



RUOKAVIRASTO

Livsmedelsverket • Finnish Food Authority



RUOKAVIRASTO
Livsmedelsverket • Finnish Food Authority

Kyberturvallisuuslaki elintarvikealalla

Keskustelutilaisuus toimijoille

8.5.2025



Keskustelutilaisuuden aiheita

1. Lain soveltamisala
 2. Millaisia yrityksiä koskee (toimiala ja kokokriteerit)
 3. Lain velvoitteet
 - a) Ilmoittautuminen toimijaluetteloon
 - b) Riskienhallintatoimenpiteet
 - c) Poikkeamailmoitus
 4. Valvonta
-



1. Lain soveltamisala

- Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555 (NIS2 - direktiivi), kyberturvallisuuslaki 124/2025
- Pyritään saavuttamaan kyberturvallisuuden (viestintäverkot ja tietojärjestelmät) yhteinen korkea taso kaikkialla unionissa sisämarkkinoiden toiminnan parantamiseksi.
- Sovelletaan direktiivin liitteissä I ja II tarkoitettua toimijatyyppiä oleviin julkisiin ja yksityisiin toimijoihin, jotka täyttävät suosituksen 2003/361/EY liitteessä olevan 2 artiklan mukaiset keskisuuria yrityksiä koskevat edellytykset tai ylittävät kyseisen artiklan 1 kohdassa säädettyt keskisuurten yritysten määrittelyssä käytettävät kynnysarvot ja jotka tarjoavat palvelujaan tai harjoittavat toimintaansa unionissa.



2. Millaisia yrityksiä koskee (toimiala ja kokokriteerit)?

- Kun elintarvikeyritys harjoittaa tukkukauppaa, teollista tuotantoa tai jalostusta ja täyttää tai ylittää keskisuuren yrityksen kokokriteerit tai täyttää koosta riippumattomien toimijoiden kriteerit.
- Keskisuuria yrityksiä ovat yritykset, joiden palveluksessa on vähintään 50 työntekijää tai jonka vuosiliikevaihto ja taseen loppusumma ylittää 10 miljoonaa euroa eli yritys on keskisuuri toimija.
- Keskisuuren yrityksen kriteerit ylittyvät, kun yrityksellä on palveluksessaan vähintään 250 työntekijää tai sen vuosiliikevaihto on yli 50 miljoonaa euroa ja tase yli 43 miljoonaa euroa eli yritys on suuri toimija.



3. Lain velvoitteet:

a) Ilmoittautuminen Ruokaviraston toimijaluetteloon

- Tarkista täyttyvätkö yrityskohtaiset (y-tunnus) toimijan kriteerit (yrityksen toimiala ja koko). Yrityksen kokomääritelmä koskee koko yritystä, ei pelkästään elintarvikealan osuutta.
- Soveltamisalaan eivät kuulu esim. alkutuotanto, rehutuotanto, vähittäiskauppa, varastointi, kuljetus, elintarvikekontaktimateriaalitoiminta ja ruokapalvelutoiminta. Kuitenkin, jos toimija myöhemmin määritetään kriittiseksi toimijaksi CER-direktiivin nojalla, koskevat kyberturvallisuuslain velvoitteet myös näitä toimijoita.
- Ilmoittaudu Ruokaviraston toimijaluetteloon Ruokaviraston sähköisen asiointipalvelu ilppan kautta **[Ilppa: Toiminnanharjoittajan ilmoitukset](#)**.
- Ilmoituksessa kerätään kyberturvallisuuslain 41§:n mukaiset tiedot toimijasta ja toiminnasta mm. yhteystiedot sekä IP-osoitealuetiedot.
- Toimijoiden on ilmoitettava muutoksista tietoihin valvovalle viranomaiselle kahden viikon kuluessa muutoshetkestä.



