestintäviraston on vastattava verkkotunnusten rekisteritietoihin pääsyä koskevaan pyyntöön ilman aiheutonta viivytystä ja viimeistään 72 tunnin kuluessa pyynnön vastaanottamisesta. Rekisterin tietojen luovuttamiseen sovelletaan muutoin viranomaisten toiminnan julkisuudesta annetun lain 16 §:ää. Liikenne- ja viestintävirasto asettaa julkisesti saataville käytössään olevat toimintaperiaatteet ja menettelyt verkkotunnusten rekisteröintitietojen luovuttamisesta.

Verkkotunnusrekisteriin merkitty verkkotunnus on voimassa enintään viisi vuotta. Verkkotunnusvälittäjä voi uudistaa verkkotunnusta koskevan merkinnän enintään viideksi vuodeksi kerrallaan.

Liikenne- ja viestintävirasto voi antaa tarkempia määräyksiä merkitsemisen teknisestä toteutustavasta ja merkitsemisen yhteydessä ilmoitettavista tiedoista sekä verkkotunnuksen käyttäjän teknisestä tunnistamisesta ja verkkotunnuksen käyttäjän tietojen varmistamisesta.

170 §

Verkkotunnusvälittäjän muut velvollisuudet

Verkkotunnusvälittäjän on:

- 1) tarjottava ennen verkkotunnuksen merkitsemistä tämän lain mukaiset tarvittavat tiedot verkkotunnuksen sisältöön ja muotoon liittyvistä edellytyksistä;
- 2) pidettävä verkkotunnusrekisteriin merkityt tiedot ajantasaisina;
- 3) kyettävä merkitsemään tietoja verkkotunnusrekisteriin Liikenne- ja viestintäviraston määrittelemällä teknisellä järjestelyllä;
- 4) tiedotettava verkkotunnuksen käyttäjää riittävästi ja tehokkaasti verkkotunnuksen voimassaoloajan päättymisestä;
- 5) poistettava verkkotunnus verkkotunnusrekisteristä verkkotunnuksen käyttäjän pyynnöstä ennen voimassaoloajan päättymistä;
- 6) huolehdittava toimintansa tietoturvasta;
- 7) ilmoitettava viipymättä Liikenne- ja viestintävirastolle, jos sen verkkotunnusten välitystoimintaan kohdistuu tai sitä uhkaa merkittävä tietoturvaloukkaus taikka muu tapahtuma, joka estää tai häiritsee sitä olennaisesti; samalla on myös ilmoitettava häiriön tai sen uhan arvioitu kesto ja vaikutukset, korjaustoimenpiteet sekä ne toimenpiteet, joilla häiriön toistuminen pyritään estämään;

Eduskunnan vastaus EV 15/2025 vp

8) asetettava julkisesti saataville toimintaperiaatteet ja menettelyt, joilla varmistetaan verkkotunnusrekisterin tietojen olevan 167 §:n 1 momentissa säädetyn mukaiset;

9) asetettava muut verkkotunnuksen rekisteröintitiedot kuin henkilötiedot julkisesti saataville ilman aiheutonta viivytystä;

10) annettava pääsy verkkotunnusten rekisteröintitietoihin tietosuojalainsäädännön mukaisesti ja maksuttomasti sekä vastattava rekisteritietoihin pääsyä oikeutetusti pyytävälle ilman aiheutonta viivytystä ja viimeistään 72 tunnin kuluessa lainmukaisen ja asianmukaisesti perustellun pyynnön vastaanottamisesta;

11) asetettava julkisesti saataville toimintaperiaatteet ja menettelyt verkkotunnusten rekisteröintitietojen luovuttamisesta.

Liikenne- ja viestintävirasto voi antaa tarkempia määräyksiä verkkotunnuksen käyttäjälle annettavista tiedoista, julkisesti saataville asetettavista tiedoista, pääsyn antamisesta tietoihin sekä 1 momentin 8 ja 11 kohdassa tarkoitetuista toimintaperiaatteista ja menettelyistä, toiminnan tietoturvallisuudesta sekä siitä, milloin 1 momentin 7 kohdassa tarkoitettu häiriö on merkittävä sekä ilmoituksen sisällöstä, muodosta ja toimittamisesta.

