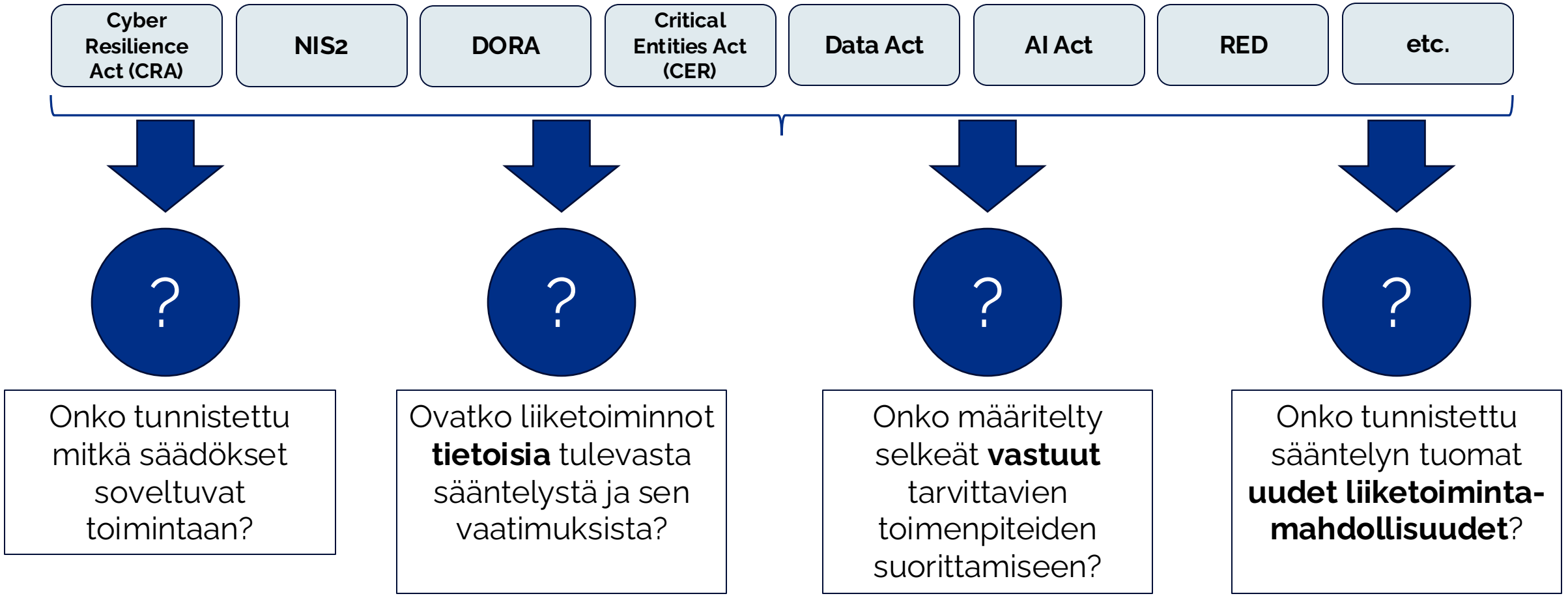
NIS 2

Jyrki Nivala, Insta Advance

Regulaatiotsunami?



Viimekädessä vastuu on organisaation ylimmällä johdolla

NIS2-lainsäädäntö lyhyesti

NIS2-direktiivin täytäntöönpano Suomessa

Direktiivin vaatimukset osaksi kansallista lainsäädäntöä

Suomessa NIS2-direktiviin velvoitteiden täytäntöönpanemiseksi säädetään uusi **laki kyberturvallisuudesta** eli ns. NIS2-yleislaki.

NIS2-yleislakia sovelletaan kaikkiin NIS2-direktiivissä määriteltyihin kriittisiin toimialoihin lukuun ottamatta julkishallintoa, jonka osalta velvoitteista säädetään tiedonhallintalaissa.

