

# Sytyke

REGULAATIOT TIEDONHALLINNAN TUKENA

# TIVIA 70

TIVIAN 70-vuotisjuhlavuoden  
huipentava **juhlaseminaari ja  
cocktailtilaisuus** järjestetään  
keskiviikkona 8.11.2023  
Messukeskuksessa Teknologia  
23 -tapahtuman yhteydessä.



Juhla kokoaa yhteen ICT-alan päättäjät,  
tekijät ja vaikuttajat.

**Juhlaseminaari** polkaistaan käyntiin klo 14.00  
TIVIA Stagella, jossa ohjelmassa on esityksiä  
ja paneelikeskustelu teemalla "ICT:llä  
tulevaisuutta tekemässä".

**Cocktailtilaisuus** Messukeskuksen Pihka  
& Bar -ravintolassa alkaa klo 16.30. Rento  
cocktailtilaisuus pitää sisällään sopivasti  
asiaa, sekä luo hyvät puitteet pitää yllä ja  
luoda uusia kontakteja. Cocktailtilaisuus  
kestää klo 21.00 asti.



Kiinnostaako TIVIA 70 -sponsoripaketit?

Ota yhteyttä toimitusjohtaja Juha Lappiin:  
juha.lappi@tivvia.fi tai 044 528 0892

➔ [tivvia.fi/tivia70](https://tivvia.fi/tivia70)



Pohjoismaiden johtava  
teknologia-alan tapahtuma  
Teknologia 23 järjestetään  
Messukeskuksessa  
7.-9.11.2023.




Tapahtuman ohjelmalavoilla järjestetään  
kolmen päivän aikana yhteensä noin 150  
puheenvuoroa. Yksi ohjelmalava on pyhitetty  
ICT:lle ja se on tuttuun tapaan TIVIA Stage.

Puheenvuorojen lisäksi tapahtuma kokoaa  
yhteen alan yritykset, asiantuntijat ja  
päättäjät verkostoitumaan, keskustelemaan ja  
oppimaan uutta.

Kaikkina kolmena päivänä omalla TIVIA  
Stagellamme on ohjelmaa DAMA Finlandin,  
TIVIA Uusimaan, Sytykkeen, Tietoturvan ja  
TIVIAN järjestämänä.




## POIMINTOJA OHJELMASTA

 **IT:n kiertotalous**  
Tuulia Virhiä

 **Tekoäly ja työn tulevaisuus**  
Petteri Järvinen

 **Tekoälyn ja datan energiakulutus**  
Janne Kalliola

 **Digitaalisen palvelun modernisointi**  
Juhana Harmanen

➔ [tivvia.fi/teknologia23](https://tivvia.fi/teknologia23)





# Ohjaako regulaatiot tiedonhallintaa?

Tietomäärien kasvu ja toiminnan kompleksisuus on lisännyt tiedonhallinnan ohjaustarvetta ja aika monella alalla onkin lakisääteisiä vaatimuksia, miten tietoa tulisi hallita. Mm. julkishallinnon tiedonhallinnan laki, pankkien Basel-regulaatiot ja kaikille yhteinen tietosuojalaki, joka varmistaa henkilötietojen laillisen käytön.

Itse olen havainnut tiedonhallinnallisen työn helposti lähtevän liikkeelle siitä, että halutaan varmistaa vain regulaatioiden vaatimukset ja perustetaan tätä varten kehitysprojekti. Se on kuin pyöräilisi yksipyöräisellä. Käytetään paljon aikaa ja energiaa, jotta viranomaiset ovat tyytyväisiä, mutta huomioidaanko tällöin muuta liiketoiminnallista kehitystä.

Kun ensimmäiset tietosuojajärjestykset on tehty, niin on huomattu, että olisiko myös muulla liiketoiminnalla tarpeita tiedonhallinnan kehitykseen. Kun on kuvattu tietovirtoja regulaatiota varten, onkin huomattu, että tästähän voisi olla hyötyä muullekin kehittämislle. Tätä maturiteettivaihetta voisi verrata ensimmäisiin polkupyöriin, jossa etupyörän tueksi on pienen pieni takapyörä.

Aikaa myöten tiedonhallintaa opitaan kehittämään omien liiketoiminnallisten tarpeiden ja vaatimusten täyttämiseksi. Yllättäen huomataan, että samoilla tiedonhallintaa kehittäville toimenpiteillä voidaankin vastata näihin regulatiivisiin vaateisiin. Ehkä nyt siis arvaat jo seuraavan vaiheen tuohon pyöräilyanalogiaan. Kyse on modernista pyörästä, jossa etu- ja takarengas ovat samankokoisia. Näin viedään organisaatiota eteenpäin sujuvasti ja tiedosta, jonka hallinta on tehokasta, syntyy aitoa pääomaa. Samalla on myös tunnustettu tarve jatkuvuuteen. Mm. organisaation tietomallin tekeminen ei ole yksittäinen projekti vaan sille on oltava hallintamalli, jolla varmistetaan tietomallin oikeellisuus myös tulevaisuudessa.