b) Riskienhallintatoimenpiteet, kyberturvallisuuslaki 9 §

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 sisällytetyt hallintatoimenpiteet sekä välittömien toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt;
- 5) **omaisuudenhallinta** ja sen turvallisuuden kannalta **tärkeiden toimintojen tunnistaminen**;
- 6) **henkilöstöturvallisuus ja kyberturvallisuuskoulutus**;



b) Riskienhallintatoimenpiteet, kyberturvallisuuslaki 9 §

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

- 7) **pääsynhallinnan ja todentamisen** menettelyt;
- 8) **salausmenetelmien käyttämistä koskevat toimintaperiaatteet ja menettelyt** sekä tarvittaessa toimenpiteet suojatun sähköisen viestinnän käyttämiseksi;
- 9) **poikkeamien havainnointi ja käsittely** turvallisuuden ja toimintavarmuuden palauttamiseksi ja ylläpitämiseksi;
- 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.



b) Riskienhallintatoimenpiteet, jatkuu...

Traficomin suositus

- Traficomin suositus on kohdistettu kansallista sääntelyä valvoville viranomaisille, mutta se tukee myös lainsäädännön soveltamisalaan kuuluvien toimijoiden omaa kyberturvallisuuden riskienhallinnan suunnittelua.
- Suositusluonnoksessa esitetään myös perustason tietoturvakäytännöt.

Perustason tietoturvakäytännöt

- Kyberhygieniakäytännöt eli perustason tietoturvakäytännöt luovat perustan organisaation kyberturvallisuudelle.
- Jos kyberturvallisuus ei ole organisaatiolle vielä kovin tuttua, kyberhygieniakäytännöillä organisaatio pääsee alkuun kyberturvallisuudesta huolehtimisessa.



c) Poikkeamailmoitus

- Kyberturvallisuuslain 11§:n mukaan toimijan on viipymättä ilmoitettava valvovalle viranomaiselle merkittävästä poikkeamasta.
- Tee ilmoitus merkittävästä poikkeamasta **Traficomin poikkeamailmoitussovellukseen** → Ruokavirasto saa tiedon poikkeamasta
- Merkittävällä poikkeamalla tarkoitetaan poikkeamaa, joka
 - on aiheuttanut tai voi aiheuttaa vakavan palvelujen toimintahäiriön tai huomattavia taloudellisia tappioita asianomaiselle toimijalle, sekä
 - 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.



4. Valvonta

- Ruokavirasto toimii NIS2-direktiivin ja sen täytäntöönpanoa koskevan kansallisen lainsäädännön valvovana viranomaisena elintarviketoimialalla.
 - Elintarvikealan yritykset → tärkeät toimijat → jälkikäteisvalvonta
 - Valvova viranomainen voi kohdistaa valvontaa myös tärkeään toimijaan, jos on perusteltu syy epäillä, että tämä ei ole noudattanut kyberturvallisuuslakia, sen nojalla annettuja määräyksiä tai NIS2-direktiivin nojalla annettuja säännöksiä.
- Varmistetaan tärkeiden toimijoiden ilmoittautuminen toimijaluetteloon
- Mahdollinen tarkastus
 - Riskiperusteinen valvonta, painotus kriittisiin kyberturvallisuusriskeihin
 - Traficomin suositus pohjana, mahdollisuus käyttää myös ulkopuolista asiantuntijaa
 - Dokumenttien katselmointi, haastattelut, tekniset menetelmät, etä/läsnä
- Tärkeälle toimijalle voidaan määrätä hallinnollinen seuraamusmaksu (max 7 000 000 euroa tai 1,4 prosenttia toimijan liikevaihdosta kumpi on suurempi), jos se tahallaan tai törkeästä huolimattomuudesta laiminlyö velvollisuudet (124/2025 35 §).
- Valvontaviranomaisten yhteistyö Traficomin vetämänä mm. yhteisten toimijoiden ja valvontakäytäntöjen osalta.



Lisätietoa

Ruokaviraston sivut

- NIS2.kyberturvallisuus@ruokavirasto.fi

Traficomin sivut

- [Direktiivin kohteena olevat organisaatiot](#) (Traficomin taulukko)
- [Traficomin suositus riskienhallinnan toimenpiteistä](#)

NIS2-direktiivi (EU) 2022/2555

Kyberturvallisuuslaki 124/2025

RUOKAVIRASTO

Livsmedelsverket • Finnish Food Authority