Kansallista lakia tulee soveltaa **18.10.2024 alkaen**.

Soveltamisala

Erittäin kriittiset ja muut kriittiset toimialat

Organisaatio kuuluu NIS2-direktiivin soveltamisalaan, **jos se toimii kriittisillä toimialoilla ja on kooltaan vähintään keskisuuri**

- Suuri toimija: palveluksessa on vähintään 250 työntekijää tai vuosiliikevaihto ylittää 50 miljoonaa euroa
- Keskisuuri toimija: palveluksessa on vähintään 50 työntekijää tai vuosiliikevaihto ja taseen loppusumma ylittävät 10 miljoonaa euroa

Soveltamisalaan kuuluvat toimijat jaetaan **keskeisiin ja tärkeisiin toimijoihin**

- **Yritys on keskeinen toimija, jos se toimii erittäin kriittisellä toimialalla ja on kooltaan suuri**
- Muut soveltamisalaan kuuluvat yritykset ovat lähtökohtaisesti tärkeitä toimijoita

ERITTÄIN KRIITTISET TOIMIALAT

- Energia
- Liikenne
- Pankkitoiminta ja finanssi-markkinoiden infrastruktuuri
- Terveys
- Jätevesi*- ja juomavesihuolto
- Digitaalinen infrastruktuuri
- TVT-palvelujen hallinta*
- Julkishallinto*
- Avaruus*

MUUT KRIITTISET TOIMIALAT

- Elintarvike*
- Valmistus*
- Posti ja kuriiripalvelut*
- Jätehuolto*
- Digitaalisen palvelun tarjoajat*
- Kemikaalisektori*
- Tutkimustoiminta*

*NIS2 uudet toimialat

Keskeiset velvoitteet toimijoille

- RISKIENHALLINTA JA JOHDON VASTUU
- RAPORTOINTI POIKKEAMISTA
- TOIMIJALUETTELOON ILMOITTAUTUMINEN

Johdon vastuu

Velvollisuus valvoa riskienhallinnan toteutumista ja huolehtia osaamisesta

Toimijan ylin johto on vastuussa viestintäverkkojen ja tietojärjestelmien kyberturvallisuutta koskevan riskienhallinnan toteuttamisesta ja valvonnasta. Vastuu tarkoittaa viimesijaista vastuuta järjestää ja resursoida riskienhallinta asianmukaisesti, sekä valvoa sen toimintaa.

Toimijan johto **hyväksyy** kyberturvallisuuden **riskienhallinnan toimintamallin sekä valvoo** riskienhallinnan toteuttamista, resursointia, toimenpiteitä, riskiarvioiden ajantasaisuutta ja toimenpiteiden vaikuttavuutta.

Toimijan johdolla tulee niin ikään olla riittävä ja ajantasainen **perehtyneisyys kyberturvallisuuden riskienhallintaan**, mikä edellyttäisi perehtyneisyyden hankkimista joko kouluttautumalla tai muulla vastaavalla tavalla säännöllisin väliajoin.

Osana riskien hallintatoimenpiteitä johto huolehtii myös **henkilöstön kyberturvallisuuskoulutuksen** järjestämisestä.