Tässä lehdessä pääset lukemaan artikkeleja sekä regulaatioiden näkökulmasta, että myös liiketoiminnallisen tiedon hyödyntämisestä. Koska tietosuoja koskee myös yhdistyksiä, kirjoitti Paula artikkelin, miten yhdistyksen tulisi huomioida tietosuojan vaatimukset toiminnassaan.

Lehden luettuasi voitkin pohtia, missä vaiheessa oman organisaatiosi tiedonhallinta on?

Hyviä lukuhetkiä ja energiaa syksyyn!

*Minna Oksanen*

## Sisältö

- 4. Myrskyn jälkeen oli bisnessää • [Tuomas Huokuna](#)
- 8. Ketterää datan hallintaa regulaatioviidakossa • [Juuso Viljanen](#)
- 10. Uusi tietosuojasopimus EU:n ja Yhdysvaltojen välille • [Juha Sallinen](#)
- 14. Kohti tarkempia tietosuojaohjeita • [Ari Andreasson](#)
- 18. Yhdistyslaki ja GDPR yhdistystoiminnassa • [Paula Miinalainen](#)
- 22. Tietojärjestelmien sääntelyn rajat ja reunaehdot • [Risto Nevalainen](#) ja [Heikki Uusitalo](#)
- 26. Tietoturvasuvasuositukset hankinnoissa • [Tuula Seppo](#)
- 30. Suomen merenkulun uusi aikakausi: Vähäpäästöisyys, logistiikkakustannukset ja viennin kilpailukyky • [Olli Soininen](#)
- 36. Historian havinaa: Tiedon elinkaari hallintaan • [Päivi Happonen](#)
- 38. Kuutamolla

**Julkaisija**  
Systeemyöyhdistys SYTYKE ry

TIVIA ry  
Firdonkatu 2 T 63  
Spaces Tripla, 6krs  
00520 Helsinki  
Vaihe: 020 741 9898

**Toimituskunta**  
Minna Oksanen  
Timo Piiparinen

**Päätoimittaja**  
Timo Piiparinen

**Painos**  
ISSN: 2323-8283  
Verkkojulkaisu  
11. vuosikerta

Lehti on aiemmin ilmestynyt  
- Sytyke-Sanomien (1987-1993)  
- Systeemyö (1994-2012)

**Taitto**  
Visionomi, [www.visionomi.net](http://www.visionomi.net)

Toimitus ei ota vastuuta yksittäisten kirjoittajien mielipiteistä eikä asiavirheistä.



## Tuomas Huokuna

Kirjoittaja työskentelee IT-alan tietosuoja- ja lakiasiaan parissa sekä tekee väitöskirjaa tietosuoja- ja yksityisyyden suhteesta Itä-Suomen yliopistossa.

[tuomas.huokuna@q-factory.fi](mailto:tuomas.huokuna@q-factory.fi)

# Myrskyn jälkeen oli bisnessää

## GDPR tuli – mitä seuraavaksi?

Toimialasta ja tehtävästä riippumatta olemme viime vuosina kohdanneet eurooppalaisen tietosuoja- ja informaatio-oikeudellisen sääntelyn lisääntymisen. Digitaalinen maisemamme, jossa analytiikka-perhoset pörräsivät ja tietovirrat solisivat vapaasti, nettipalvelujen polut mutkittelivat vapailla mailla ja tiedon valtaväylää kuljettiin mieli keveänä, on muuttunut pysyvästi huomattavasti säädellymmäksi ympäristöksi.

Tietosuoja-sääntelyn kruununjalokivenä yleinen tietosuoja-asetus (tästädes GDPR) toi Brysselin keskiöön mitä tulee internetin pelisääntöihin ja henkilötietojen käsittelyyn. Samaan aikaan monimutkaistuva, digitalisoitua ja muuttuva maailmamme vaatii enemmän sähköisiä palveluja. Toisaalta mitä edemmä digitalisaatio etenee, sitä voimakkaammin se näkyy yksilön arjessa – monella asiassa aiemmin digitaalinen vaihtoehto on asettumassa ainoaksi vaihtoehdoksi. Merkittävä osa palveluista on yhteiskunnan ydintoimintoja tai jokapäiväisiä palveluja, joita jokainen voi tarvita kuten sähköiset hakemuskanavat, taksisovellukset, asiakaspalvelutilanteet ja pankkipalvelut. Ei puhuta enää vain edelläkävijöiden murheesta, vaan tilannetta on ainakin lainsäätäjän tarkasteltava myös saavutettavuuden ja yhdenvertaisen käytettävyyden kannalta.


Tietosuojalainsäädännön maisemaa hallitsi

jonkin aikaa yksi iso, ehkä tavoittamattomaksikin koettu huippu – GDPR. Aiemman sääntelyn puitteissa kevyesti kulkeneet rekisterinpitäjät joutuivat tietosuoja-asetuksen jyrkenteille, ja askeleet täytyy nykyään sovittaa tarkemmin kuin aikaisemmin. Tietosuoja-asetuksen lisäksi Unioni lainsäätäjänä on kääntänyt katseensa tekoälyn, digitaalisen ja digitaalisten palvelujen yhteismarkkinan<sup>1)</sup> sekä digitaalisen tiedon hyödyntämisen suuntaan. Digi- ja internetlainsäädäntö laajenee henkilötietojen ohi muidenkin tietolustojen ja -varantojen suuntaan.