Kyberturvallisuuslain 2 §:n 3 kohdassa tarkoitetun DNS-palveluntarjoajan velvollisuudesta huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta ja poikkeamien ilmoittamisesta säädetään kyberturvallisuuslaissa.

247 §

Viestinnän välittäjän ja lisäarvopalvelun tarjoajan velvollisuus huolehtia tietoturvasta

Tietoturvasta huolehtimiseen sovelletaan lisäksi, mitä kyberturvallisuuslaissa säädetään sellaisen viestinnän välittäjän ja lisäarvopalvelun tarjoajan osalta, joka kuuluu NIS 2 -direktiivin soveltamisalaan.

275 §

Häiriöilmoitukset Liikenne- ja viestintävirastolle

Teleyrityksen on ilmoitettava viipymättä Liikenne- ja viestintävirastolle, jos sen palveluun kohdistuu tai sitä uhkaa merkittävä tietoturvaloukkaus taikka muu tapahtuma, joka estää viestintäpalvelun toimivuuden tai häiritsee sitä olennaisesti. Teleyrityksen on ilmoitettava myös ilman aiheutonta viivästystä häiriön tai sen uhan arvioitu kesto ja vaikutukset, korjaustoimenpiteet sekä ne toimenpiteet, joilla häiriön toistuminen pyritään estämään.

Jos häiriöistä ilmoittaminen on yleisen edun mukaista, Liikenne- ja viestintävirasto voi velvoittaa teleyrityksen tiedottamaan asiasta tai kuultuaan ilmoitusvelvollista tiedottaa asiasta itse.

Liikenne- ja viestintävirasto voi antaa tarkempia määräyksiä siitä, milloin 1 momentissa tarkoitettu häiriö on merkittävä, sekä 1 momentissa tarkoitettujen ilmoitusten sisällöstä, muodosta ja toimittamisesta.

Liikenne- ja viestintäviraston on arvioitava, koskeeko 1 momentissa tarkoitettu häiriö muita Euroopan unionin jäsenvaltioita ja ilmoitettava tarvittaessa muille asiaan liittyville jäsenvaltioille. Edellä 1 momentissa tarkoitettusta häiriöstä on lisäksi tarvittaessa ilmoitettava Euroopan unio-

Eduskunnan vastaus EV 15/2025 vp

nin kyberturvallisuusvirastolle. Häiriöilmoituksiin sovelletaan lisäksi, mitä kyberturvallisuuslaissa säädetään poikkeamailmoituksista.

308 §

Yhteistyö eri viranomaisten kanssa

Liikenne- ja viestintäviraston on toimittava yhteistyössä muiden Euroopan unionin jäsenvaltioiden verkko- ja tietoturvallisuutta valvovien viranomaisten, tietoturvaloukkauksiin reagoivien yksiköiden sekä NIS 2 -direktiivin 14—16 artiklassa tarkoitetun yhteistyöryhmän, CSIRT-verkoston ja Euroopan kyberkriisien yhteysorganisaatioiden verkoston kanssa.

313 §

Valvonta-asioiden käsittely Liikenne- ja viestintävirastossa

Liikenne- ja viestintävirasto voi asettaa tässä laissa säädetty valvontatehtävänsä tärkeysjärjestykseen. Liikenne- ja viestintävirasto voi jättää asian tutkimatta, jos:

2) asialla on epäilystä virheestä tai laiminlyönnistä huolimatta viestintämarkkinoiden toimivuuden, viestintäpalvelujen luotettavuuden tai sähköisen viestinnän häiriöttömyyden turvaamisen ja palveluja käyttävien edun kannalta vain vähäinen merkitys; tai