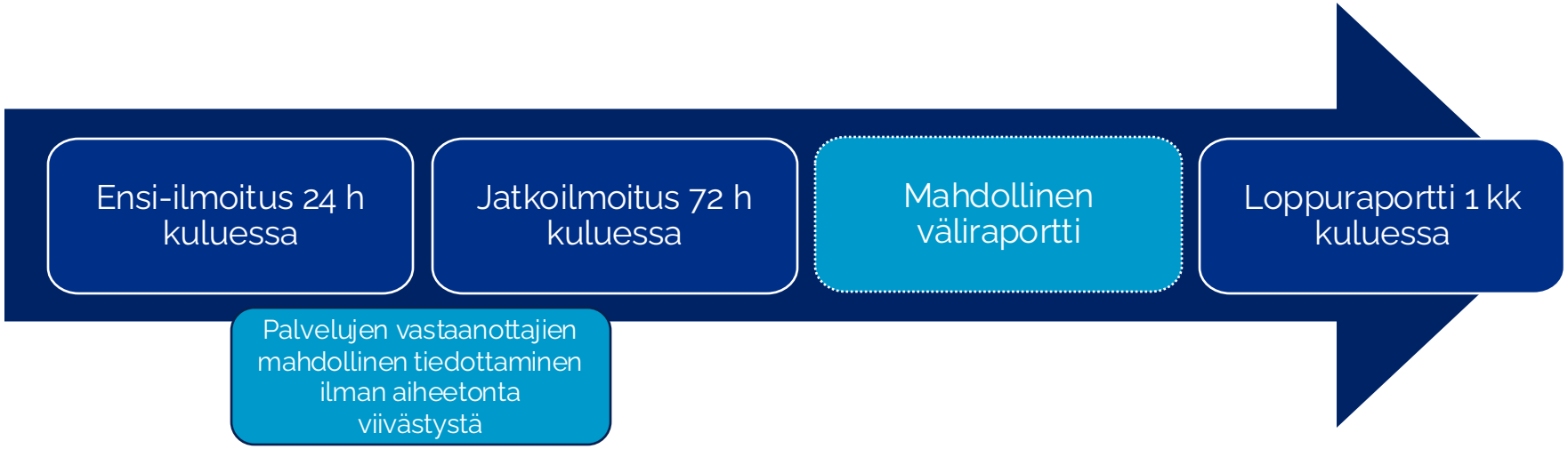
Valvova viranomainen voi rajoittaa keskeisen toimijan johdossa toimivien henkilöiden toimintaa, jos nämä toistuvasti ja vakavasti rikkovat velvollisuuksiaan.

Raportointivelvoite

NIS2-direktiivillä luodaan kolmiportainen raportointivelvollisuus valvovalle viranomaiselle merkittävistä kyberpoikkeamista.

Hallituksen esityksen mukaisesti liikenne- ja viestintäviraston Kyberturvallisuuskeskus toimisi tietoturvaloukkauksiin reagoivana ja niitä tutkivana CSIRT-yksikkönä.

Lisäksi toimijoiden on informoitava palvelujensa vastaanottajia merkittävistä kyberuhkista, jolla voi olla vaikutusta heihin, sekä toimenpiteistä, joita vastaanottajat voivat tehdä hallitakseen uhkaa.



Toimijaluetteloon ilmoittautuminen

Ilmoittautuminen jäsenvaltioiden ylläpitämään luetteloon keskeisistä ja tärkeistä toimijoista

Jäsenvaltiot ylläpitävät luetteloa keskeisistä ja tärkeistä toimijoista.

Toimijoilla on velvollisuus ilmoittaa toimijaluetteloa varten valvovalle viranomaiselle direktiivissä yksilöidyt tiedot sekä tiedon siitä, onko toimija keskeinen toimija. Valvovalle viranomaiselle on ilmoitettava myös osallistumisesta 22 §:ssä tarkoitettuun kyberturvallisuustietojen vapaaehtoiseen jakamisjärjestelyyn.

Valvova viranomainen voisi antaa tarkempia teknisiä määräyksiä tietojen ilmoittamisesta toimijaluetteloon.

Muutoksista toimijaluetteloon annettuihin tietoihin on ilmoitettava säädetyissä määräajoissa.

Valvontatoimenpiteet ja sanktiot

Sekä keskeisiin että tärkeisiin toimijoihin sovelletaan samoja riskienhallinta- ja raportointivelvollisuuksia. Valvonta- ja seuraamusjärjestelmät ovat kuitenkin tiukempia keskeisten toimijoiden osalta.