Muuttuva säädosympäristö ja laajeneva sääntelyn fokus tarjoaa kuitenkin mahdollisuuksia, kuten digimarkkinasääntely, joka on suunnattu tuomaan yhteismarkkinan mahdollisuudet paremmin myös pienempien kaupallisten toimijoiden ulottuville. Digital Services Act ja Digital Markets Act pakottavat ”portinvartijat” – alustapalvelut, tiedonkerääjät, ekosysteemien omistajat – avaamaan pääsyä tietoon ja sen hyödyntämiseen myös pienemmille toimijoille – yksilön oikeudet ja vapaudet muistaen.

Yhtenä kannustimena viilata prosesseista turhaa käsittelyä ja päällekkäisyyttä pois, sekä mahdollistaa mahdollisimman sujuvaa tiedonkäsittelyä voinee nähdä myös vastuullisuuskysymykset; jo nykyään digitaalisen toiminnan energiankulutus nousee toisinaan keskusteluun. Sujuvat tietopro-





sessit ovat tehokkaita ja sikäli tukevat myös ESG-ohjelmien toteuttamista.

Sääntelyyn valittu malli ei kuitenkaan ole ongelmaton. GDPR:n osalta monelle tulivat tutuksi sanktioita koskevat kirjaukset. Hallinnollinen seuraamusmaksu asetusta tehostamassa ei sinänsä ole uusi keksintö, vaan seuraamusmaksut ovat Unionin oikeutta seuraavalle tuttuja jo kilpailuoikeuden puolelta. Kilpailuoikeudellista järjestelmää voi jossain määrin pitää myös verrokkina sille, miten tietosuojasääntely kehittyi: vuosikymmenten oikeuskäytäntö ja määrätietoinen lainsäädäntötyö ovat kehittäneet Unionin kilpailuoikeuden suhteellisen ennustettavaksi järjestelmäksi. Tietosuojaan ja digitaalisiin palveluihin liittyy kuitenkin kilpailuoikeudellisesti vähemmän korostunut sudenkuoppa: palveluja on helppo hankkia mistä vain. Digitaaliset palvelut ovat siis alttiina eri valtioiden tietosuojaa valvovien viranomaisten tutkimuksille. Säädöskehikko on sama Unionin laajuisesti, mutta valvovien viranomaisten suhtautuminen ja toimintatapa voivat erota, mikä asettaa haasteita rajat ylittävän toiminnan suhteen. Toisena lainsäädäntöhankkeita yhdistävänä haasteena on se, että teknologianeutraalin sääntelyn sijaan säännellään yksittäisiä teknologioita – kuten tekoälyä. Toisaalta sääntely, joka asettaa vain periaatteellisia rajoja, ei sekään ole kovin helppo pähkinä purtavaksi, kuten

GDPR:n muotoilut monin paikoin osoittavat. Teknologiakohtainen sääntely on altis aukoilille ja sille, että se ei yksinkertaisesti pysty huomioimaan uusia teknologioita. Esimerkiksi 2023 kevään aikana suureen tietoisuuteen murtautunut ChatGPT on hyvä esimerkki teknologiasta, jonka kontrolloiminen lainsäädännöllä on vaikeaa. Italiassa se päädyttiin hetkellisesti kieltämään tietosuojassa olleiden puutteiden perusteella.<sup>2)</sup>

Liiketoiminnan näkökulmasta haasteena on se ristiveto, joka vallitsee GDPR:n hyvin laajan ja helposti relevantiksi tulevan henkilötiedon ja käsittelyn määritelmien ja toisaalta suojatoimien monimutkaisuuden mukaan. Väinö Linnan Lammiota mukaillen voisi todeta että ”tietosuojalainsäädäntö astuu voimaan kaikessa ankaruudessaan” hyvin kevyin perustein. Ankarien tietosuojavastuiden neuvottelemisen sopimuksiin tilanteissa, joissa esimerkiksi konsultti saattaa nähdä asiakkaan yhteyshenkilöiden tietoja – tallentamatta tai tiedolla mitään tekemättä, ja todennäköisesti vartissa ne jo unohtaneena – ei ole omiaan vahvistamaan kokemusta sääntelyn noudattamisen mielekkyydestä. Tietosuoja, kuten muukin turvallisuus, syntyy pohjimmitaan pienistä asioista ja perusteiden alituisesta ja tinkimättömästä huomioimisesta, minkä takia sääntelyn olisi näyttydyttävä aina perusteltuna ja oikein kohdentuvana.

Samalla kun yhtiöt puurtavat käsittelyperiaatteidensa kanssa kukin resurssiensa rajoissa parhaansa mukaan, on maisemassamme eräs myrskyrintama, joka tuntuu palaavan aina takaisin – tiedonsiirrot kolmansiin maihin. Määritelmällisesti tämä sisältää myös kolmannesta maasta omistetun pilvipalvelun käyttämisen<sup>3)</sup>. Kolmansiin maihin (Yhdysvallat olennaisimpana) siirtyy paljon tietoa. Tässäkin laajat määritelmät tuovat haasteita erityisesti sen arvioimisessa mitä täydentäviä suojatoimia tarvitaan. Aiheeseen liittyen on ollut mielenkiintoista seurata Itämeren rannoilla Tukholman ja Helsingin jossain määrin toisistaan poikkeavaa suhtautumista asiaan.