318 §

Tietojen luovuttaminen viranomaisesta

Liikenne- ja viestintäministeriöllä ja Liikenne- ja viestintävirastolla on oikeus luovuttaa salassa pidettävä asiakirja sekä ilmaista salassa pidettävä tieto komissiolle, Euroopan sähköisen viestinnän sääntelyviranomaisten yhteistyöelimelle ja toisen ETA-valtion valvontaviranomaiselle, jos se on viestintämarkkinoiden valvonnan kannalta välttämätöntä. Liikenne- ja viestintävirastolla on oikeus luovuttaa 170 §:n 1 momentin 7 kohdan, 171 §:n ja 275 §:n 1 momentin nojalla saamansa salassa pidettävä asiakirja sekä ilmaista salassa pidettävä tieto toisen ETA-valtion valvontaviranomaiselle, NIS 2 -direktiivin 14 artiklassa tarkoitetulle yhteistyöryhmälle ja mainitun direktiivin 15 artiklassa tarkoitetulle CSIRT-verkostolle, jos se on verkko- ja tietoturvallisuuden valvonnan kannalta välttämätöntä eikä luovuttaminen vaaranna mainituissa pykälissä tarkoitettujen toimijoiden turvallisuuteen ja liikesalaisuuksiin liittyviä etuja tai annettujen tietojen luottamuksellisuutta.

Eduskunnan vastaus EV 15/2025 vp

342 §

Oikaisuvaatimus

Liikenne- ja viestintäviraston päätökseen, joka koskee 39 §:ssä tarkoitettua radiolupaa, 44 §:ssä tarkoitettua radiotaajuuksien varausta koskevaa päätöstä, 100 §:ssä tarkoitettua numeerointipäätöstä, 167 §:n 2 momentissa tarkoitettua verkkotunnuksen rekisteröinnin estämistä, 169 §:n 1 momentissa tarkoitettua verkkotunnuksen poistamista, 288 §:ssä tarkoitettua markkinaehtoista taajuusmaksua, 289 §:ssä tarkoitettua tietoyhteiskuntamaksua, 293 §:ssä tarkoitettua televisio- ja radiotoiminnan valvontamaksua tai datanhallinta-asetuksen 19 artiklan 5 kohdassa tarkoitettua rekisteröintiä, saa vaatia oikaisua.

Tämä laki tulee voimaan päivänä kuuta 20 .

Tämän lain voimaan tullessa voimassa olleen 275 §:n nojalla annetut määräykset jäävät voimaan.

Laki

ilmailulain 128 a ja 128 b §:n kumoamisesta

Eduskunnan päätöksen mukaisesti säädetään:

1 §

Tällä lailla kumotaan ilmailulain (864/2014) 128 a ja 128 b §, sellaisina kuin ne ovat laissa 965/2018.

2 §

Tämä laki tulee voimaan päivänä kuuta 20 .

Laki

raideliikennelain 169 §:n kumoamisesta

Eduskunnan päätöksen mukaisesti säädetään:

1 §

Tällä lailla kumotaan raideliikennelain (1302/2018) 169 §.

2 §

Tämä laki tulee voimaan päivänä kuuta 20 .

Laki

liikenteen palveluista annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti

kumotaan liikenteen palveluista annetun lain (320/2017) 161 §, sellaisena kuin se on laissa 1256/2020, sekä

muutetaan 140 §, sellaisena kuin se on laeissa 579/2018, 984/2018 ja 371/2019, seuraavasti:

140 §

Tietoturva tieliikenteen ohjaus- ja hallintapalvelussa

Tieliikenteen ohjaus- ja hallintapalvelun tarjoajan velvollisuudesta huolehtia käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta ja poikkeamien ilmoittamisesta säädetään kyberturvallisuuslaissa (/).

Tieliikenteen ohjaus- ja hallintapalvelun tarjoajan on tallennettava ja säilytettävä tieliikenteen tilannekuva tavalla, joka turvaa tallenteet oikeudettomalta puuttumiselta. Tallenteita on säilytettävä 14 vuorokautta.

