



VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Kyberturvallisuutta koskevat velvollisuudet - tiedonhallintalain uusi 4 a luku

EEVA LANTTO, LAINSÄÄDÄNTÖNEUVOS

WEBINAARI: KYBERTURVALLISUUSVELVOLLISUUKSIEN TOIMEENPANO JULKISESSA
HALLINNOSSA 1.4.2025

NIS 2 –direktiivin täytäntöönpano

- hallituksen esitys 57/2024 eduskunnalle kyberturvallisuusedirektiivin (NIS 2 -direktiivi) täytäntöönpanoa koskevaksi lainsäädännöksi
 - annettu eduskunnalle 23.5.2024
 - käsittelysivut:
https://www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/HE_57+2024.aspx
- pääasiallisesti direktiivi pannaan täytäntöön kyberturvallisuuslailla ja tiedonhallintalain muutoksilla (4 a luku)
- lait hyväksyttäneen Tasavallan presidentin esittelyssä 4.4. ja ne tulevat voimaan 8.4.2025

Tiedonhallintalain NIS 2-sääntelyn soveltaminen julkishallinnon toimijoihin (vähimmäissoveltamisala)

Sovelletaan (lähtökohtaisesti)

- Valtion hallintoviranomaisiin, valtion virastoihin ja laitoksiin, valtion liikelaitoksiin, itsenäisiin julkisoikeudellisiin laitoksiin sekä hyvinvointialueisiin, hyvinvointiyhtymiin ja Helsingin kaupunkiin niiden hoitaessa hyvinvointialueiden järjestämisvastuulle säädettyjä tehtäviä.
- [CER-lain] nojalla julkishallinnon toimialan kriittisiksi toimijoiksi määriteltyihin toimijoihin (uusi HE annetaan eduskunnalle NIS 2 ja CER täytäntöönpanon yhteensovittamisesta)

Ei sovelleta

- tuomioistuimiin tai valitusasioita käsittelemään perustettuihin lautakuntiin
- yliopistoihin, ammattikorkeakouluihin taikka Pelastusopistoon tai muihin valtion opetus- ja koulutusalan laitoksiin
- Muihin kuntiin tai kuntayhtymiin
- tasavallan presidentin kansliaan, eduskunnan virastoihin, Puolustusvoimiin, Puolustuskiinteistöihin, poliisin hallinnosta annetussa laissa (110/1992) tarkoitettuihin poliisiyksikköihin, Rajavartiolaitokseen, Tullin rikostorjuntaan, Syyttäjälaitokseen, Suomen Pankkiin
- turvallisuusverkkolaissa (10/2015) tarkoitettuun turvallisuusverkon palvelutuotantoon ja palvelujen käyttöön.
- muihin kuin viranomaisena toimiviin julkista hallintotehtävää hoitaviin
- viranomaisiin, jotka on perustettu yhdessä Euroopan talousalueen ulkopuolisen maan (kolmas maa) kanssa kansainvälisen sopimuksen mukaisesti eikä kolmansissa maissa sijaitseviin diplomaattisiin edustustoihin tai konsuliedustustoihin taikka näiden verkko- ja tietojärjestelmiin, siltä osin kuin tällaiset järjestelmät sijaitsevat edustuston tiloissa tai niitä ylläpidetään kolmannessa maassa olevia käyttäjiä varten.
- valvontaa ei sovellettaisi valtioneuvoston oikeuskanslerin tai eduskunnan oikeusasiamiehen toimintaan

Erityisesti kunnista ja hyvinvointialueista

- julkishallinnon toimialan (tiedonhallintalain) NIS2-sääntelyä ei sovelleta kuntiin (paitsi Helsinkiin), mutta kyberturvallisuuslakia sovelletaan, jos kunta harjoittaa toimintaa lain liitteen toimialalla
- julkishallinnon toimialan NIS2-sääntelyä sovelletaan hyvinvointialueisiin ja –yhtymiin, joihin sovelletaan myös kyberturvallisuuslakia Terveys-toimialalla

Toimijoiden velvoitteet tiedonhallintalain 4 a luvussa

1. Toimintaa koskeva ilmoitus valvovalle viranomaiselle (18 a §)
2. Kyberturvallisuuden riskienhallintavelvoite (18 b ja c §)
 - Velvollisuus hallita riskejä, riskienhallinnan toimintamalli, riskienhallintatoimenpiteiden toteuttaminen ja dokumentointi riskienhallinnan toimintamalliin, johdon vastuu riskienhallinnasta ja sen toteuttamisen valvonnasta
3. Ilmoitusvelvollisuudet poikkeamista ja kyberuhkista (18 d ja g §)
 - Velvollisuus ilmoittaa merkittävistä poikkeamista valvovalle viranomaiselle
 - Velvollisuus ilmoittaa merkittävästä poikkeamasta palvelujen vastaanottajille ja yleisölle sekä ilmoittaa merkittävästä kyberuhkasta sekä kyberuhkan hallitsemiseksi käytettävissä olevista toimenpiteistä niille palvelujen vastaanottajille, joihin merkittävä kyberuhka saattaa vaikuttaa

Valvonta julkishallinnon toimialalla

- Julkishallinnon toimialan valvova viranomainen olisi Liikenne- ja viestintävirasto
 - Antaa ohjausta ja neuvontaa
 - Neuvoa tarvittaessa poikkeamien käsittelyssä (yhteistyö CSIRT:n kanssa)
 - Voi velvoittaa toimijan korjaamaan puutteet sääntelyn noudattamisessa.
 - Tiedonsaanti- ja tarkastusoikeus sekä arvioinnin teettämisoikeus tietyin edellytyksin
- Julkishallintoon ei sovellettaisi seuraamusmaksua koskevaa sääntelyä eikä johdon toiminnan rajoittamiseen liittyvää sääntelyä

Tiedonhallintalain suhde ns. NIS 2 -yleislakiin

- Tiedonhallintalain muutoksilla saatetaan NIS 2 –direktiivi voimaan (direktiivin liitteen I kohta 10) julkishallinnon toimialalla. Muilta osin direktiivi saatetaan voimaan LVM:n valmistelemalla kyberturvallisuuslailla
- Vain yleislaissa direktiivin edellyttämät säännökset:
 - Velvoitteet ja valvonta muilla direktiivin liitteiden toimialoilla
 - kansallisesta kyberturvallisuusstrategiasta sekä laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien hallintasuunnitelmasta
 - CSIRT-yksiköstä (Liikenne- ja viestintävirastossa)
 - Keskitetystä yhteyspisteestä (Liikenne- ja viestintävirastossa)
 - Liikenne- ja viestintäviraston tietojen (toimintaa koskevat ilmoitukset, poikkeamailmoitukset sekä muut valvontatehtävässä saadut tiedot) käsittelystä sekä yhteistyöstä muiden viranomaisten ja Euroopan unionin elinten kanssa sekä tietojen luovuttamisesta niille



VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Kiitos

EEVA LANTTO, LAINSÄÄDÄNTÖNEUVOS
ETUNIMI.SUKUNIMI@GOV.FI
VM.FI | @VMUUTISET