Tiedonsiirtojen osalta ennustettavaa on lähinnä se, että tilannetta ratkotaan ”paikkaa paikan päälle”-ratkaisuilla, jotka tietosuoja-aktiivit kaatavat EU:n tuomioistuimessa kotvasen kuluttua, jonka jälkeen epävarmuus taas jatkuu, kunnes poliittinen koneisto tuottaa seuraavan kompromissin. Tämän kirjoittamishetkellä EU-US Data Privacy Framework-sopimus EU:n ja Yhdysvaltojen välillä ottaa ensiaskeleitaan. On mielenkiintoista nähdä, miten pitkäikäiseksi se osoittautuu.

Lainsäädännön vaatimukset ovat luonteeltaan sellaisia, että liiketoiminnan pitäminen vaatimusten

mukaisella tasolla vaatii jatkuvaa työtä. Jotta tietovirrat, käsittelypisteet, käsittelijäryhmät ja tietojen luovutukset pystytään vaatimusten mukaisesti kartoittamaan, analysoimaan, täytyy organisaation oikeasti tuntea nämä asiat. Tarkoituksen – eikä vaatimusten! mukaista ei ole se, että tietosuojavastaava kammiossaan kirjaa haavekuvansa viralliseksi politiikaksi ja tilannetiedoksi. Digitaaliset palvelut ja niihin liittyvät prosessit ovat vahvasti osa liiketoimintaa melkein yhtiössä kuin yhtiössä, joten niiden aito ymmärtäminen tuottaa väistämättä tilannekuvaa myös liiketoiminnan prosesseista. Tieto on valtaa, ja lainsäädäntö pakottaa digitaaliset palvelut ja niiden toimijat tuntemaan itsensä ja kumppaninsa.

Eurooppalaisilla yhtiöillä on myös se etu, että kun ne noudattavat ”kotilainsäädäntönsä” vaatimuksia, ei yleensä tarvitse kehittää toimintaa uusille markkinoille siirryttäessä. Tutkimuksessa tätä kutsutaan ”Bryssel-efektiksi”: kansainvälisesti toimivat yhtiöt harmonisoivat globaalisti toimintamallinsa Euroopassa vaaditulle tasolle, koska Euroopassa toiminen edellyttää niin korkeatasoisten vaatimusten täyttämistä, että eurooppalaisesti hyväksyttävä toimintamalli täyttää vaatimukset muillakin alueilla.<sup>4)</sup>



## Lähteet

1. EU-asetukset 2022/1925 (Digital Markets Act) ja 2022/2065 (Digital Services Act)
2. <https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9870847#english> (31.8.2023)
3. EDPB Guidelines 05/2021, v 2.0, saatavilla [https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052021-interplay-between-application-article-3\\_en](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052021-interplay-between-application-article-3_en)
4. Anu Bradford: The Brussels Effect - How the European Union Rules the World. OUP 2020.





Ilmianna itsesi tai tuntemasi hyvä tyyppi

## SYTYKKEEN HALLITUKSEEN

Meillä hallituksessa ei briljeerata käyntikorteilla,  
emmekä me lainaa latinankieltä, koska emme pohdi  
toistemme ansioluettelo.

Meillä hallituksessa vasta valmistuvan tai valmistuneen nuoren  
näkökannat ovat aivan yhtä merkitykselliset kuin  
jo monessa liemessä marinoituneen konkarin aivoitukset.  
Toki muistamme antaa arvon myös kokemukselle.

Meillä hallituksessa olemme suomalaisen tietojärjestelmätyön ytimessä.  
Meidän kauttamme emme ole pelkästään näköalapaikalla  
vaan myös luomassa näköalaa. Koko toimialalle.  
Olemme vahvoja esille nostajia, olemme keskustelun aloittajia.  
Meidän julkaisuja lainataan akateemisessa maailmassa.  
Meillä hallituksessa pääset oikeasti vaikuttamaan.  
Meillä on ääni.

Ota rohkeasti yhteyttä, ilmoita itsesi tai tuntemasi hyvä tyyppi.  
Kerro itsestäsi tai hänestä vapaamuotoisesti ja postita tuo  
kertomus puheenjohtajallemme:  
puheenjohtaja (ät) sytyke.org





## Juuso Viljanen

Kirjoittaja toimii johtavana konsulttina Knowit Solutionsissa. Datan ja analytiikan kehitys tekniseltä, kulttuuriselta sekä strategiselta kulta-  
malta ovat hänen vahvuusalueita. Kiinnostus-  
alueita löytyy niin kestävästä kehityksen, visuaa-  
lisen analytiikan kuin myös palvelumuotoilun  
osa-alueilta. Regulaatiot, niiden vaikutus datan  
ja analytiikan osa-alueilla sekä niiden muodos-  
tamien vaikutukset ja mahdollisuudet ovat osa  
Juuson päivittäistä työtä.