Tämä laki tulee voimaan päivänä kuuta 20 .

Laki

alusliikennepalvelulain 18 a §:n kumoamisesta

Eduskunnan päätöksen mukaisesti säädetään:

1 §

Tällä lailla kumotaan alusliikennepalvelulain (623/2005) 18 a §, sellaisena kuin se on laissa 947/2018.

2 §

Tämä laki tulee voimaan päivänä kuuta 20 .

Laki

eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annetun lain 7 e ja 7 f §:n kumoamisesta.

Eduskunnan päätöksen mukaisesti säädetään:

1 §

Tällä lailla kumotaan eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annetun lain (485/2004) 7 e ja 7 f §, sellaisina kuin ne ovat laissa 955/2018.

2 §

Tämä laki tulee voimaan päivänä kuuta 20 .

Laki

sosiaali- ja terveydenhuollon asiakastietojen käsittelystä annetun lain 2 ja 90 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan sosiaali- ja terveydenhuollon asiakastietojen käsittelystä annetun lain (703/2023) 2 §:n 3 momentti ja 90 § seuraavasti:

2 §

Soveltamisala ja suhde muuhun lainsäädäntöön

Tällä lailla annetaan 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 annettua Euroopan parlamentin ja neuvoston direktiiviä (EU) 2022/2555 (*NIS 2 -direktiivi*) ja kyberturvallisuuslakia (/) täydentävät ja täsmentävät säännökset käsiteltäessä sosiaali- ja terveydenhuollon asiakastietoja ja asiakkaan itsensä tuottamia hyvinvointitietoja sosiaali- ja terveyspalveluita järjestettäessä ja toteutettaessa.

90 §

Ilmoittaminen tietojärjestelmän ja hyvinvointisovelluksen olennaisten vaatimusten poikkeamista sekä tietoverkkoihin kohdistuvista tietoturvallisuuden häiriöistä

Jos palvelunantaja tai apteekki havaitsee, että tietojärjestelmän olennaisten vaatimusten täytymisessä on merkittäviä poikkeamia, sen on ilmoitettava asiasta tietojärjestelmäpalvelun tuottajalle. Jos tietojärjestelmän tai hyvinvointisovelluksen poikkeama voi aiheuttaa merkittävän riskin asiakas- tai potilasturvallisuudelle tai tietoturvalle, on palvelunantajan, apteekin, tietojärjestelmäpalvelun tuottajan tai tietojärjestelmän valmistajan, hyvinvointisovelluksen valmistajan, Kansaneläkelaitoksen tai Terveysalan ja hyvinvoinnin laitoksen ilmoitettava siitä Sosiaali- ja terveysalan lupa- ja valvontavirastolle. Myös muu taho voi ilmoittaa Sosiaali- ja terveysalan lupa- ja valvontavirastolle havaitsemistaan riskeistä. Jos tietojärjestelmän poikkeama voi aiheuttaa merkittävän riskin apteekin toiminnalle, on apteekin ilmoitettava siitä lisäksi Lääkealan turvallisuus- ja kehittämiskeskuskeskukselle. Henkilötietojen tietoturvaloukkauksista ilmoittamisesta tietosuojavaltuutetulle säädetään tietosuoja-asetuksen 33 artiklassa.

Palvelunantajan, apteekin, Kansaneläkelaitoksen ja tietojärjestelmäpalvelun tuottajan tai tietojärjestelmän valmistajan tai välittäjän on ilmoitettava viipymättä Sosiaali- ja terveysalan lupa- ja valvontavirastolle sellaisesta sen käyttämiin käyttöympäristöihin ja tietoverkkoihin kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä, jonka seurauksena tietojärjestelmien käyttö ja sosiaali- ja terveyspalveluiden toteuttaminen voi merkittävästi vaarantua. Sosiaali- ja terveysalan lupa- ja valvontavirasto voi antaa tarkempia määräyksiä siitä, milloin häiriö on merkittävä, sekä ilmoituksen sisällöstä, muodosta ja toimittamisesta.