Keskeinen toimija toimii **erittäin kriittisellä** toimialalla ja on **kooltaan suuri**

Keskeinen toimija	Tärkeä toimija
• Ennakkovalvonta • Jälkivalvonta	• Ei ennakkovalvontaa • Jälkivalvonta
• Seuraamukset velvoitteiden laiminlyönnistä **enintään 10 milj. euroa tai 2,0 % vuosittaisesta liikevaihdosta**	• Seuraamukset velvoitteiden laiminlyönnistä **enintään 7 milj. euroa tai 1,4 % vuosittaisesta liikevaihdosta**

Riskienhallinta

Riskienhallintatoimenpiteet

1) kyberturvallisuuden **riskienhallinnan toimintaperiaatteet** ja riskienhallinnan toimenpiteiden vaikuttavuuden arviointi;

2) viestintäverkkojen ja tietojärjestelmien turvallisuutta koskevat toimintaperiaatteet;

3) viestintäverkkojen ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuus sekä tarvittavat menettelyt haavoittuvuuksien käsittelyyn ja julkistamiseen;

4) toimitusketjun toimittajien tuotteiden ja palveluntarjoajien palvelujen yleinen laatu ja häiriönsietokyky, tuotteisiin ja palveluihin sisällytetyt kyberturvallisuusriskien hallintatoimenpiteet sekä toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt;

5) omaisuudenhallinta ja turvallisuuden kannalta tärkeiden toimintojen tunnistaminen;

6) henkilöstöturvallisuus ja kyberturvallisuuskoulutus;

7) pääsynhallinnan ja todentamisen menettelyt;

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

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 toimijan toiminnassa;

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

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

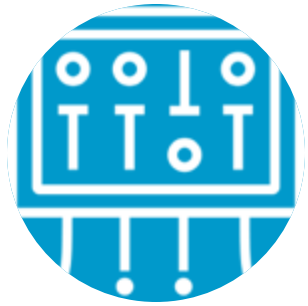
Havainnot NIS 2 projekteista

Johdon vastuu ja riskienhallinta

Riskienhallintakäytännöt eivät kata kyberturvallisuusriskejä.

Johto ei ole määritellyt kyberturvallisuuden riskienhallinnan toimintamallia

Johdon koulutuksen puutteet



Verkkojen ja järjestelmien turvallisuus

Ylätason dokumentaatio on (=tietoturvapolitiikka)

Tarkentavat politiikat puuttuu usein, esimerkiksi:
Verkon turvallisuus
Datan turvallisuus
…

Toimitusketju

Yhteistyökumppaneiden kyberturvallisuusvastuut ja kriittisyys

Häiriöiden vaikutusta liiketoimintaan ei ole kuvattu

Yleiset sopimusehdot

Havainnot NIS 2 projekteista

Pääsynhallinta

Least privilege käytännöt

Roolien kuvaukset

Dokumentaatio

Jatkuvuussuunnittelu

Palautumissuunnitelmat

Varmuuskopioinnin käytännöt

Testaaminen ja harjoittelu

Poikkeamien hallinta

Prosessikuvaukset

Juurisyyn selvittäminen

Raportointivelvoitteen täyttäminen

NIS 2 projekti

Kuvaus esimerkkiprojektista

Tavoitetilalle asetettu määräaika

Vaihe 1 | **Vaihe 2** | **Vaihe 3**

Aloitustilaisuus
- NIS2 esittely
- Johdon koulutus
- Projektin aikataulusta sopiminen

Nykytila-arvio
- Puutteet
- Riskienhallintaperiaatteet
- Priorisoitu road map

Toteutusvaihe
- Tunnistettujen puutteiden korjaaminen ja suunniteltujen toimenpiteiden toteuttaminen sisältäen mm.:
  - viestintäverkkojen ja tietojärjestelmien turvallisuutta koskevat toimintaperiaatteet
  - toimitusketjun kyberturvallisuuden hallinta
  - pääsynhallintamenettelyt
  - jatkuvuussuunnittelu sekä varmuuskopiointi ja palautumissuunnittelu
  - Poikkeamien hallintayms.
  - Tarvittavien koulutusten järjestäminen