# Ketterää datan hallintaa regulaatioviidakossa

Datan ja datalähteiden määrä kasvaa räjähdysmäisesti samalla kun regulaatio datan hallinnan ympärillä tiukentuu. Datan hallinta aiheuttaa haasteita etenkin maailmassa, jossa dataa mieluiten hyödynnettäisiin ketterästi. Ketterä datan hallinta vaatii toimintaympäristön tuntemista, hyvin suunniteltuja prosesseja, teknologiaa ja osaamista.

Ketterä datan hallinta antaa kykyä sopeutua nopeasti muuttuviin tarpeisiin ja mahdollisuuksiin, mahdollistaen datan nopean analysoinnin ja käytön päätöksenteossa. Kun dataa saadaan tarvittaessa käyttöön nopeasti, voidaan mahdollistaa esimerkiksi reaaliaikaiseen asiakastietoon pohjaava henkilö palvelu. Datan ketterä hyödyntäminen voi myös auttaa reagoimaan nopeammin kilpailijoiden toimiin ja edistää innovointia, esimerkiksi tuomalla poikkeavia kohderyhmiä tai käyttökohteita näkyviksi.

Toisin kuin usein ajatellaan, regulaatiosta voi itse asiassa olla paljonkin hyötyä datan hallinnalle. Tietosuojan ja tietoturvan varmistaminen rakentaa luottamusta asiakkaisiin ja sidosryhmiin ja osaltaan mahdollistaa toimimista myös kansainvälisissä ympäristöissä. Regulaatioiden asettamat vaatimukset datan keräämiselle, tallentamiselle ja käsittelylle voivat myös auttaa yrityksiä parantamaan datan laatua ja tarkkuutta. Yhteistyö regulaattoreiden ja oman alan vertaisorganisaatioiden kanssa voi auttaa toimimaan parhaiden käytäntöjen mukaisesti.

Jotta datan hallinnassa voitaisiin noudattaa vaadittavaa regulaatiota ja olla yhä ketteriä, on noudatettava muutamia keskeisiä periaatteita:

## Tunne toimintaympäristösi

Ensimmäinen askel toimivaan datan hallintaan

on ymmärtää liittyvät säännökset. Osa datasta on julkista tietoa, jota ei tarvitse erityisesti suojella. Sen sijaan henkilötiedot ja esimerkiksi terveystiedot täytyy pitää visusti salassa. Juuri henkilötietojen keräämiseen ja käsittelyyn keskittyy myös datan hallintaa viime vuosikymmenen lopulla mullistanut yleinen tietosuojalaki GDPR. Seuraavaksi yhä useammilta yrityksiltä vaaditaan tarkempaa vastuullisuusraportointia.

## Luo datan hallinnan strategia ja valjasta teknologia avuksesi

Modernit analytiikkatyökalut ovat helppokäyttöisiä ja tehokkaita, joten niiden avulla muutkin kuin IT-asiantuntijat voivat tehdä töitä datan parissa. Tiedonhallinnan kannalta katsottuna modernit työkalut voivat kuitenkin olla sekä siunaus että kiros. Ilman selkeää ymmärrystä kuka omistaa mitkin ja kenellä on vastuu mistäkin, voi olla hyvin hankalaa pitää modernien työkalujen muodostamat mahdollisuudet niin sanotusti kurissa.

Datan hallinnalle tulee laatia selkeä strategia, joka ottaa huomioon sekä regulaatiot että organisaatiosi tarpeet datan käytölle. Datan hallinnan strategian tulisi sisältää suunnitelmat tiedonkeruusta, tallennuksesta, datan käsittelystä ja sen poistamisesta. Strategiaa laatiessa on syytä arvioida mahdolliset datan käsittelyyn liittyvät riskit ja laatia



Alistaminen

Standardit  
Säännöt  
Kontrolli  
Vakaus

Nopeus  
Vapaus  
Luovuus  
Muutos

Kaaos

## Kaaoksen ja alistamisen tasapaino

Lähde: bi-survey.com

suunnitelma niiden vähentämiseksi ja hallitsemiseksi.

Avuksi kannattaa ottaa tietosuojateknologiat ja -ratkaisut, jotka auttavat sinua automatisoimaan ja hallitsemaan tietosuojan ja tietoturvan vaatimuksia. Esimerkiksi pseudonymisointi, salausta ja käyttöoikeuksien hallinta ovat hyödyllisiä apuvälineitä.

### Etsi tasapaino kontrollin ja vapauden välillä

Datan hallinnan keskeinen päätös liittyy siihen, kuka mitään dataa saa nähdä tai käsitellä. Täydellinen turvallisuus voidaan saavuttaa ainoastaan, jos kenelläkään ei ole pääsyä mihinkään dataan. Silloin datasta ei tosin ole mitään hyötyäkään.

Datan hallinta on sen optimikohdan etsimistä, jossa vähintäänkin noudatetaan lainsäätäjien tahtoa ja huolehditaan tietoturvasta, mutta annetaan riittävästi vapautta datan hyödyntämiseen, että työntekijät voivat tehdä valistuneita liiketoimintapäätöksiä. Kyse on käytännössä tasapainoilusta alistamisen ja kaaoksen välillä.