Apteekin on lisäksi ilmoitettava viipymättä Lääkealan turvallisuus- ja kehittämiskeskuskeskukselle sellaisesta sen käyttämiin käyttöympäristöihin ja tietoverkkoihin kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä, jonka seurauksena apteekin toiminta voi merkittävästi vaarantua. Lääkealan turvallisuus- ja kehittämiskeskus voi antaa tarkempia määräyksiä siitä, milloin häiriö on merkittävä, sekä ilmoituksen sisällöstä, muodosta ja toimittamisesta.

Jos 1 ja 2 momentissa tarkoitettu tietoturvallisuuteen liittyvästä poikkeamasta tai häiriöstä ilmoittaminen on yleisen edun mukaista, Sosiaali- ja terveysalan lupa- ja valvontavirasto voi velvoittaa palvelunantajan, apteekin, Kansaneläkelaitoksen, tietojärjestelmäpalvelun tuottajan tai tietojärjestelmän valmistajan taikka välittäjän tiedottamaan yleisölle asiasta taikka kuultuaan ilmoitusvelvollista tiedottaa asiasta itse. Lisäksi Lääkealan turvallisuus- ja kehittämiskeskus voi

Eduskunnan vastaus EV 15/2025 vp

velvoittaa apteekin tiedottamaan yleisölle 3 momentissa tarkoitettusta häiriöstä taikka kuultuaan ilmoitusvelvollista tiedottaa häiriöstä itse.

Tämä laki tulee voimaan _____
päivänä _____ kuuta 20 ____.

Laki

sähkömarkkinalain muuttamisesta

Eduskunnan päätöksen mukaisesti
kumotaan sähkömarkkinalain (588/2013) 29 a § sekä 49 a §:n 5 momentti, sellaisina kuin ne
ovat, 29 a § laissa 287/2018 ja 49 a §:n 5 momentti laissa 108/2019, sekä
muutetaan 62 §:n 1 momentti, sellaisena kuin se on laissa 497/2023 seuraavasti:

62 §

Suljettua jakeluverkkoa koskevat erityissäännökset

Suljettuun jakeluverkkoon ja suljetun jakeluverkonhaltijaan ei sovelleta 23, 23 a eikä 26 a §:ää,
27 §:n 3 momenttia, 28, 29, 29 b, 50—52, 52 a, 53, 53 a, 54—56, 56 a, 58 eikä 59 §:ää ja 61 a §:n
2 momenttia.

Tämä laki tulee voimaan _____
päivänä _____ kuuta 20 ____.

Laki

maakaasumarkkinalain 34 a §:n kumoamisesta

Eduskunnan päätöksen mukaisesti säädetään:

1 §

Tällä lailla kumotaan maakaasumarkkinalain (587/2017) 34 a §, sellaisena kuin se on laeissa
288/2018 ja 327/2020.

Eduskunnan vastaus EV 15/2025 vp

Tämä laki tulee voimaan 2 §
päivänä kuuta 20 .

Laki

Energiavirastosta annetun lain 1 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan Energiavirastosta annetun lain (870/2013) 1 §:n 2 momentin 20 kohta, sellaisena kuin se on laissa 939/2024, sekä
lisätään 1 §:n 2 momenttiin, sellaisena kuin se on laeissa 634/2020, 804/2020, 606/2021, 500/2023 ja 939/2024, uusi 21 kohta seuraavasti:

1 §

Tehtävät

Energiavirasto hoitaa tehtävät, jotka sille on annettu:

20) merituulivoimasta talousvyöhykkeellä annetussa laissa (937/2024);
21) kyberturvallisuuslaissa (/).

Tämä laki tulee voimaan päivänä kuuta 20 .