Validointi
- Prosessien testaus
- (Sisäinen) auditointi

Ohjeita ja apuvälineita

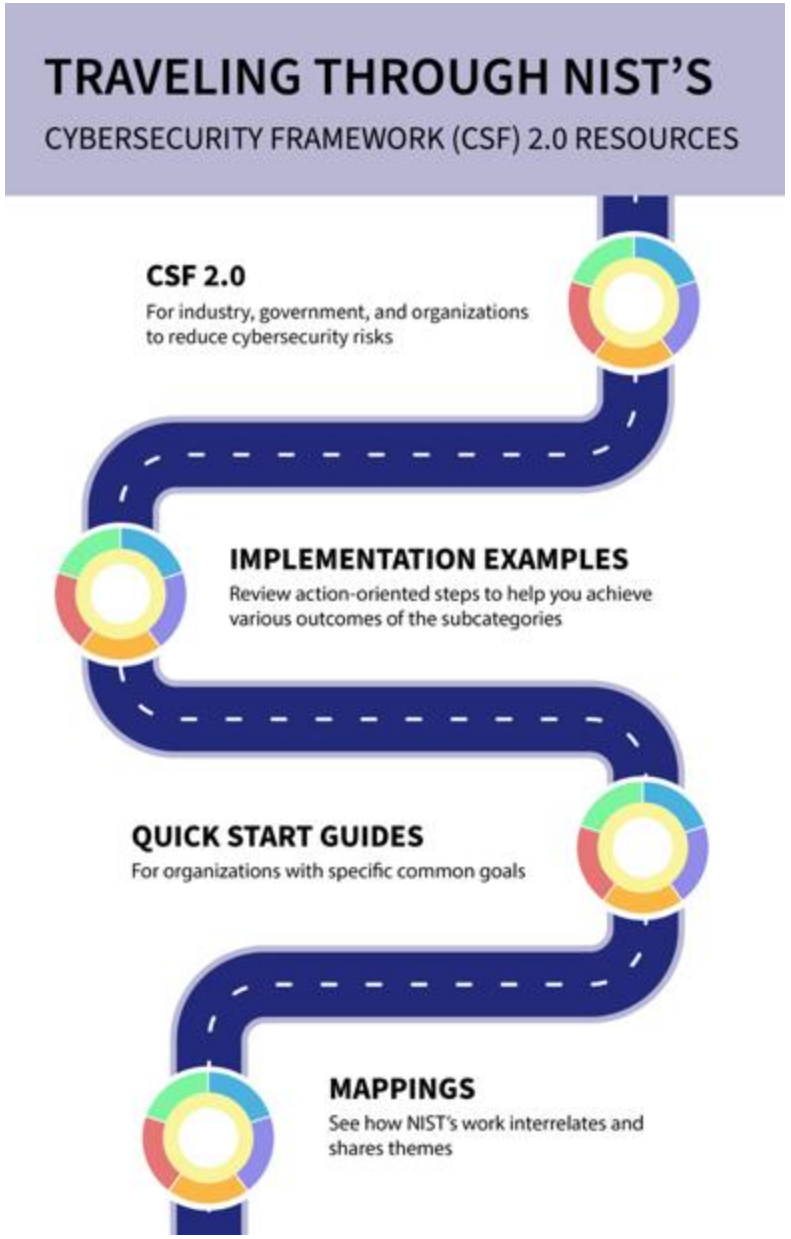
NIST CSF - ISO 27001 -Kybermittari

Finnish Information Security Cluster (FISC) on julkaissut EU:n verkko- ja tietoturvallisuusdirektiivi NIS2:n kansallisen **soveltamisoppaan**