Datekemistä ei missään nimessä pidä rajata IT-osastolle. Datan omistaja saisi mieluiten olla sellainen, jolla on mahdollisuus tehdä toimintaan liittyviä päätöksiä datan pohjalta. Omistajan täytyy tiedostaa oma roolinsa ja ymmärtää, että

esimerkiksi datan laatuun liittyvissä ongelmissa vastuu on ensisijaisesti hänellä. Pitkälti digitalisoituneessa maailmassa ei ole mitenkään perusteltua ajatella, että kaikki digitaaliset tehtävät kuuluisivat vain tietotekniikan asiantuntijoille.

Kouluta ja viesti jatkuvasti ja ole valmis sopeutumaan

Datan hyödyntämisen täytyy olla yrityksen arkea, ja johdon täytyy näyttää asiassa esimerkkiä. Henkilökuntaa täytyy kouluttaa säännöllisesti regulaatioiden vaatimuksiin ja niiden muutoksiin. Regulaatioiden noudattamiseen kannattaa myös luoda valvontaprosessi.

Datan suojaamisesta ja regulaation noudattamisesta kannattaa viestiä selkeästi organisaatiosi sisällä ja sidosryhmille. Tämä on omiaan lisäämään luottamusta ja avoimuutta. Regulaatioiden noudattamiseen kannattaa kehittää oma seuranta- ja raportointiprosessinsa.

Datanhallintaprosessit kannattaa rakentaa joustaviksi ja skaalautuviksi, jotta voit sopeutua muuttuviin regulaatioihin ja kasvavaan datan määrään. Vaikka regulaatiot voivat tuoda lisähaasteita datanhallintaan, ne myös auttavat lisäämään tietosuojaa, tietoturvaa ja sen myötä kasvattavat asiakkaiden luottamusta. Hyvin rakennettu datanhallintastrategia ja -prosessit voivat auttaa organisaatiotasi saavuttamaan ketteryyttä regulaatioista huolimatta.





## Juha Sallinen

Juha Sallinen on yrittäjä, tiedonhallinta- ja teknologia-arkkitehti. Sallisen vuonna 2016 perustama yritys GDPR Tech on Pohjoismaiden johtava ja kokenut EU:n tietosuojasopimukseen keskittynyt yritys. Yrityksen ratkaisupalikoimaan kuuluu muun muassa GDPR konsultointi ja koulutukset. Yritys toimii sekä Pohjoismaissa että Baltiassa.

[www.gdprtech.com](http://www.gdprtech.com)

# Uusi tietosuojasopimus EU:n ja Yhdysvaltojen välille

Euroopan komissio antoi 10.7.2023 riittävyyspäätöksen Euroopan Unionin (EU) ja Yhdysvaltojen väliselle tietosuojakehykselle. Euroopan komission tekemä riittävyyspäätös Data Privacy Framework (DPF) sallii nyt henkilötietojen siirron EU:sta Yhdysvaltoihin niiden toimijoiden välillä, jotka ovat DPF:n piirissä.

Mutta mitä "siirto" todella tarkoittaa? Voimmeko nyt luotettavasti käyttää yhdysvaltalaisia palveluntarjoajia? Ja kuinka tunnistaa, kuuluuko jokin toimija DPF-sopimuksen piiriin? Tässä artikkelissa käymme läpi nämä kysymykset ja tarjoamme selkeitä vastauksia.

## Termit tutuiksi – mitä tarkoittavat henkilötiedot ja henkilötietojen käsittely?

Ennen tarkempaa syventymistä itse aiheeseen ja henkilötietojen siirtoon, on hyvä täsmentää, mitä henkilötiedot ja henkilötietojen käsittely tarkoittavat. Suomen tietosuojavaltuutetun toimisto ohjeistaa lyhyesti: ”Henkilötietoja ovat kaikki tiedot, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan henkilöön. Henkilötietoja ovat esimerkiksi nimi, puhelinnumero ja sijaintitiedot. Lisäksi suuri joukko muuta tietoa voidaan lukea henkilötietojen alle, kuten asiakas-ID ja IP-osoite.”

Henkilötietojen käsittely puolestaan tarkoittaa esimerkiksi henkilötietojen keräämistä, säilyttämistä, käyttöä, siirtämistä ja luovuttamista. Henkilötietojen siirtoa ja siirtoon liittyviä termejä sekä prosesseja avataan ja käsitellään myöhemmin tässä artikkelissa.

## Tietosuojalainsäädäntö koskee sinua ja organisaatiotasi

Tietosuojalainsäädäntö ja tietosuojalaki koskee käytännössä kaikkia organisaatiota, joilla on jäseniä, asiakkaita tai työntekijöitä, koska tällöin orga-

nisaatio käsittelee henkilötietoja tai henkilöön liittyviä asioita. On yksin organisaation vastuulla huolehtia niin omalta kuin yhteistyökumppaneiden osalta henkilötietojen lainmukaisesta käsittelystä. Yhteistyökumppaneiden, toimittajien ja alihankkijoiden kohdalla kannattaa varmistaa sopimuksilla, että myös kumppanit toimivat lainmukaisesti.