Laki

sähkö- ja maakaasumarkkinoiden valvonnasta annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan sähkö- ja maakaasumarkkinoiden valvonnasta annetun lain (590/2013) 9 §, 23 §:n 4 ja 5 kohta sekä 28 §:n 1 momentin 1 kohta, sellaisina kuin niistä ovat 23 §:n 4 ja 5 kohta laissa 589/2017 ja 28 §:n 1 momentin 1 kohta laissa 1002/2018, sekä
lisätään 2 §:ään, sellaisena kuin se on laeissa 633/2020 ja 499/2023, uusi 2 momentti ja 23 §:ään, sellaisena kuin se on laissa 589/2017, uusi 6 kohta seuraavasti:

Eduskunnan vastaus EV 15/2025 vp

2 §

Soveltamisala

Tämän lain 23 ja 24 §:ää sovelletaan lisäksi niiden tehtävien hoitamiseen, jotka säädetään Energiaviraston tehtäviksi kyberturvallisuuslaissa (/).

9 §

Energiaviraston toimivalta valvonta-asioissa

Jos joku rikkoo tai laiminlyö 2 §:n 1 momentissa tarkoitettussa kansallisessa tai Euroopan unionin lainsäädännössä säädettyjä velvoitteitaan, Energiaviraston on velvoitettava hänet korjaamaan rikkomuksensa tai laiminlyöntinsä. Päätöksessä voidaan määrätä, millä tavoin rikkomus tai laiminlyönti tulee korjata. Päätöksessä voidaan myös määrätä palauttamaan asiakkaalle virheellisesti peritty maksu, jos palautukseen ei sovelleta 14 §:ssä säädettyä palautusmenettelyä.

23 §

Sähkö- ja maakaasuverkkoluvan peruuttaminen

Energiavirasto voi peruuttaa sähköverkkoluvan, maakaasuverkkoluvan sekä sähkömarkkinalain 12 §:ssä ja maakaasumarkkinalain 11 §:ssä säädetyn vapautuksen tai poikkeusluvan:

4) jos luvanhaltija toistuvasti ja oleellisesti rikkoo maakaasuverkoasetusta tai sen nojalla annettujen, suuntaviivoja koskevien komission asetusten tai päätösten säännöksiä, siltä osin kuin niitä sovelletaan Suomessa, eikä luvanhaltijalle etukäteen annettu varoitus luvan peruuttamisesta ole johtanut toiminnassa esiintyneiden puutteiden korjaamiseen;

5) jos luvanhaltija toistuvasti ja oleellisesti rikkoo maakaasun siirtoverkonhaltijan eriyttämisestä annetun lain säännöksiä eikä luvanhaltijalle etukäteen annettu varoitus luvan peruuttamisesta ole johtanut toiminnassa esiintyneiden puutteiden korjaamiseen; tai

6) jos luvanhaltija toistuvasti ja oleellisesti rikkoo kyberturvallisuuslakia (/), eikä luvanhaltijalle etukäteen annettu varoitus luvan peruuttamisesta ole johtanut toiminnassa esiintyneiden puutteiden korjaamiseen.

28 §

Energiaviraston oikeus luovuttaa tietoja toiselle viranomaiselle

Sen lisäksi, mitä viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999) säädetään, Energiavirastolla on oikeus luovuttaa salassapitosäännösten estämättä tietoja:

1) Finanssivalvonnalle, Kilpailu- ja kuluttajavirastolle ja kuluttaja-asiamiehelle niiden tehtävien hoitamista varten;

Eduskunnan vastaus EV 15/2025 vp

Tämä laki tulee voimaan _____ päivänä _____ kuuta 20 ____.

Laki

vesihuoltolain 35 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan vesihuoltolain (119/2001) 35 §:n 2 momentti, sellaisena kuin se on laissa 1013/2018, seuraavasti:

35 §

Salassapitovelvollisuus

Viranomaisten toiminnan julkisuudesta annetussa laissa säädetyn salassapitovelvollisuuden estämättä saa tämän lain mukaisia tehtäviä suorittaessa saatuja tietoja yksityisen ja yhteisön taloudellisesta asemasta, liikesalaisuudesta sekä yksityisen henkilökohtaisista oloista luovuttaa:

- 1) valvontaviranomaiselle tämän lain mukaisten tehtävien suorittamista varten; sekä
- 2) rikoksen selvittämiseksi syyttäjä- tai poliisiviranomaiselle.