- https://www.fisc.fi/fi/ajankohtaista/uutinen/kyberala-ry-julkaisi-eun-verkko-ja-tietoturvallisuusdirektiivin-nis2

Traficom: millaisia tavanomaisia toimenpiteitä laissa säädettäviin vaatimuksiin voi kuulua:

- https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=ebc51269-712e-4115-b137-b0b2a710dac4



Datasäädös
Data Act

Insta

Data and Cyber Compliance -palvelut

Datasäädös

Euroopan unionin datasääntely uudistuu. Suomalaisyritysten kannalta merkittävimpiin säädöksiin kuuluu EU:n uusi **datasäädös** (Data Act), joka tuli voimaan tammikuussa 2024. Sen soveltaminen aloitetaan vaiheittain siten, että merkittävää osaa datasäädöksen vaatimuksista tulee **noudattaa vuoden 2025 syyskuusta** alkaen.

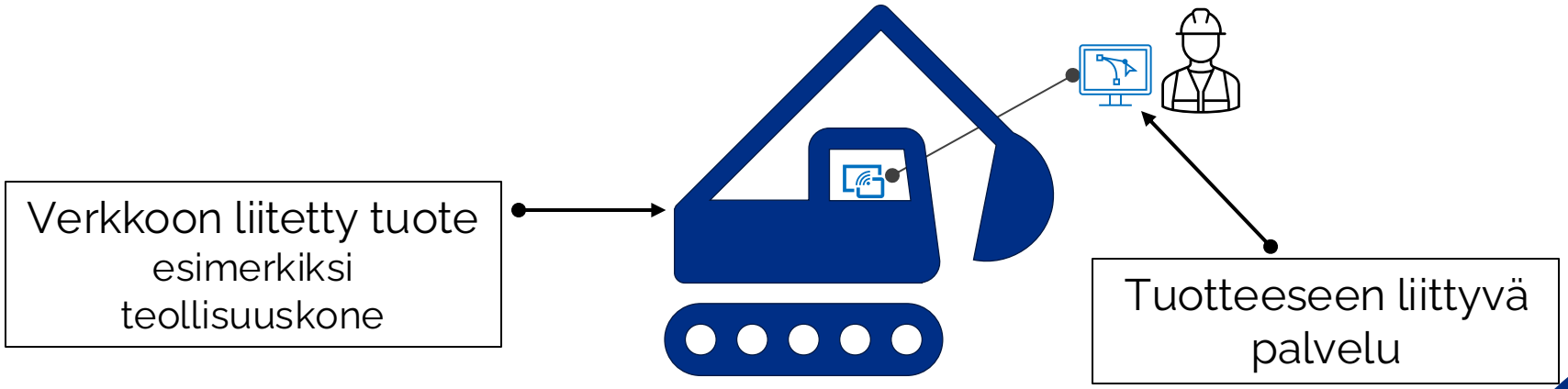
Datasäädöksellä on laajoja vaikutuksia mm. verkkoon liitettyjen tuotteiden valmistajille ja niihin liittyvien palveluiden tarjoajille.

Säädöksen merkittävimpiin velvoitteisiin kuuluu mm. se, että **verkkoon liitetyt tuotteet** ja niiden **liitännäispalvelut** tulee suunnitella siten, että käyttäjällä on lähtökohtaisesti pääsy omaan dataansa ja mahdollisuus jakaa sitä myös kolmansille osapuolille.

Datasäädös

Verkkoon liitetyillä tuotteilla tarkoitetaan muun muassa teollisuuskoneita ja älykkäitä kodinkoneita, jotka saavat, tuottavat tai keräävät sen käyttöä tai ympäristöä koskevia tietoja, ja jotka pystyvät välittämään dataa sähköisen viestintäpalvelun, fyysisen yhteyden tai laiteyhteyden kautta.