Suomessa on kuitenkin edelleen hyvin yleistä, että organisaatiot eivät tunnista EU:n yleisen tietosuojasopimuksen koskevan myös heitä. Suomen Yrittäjät teetti helmikuussa 2022 tutkimuksen, jonka yhtenä aiheena käsiteltiin henkilötietoja. Tutkimuksessa kysyttiin muun muassa ”Käsitteleekö yrityksesi henkilötietoja?” ja huimat 40 % 1 049 vastaajasta vastasi, ettei käsittele tai ei ainakaan tiedä käsittelevänsä niitä.

## Digitaalinen kehitys on muokannut tietosuojavaatimuksia erilaisiksi eri maissa

Viimeisen 30 vuoden aikana digitaalinen maailma on kokenut huimaa muutosta, mikä on vaikuttanut myös tietosuojalainsäädäntöön eri maissa. Vuonna 1995 Eurooppa otti käyttöön ensimmäisen tietosuojadirektiivin, kun digitaalinen maailma oli vasta heräämässä: Internet oli tuore



ilmiö ja käytössä oli ohjelmistoja kuten Windows 95.

Tämä direktiivi tarjosi jäsenvaltioilleen mahdollisuuden soveltaa tietosuojaa eri tavoin kansallisella tasolla. Suomessa tästä seurasi Henkilötietolaki (523/1999), kun taas esimerkiksi Englannissa tulkinta oli tiukempi ja mahdollisti jopa 500 000 punnan sakot. Vaikka Pohjoismaissa, kuten Suomessa, henkilötietolain tausta-ajatus olikin kun- nianhimoinen, sakkoja ja sanktioita ei käytännössä jaettu.

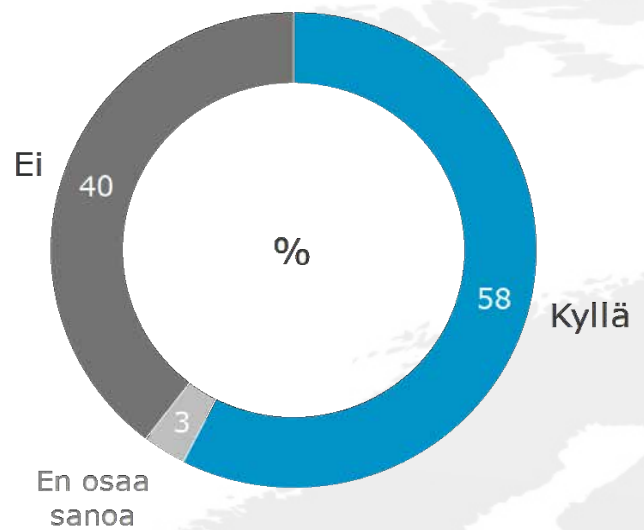
Vuoden 1995 jälkeen tietosuojan maisema on muuttunut moninaiseksi. Kanada on esimerkiksi ollut edelläkävijä henkilötietojen suojassa Pohjois-Amerikassa, ja maa on ottanut useita askelia varmistaakseen kansalaistensa tietosuojaoikeudet. Euroopassa puolestaan astui vuonna 2016 voimaan EU:n yleinen tietosuoja-asetus (GDPR), jota alettiin soveltaa kahden vuoden siirtymäajan jälkeen. Tämä asetus yhdenmukaisti tietosuojalainsäädäntöä EU:n sisällä merkittävästi. Kuten aiemmassa direktiivissä, henkilötietojen siirto Euroopan Unionin ja Euroopan talousalueen ulkopuolelle sallitaan vain, jos EU:n komissio on myöntänyt kyseiselle maalle niin sanotun vastaavuuspäätöksen.

### [Euroopan ja Yhdysvaltojen välinen tietosuojataival tähän päivään](#)

Ensimmäinen ja alkuperäinen Euroopan ja Yhdysvaltojen välinen tietosuojasopimus Safe Harbor kumottiin vuonna 2015. Sen tilalle astui vuotta myöhemmin Data Privacy Shield, joka asetti organisaatioille tietyt vaatimukset tietosuojasta. Vaikka organisaatioiden oli määrä noudattaa näitä vaatimuksia, todellisuus ei aina vastannut näitä säännöksiä. Vuonna 2020 Privacy Shield -sopimus kumottiin, sillä oli huolta siitä, että Yhdysvaltojen viranomaiset voivat saada liian vapaasti pääsyn eurooppalaisten henkilötietoihin.

Uutta sopimusta odotettiin vuodesta 2020 asti ja nyt heinäkuussa 2023 uusi EU-US Data Privacy Framework otettiin käyttöön, määritellen säännöt tietojen siirrolle. Sopimuksen piiriin kuuluvien toimijoiden, jotka ovat DPF:n hyväksyntälistalla, katsotaan tarjoavan riittävän tietosuojan. Kuitenkin uhkakuvana on mahdollisuus, että DPF voidaan kumota, mikäli Yhdysvaltojen presidentti vaihtuu tai jos NOYB, Max Schremsin johtama Euroopan digitaalisten oikeuksien keskus, haastaa sen. Molemmat skenaariot palauttaisivat tilanteen kolmen vuoden takaiseen.