Tämä laki tulee voimaan _____ päivänä _____ kuuta 20 ____.

Laki

sakon täytäntöönpanosta annetun lain 1 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan sakon täytäntöönpanosta annetun lain (672/2002) 1 §:n 2 momentin 33 kohta, sellaisena kuin se on laissa 845/2024, sekä
lisätään sakon täytäntöönpanosta annetun lain 1 §:n 2 momenttiin, sellaisena kuin se on laeissa 1183/2023, 23/2024, 36/2024, 545/2024, 651/2024, 845/2024, 952/2024 ja 1122/2024, uusi 34 kohta seuraavasti:

Eduskunnan vastaus EV 15/2025 vp

1 §

Lain soveltamisala

Siten kuin tässä laissa säädetään, pannaan täytäntöön myös:

- 33) uusiutuvien polttoaineiden käytön edistämisestä liikenteessä annetun lain (446/2007) 11, 11 a ja 11 e §:ssä tarkoitetut seuraamusmaksut ja 12 §:ssä tarkoitettu virhemaksu;
34) kyberturvallisuuslain (/) 35 §:ssä tarkoitettu seuraamusmaksu.

Tämä laki tulee voimaan _____ päivänä _____ kuuta 20 ____ .

Laki

maa-aseamista ja eräistä tutkista annetun lain 8 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan maa-aseamista ja eräistä tutkista annetun lain (96/2023) 8 §:n 1 momentin 3 kohta seuraavasti:

8 §

Luvan muuttaminen ja peruuttaminen

Luvan myöntänyt viranomainen voi muuttaa maa-asema- tai tutkatoiminnan harjoittamiseen myönnettyä lupaa tai peruuttaa luvan, jos:

- 3) toiminnanharjoittaja on olennaisella tavalla laiminlyönyt tai rikkonut tässä laissa tai kyberturvallisuuslaissa (/) säädettyä velvollisuutta tai rajoitusta taikka luvan ehtoja;

Tämä laki tulee voimaan _____ päivänä _____ kuuta 20 ____ .

Laki

vaarallisten kemikaalien ja räjähteiden käsittelyn turvallisuudesta annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti
lisätään vaarallisten kemikaalien ja räjähteiden käsittelyn turvallisuudesta annetun lain (390/2005) 5 §:ään, sellaisena kuin se on laeissa 358/2015, 795/2020 ja 798/2023, uusi 10 momentti sekä lakiin uusi 109 a § seuraavasti:

5 §

Suhde muuhun lainsäädäntöön

Kyberturvallisuuden riskienhallinta- ja raportointivelvoitteista sekä viranomaisten yhteistyöstä kyberturvallisuuspoikkeamien ja -riskien hallitsemiseksi säädetään kyberturvallisuuslaissa (/).

109 a §

Kyberturvallisuutta koskevien velvoitteiden laiminlyömisestä johtuva luvan peruuttaminen

Jos toiminnanharjoittaja olennaisesti ja vakavasti laiminlyö kyberturvallisuuslaissa säädettyjä velvollisuuksia, on valvontaviranomaisen asetettava toiminnanharjoittajalle riittävä määräaika asian korjaamiseksi. Jos toiminnanharjoittaja ei ole korjannut puutteita määräajan kuluessa, valvontaviranomainen voi peruuttaa myöntämänsä toiminnanharjoittamista koskevan luvan osittain tai kokonaan.

Tämä pykälä koskee toimintaa, jossa Turvallisuus- ja kemikaalivirasto on valvova viranomainen 115 §:n mukaisesti.

Tämä laki tulee voimaan päivänä kuuta 20 .

Eduskunnan vastaus EV 15/2025 vp

Helsingissä 11.3.2025

Eduskunnan puolesta

puhemies

pääsihteeri