Tuotteeseen liittyvällä palvelulla tarkoitetaan digitaalista palvelua kuten ohjelmistoa, joka sisältyy tai on liitetty tuotteeseen siten, että tuote ei pystyisi ilman sitä suorittamaan jotain sen toiminnoista.



Installa on hallinnollisen tietoturvan, teknisen tietoturvan, ohjelmistokehityksen & datasääntelyn osaaminen samassa talossa, ja tämä mahdollistaa kokonaisvaltaisen kyvyn avustaa asiakkaitamme uudesta sääntelystä tulevien vaatimusten täyttämisessä.

Autamme organisaatiotasi saavuttamaan datasäädöksen edellyttämän vaatimustenmukaisuuden

Datasäädös (Data Act)

Kuinka valmistautua datan jakoon liittyviin velvoitteisiin?

Datainventaari ja tietojen luokittelu

- **Tunnista ja luokittele** säädöksen soveltamisalaan kuuluva data (ml. liikesalaisuudet, arkaluonteiset tiedot, henkilötiedot)
- **Määrittele** tiedot, jotka tulevat olemaan suoraan käyttäjien saatavilla
- **Määrittele** tiedot, jotka tulevat olemaan haettavissa ja toimitettavissa käyttäjän pyynnöstä kolmansille osapuolille

Riskienhallinta

- **Tunnista ja arvioi** datan jakamiseen ja pääsyyn liittyvät riskit
- **Suunnittele ja toteuta** riittävät tekniset ja organisatoriset suojakeinot data- ja kyberriskien hallitsemiseksi → ota huomioon GDPR ja tietosuojaan liittyvät vaatimukset, sekä liikesalaisuuksien suojaaminen

Suunnittele pääsy dataan

- **Suunnittele** miten käyttäjien suora pääsy dataan mahdollistetaan
- **Suunnittele** miten 'helposti saatavilla oleva data' tullaan toimittamaan tai asettamaan käyttäjän pyynnöstä kolmansien osapuolien saataville
- **Suunnittele** prosessi ja mekanismi datan jakamiseen liittyvien pyyntöjen käsittelyyn

Sopimukset ja läpinäkyvyys

- **Valmistele säädöksen edellyttämä dokumentaatio** käyttäjän informoimiseksi tuotteen tai palvelun datan keräämisestä ja käytöstä
- **Suunnittele ja valmistele** tarvittavat muutokset sopimuksiin → ota huomioon mm. GDPR ja tietosuojaan liittyvät vaatimukset, sekä liikesalaisuuksien suojaaminen

Datasäädös – kuinka saavuttaa vaatimustenmukaisuus?

Kuvaus esimerkkiprojektista Instan fasilitoimana

Tavoitetilalle asetettu määräaika

Vaihe 1 | **Vaihe 2** | **Vaihe 3**

Aloitustilaisuus
- Datasäädöksen esittely
- Osapuolten esittely
- Toimintatapojen määritteleminen
- Projektin aikataulusta sopiminen

Nykytila-arvio
- Datasäädöksen vaatimuksiin vastaavien kyvykkyyksien tunnistaminen
- Datainventaarin ja tietojen luokittelun nykytila arvioiminen
- Tavoitetilan ja tarvittavien toimenpiteiden suunnitteleminen (Road Map)

Toteutusvaihe
- Tunnistettujen puutteiden korjaaminen ja suunniteltujen toimenpiteiden toteuttaminen sisältäen mm.:
  - datainventaari ja tietojen luokittelu;
  - tekniset resurssit;
  - dokumentaatio;
  - prosessit;
  - sopimuspohjat ja käyttöehdot;
  - tekniset ja organisatoriset suojakeinot;
  - yms.
- Tarvittavien koulutusten järjestäminen

Validointi
- Prosessien testaus
- (Sisäinen) auditointi

https://www.insta.fi/fi/kyberturvallisuus/

jyrki.nivala@insta.fi

0407208007