NOYB kommentoi vuonna 2023: "Uusi 'Trans-Atlantic Data Privacy Framework' on käytännössä kopio vuoden 2016 Privacy Shield -sopimuksesta, joka puolestaan perustui vuoden 2000 'Safe Harbor' -sopimukseen. Koska nämä aiemmat lähestymistavat ovat jo kahdesti epäonnistuneet, uuden sopimuksen juridista pohjaa voidaan pitää kyseenalaisena. Sopimuksen olemassaolo perustui lähinnä poliittiseen logiikkaan."



Suomen Yrittäjät tutkimuksen kysymyksen "Käsitteleekö yrityksesi henkilötietoja?" vastaus.

### [Milloin ja miten siirrän tietoja ulkomaille?](#)

Tietojen siirtäminen ulkomaille saattaa tapahtua huomaamattasi. Tietosuojavaltuutetun määritelmän mukaan "siirron käsite" voi olla monitahoinen ja aiheuttaa väärinkäsityksiä. Käytännössä, kun käytät yhdysvaltalaisista pilvipalvelua, saatat jo siirtää henkilötietoja Yhdysvaltoihin. Mielenkiintoinen yksityiskohta on, että pelkkä etäyhteyden mahdollisuus Yhdysvalloista käsin katsotaan tietojen siirroksi.

Euroopan tietosuojaneuvoston (EDPB) mukaan: "Henkilötietojen siirtäminen Euroopan talousalueen (ETA) ulkopuolelle on usein tarpeellista kansainvälisissä liiketoimissa. Esimerkiksi pienet ja keskisuuret yritykset saattavat jakaa henkilötietoja liikekumppanien tai toimittajien kanssa, jotka sijaitsevat ETA:n ulkopuolella." Tämän vuoksi yhteistyö suurten toimittajien, kuten Oracle, Microsoft ja Google, kanssa voi merkitä tietojen siirtoa Yhdysvaltoihin. Keskeistä on tunnistaa ja varmistaa, ettei tietojen käsittely riko tietosuojaan liittyvää lainsäädäntöä, erityisesti kun tietoihin pääsy etäyhteydellä on mahdollista Yhdysvalloista.

### [Arkkitehtuurin ja sopimusten merkitys henkilötietojen siirtoriskien hallinnassa](#)

Arkkitehtuurikuvaukset ja järjestelmien sopimusarkistot, erityisesti tietojenkäsittelysopimukset (Data Processing Agreement - DPA), ovat korvaamattomia työkaluja henkilötietojen siirtojen hallinnassa. Tällaisilla kuvausmenetelmillä voidaan esimerkiksi havainnollistaa työnhakuprosessiin liittyviä järjestelmiä ja niiden yhteyksiä. Vaikka kuvaustapoja on useita, niiden avulla voidaan tehokkaasti ymmärtää toimittajien sijainnit ja niiden mahdolliset yhteydet muihin järjestelmiin. Jos esimerkiksi verkkosivusi on rakennettu suomalaisen toimittajan toimesta, mutta se toimii teknisesti Amazon AWS:n

pilvipalvelussa, saattavat tiedot siirtyä Yhdysvaltoihin.

Tarkastelemalla järjestelmien arkkitehtuurikuvauksia ja niiden toimittajalistaa voidaan selvittää mahdolliset riskikohdat ja henkilötietojen siirtoon liittyvät seikat. On olemassa myös automatisoituja työkaluja, jotka auttavat hahmottamaan järjestelmien ja palveluiden rakenteita, olivatpa ne sitten omalla palvelimella tai pilvessä.

Alla oleva esimerkkikuva esittää suomalaisen yrityksen verkkosivuihin liittyviä toimittajia ja palveluita. Vaikka verkkosivujen tekninen alusta olisi yhden palveluntarjoajan hallussa, muut palvelut, kuten asiakkuudenhallintajärjestelmä Hubspot, Cookiebot sekä kolmannen osapuolen palvelut, kuten Facebook ja Google, voivat olla osa verkkosivun ekosysteemiä. Arkkitehtuurikuvaukset ja analyysit siis auttavat tunnistamaan ja varmistamaan, mihin tietoja todellisuudessa siirretään ja mitä seurauksia tällä voi olla tietosuojan näkökulmasta.

### Tietojen käsittelyn tarkistuslista

Vaikka toimittajiin ja sopimukseen on tärkeää luottaa, organisaatioilla on myös oma vastuunsa. Kun tarkastellaan olemassa olevia järjestelmiä, on tärkeä tarkistaa seuraavat kohdat:

#### 1. Käsiteltävät tiedot:

- Mitä tietoja käsitellään?
- Liittyykö käsittelyyn riskejä yksilölle?
- Käsitelläänkö erityisiä henkilötietoryhmiä eli sensitiivisiä tietoja? Tällöin tietojen käsittelyssä on oltava erityisen varovainen.

#### 2. Tietojenkäsittelysopimus (DPA):

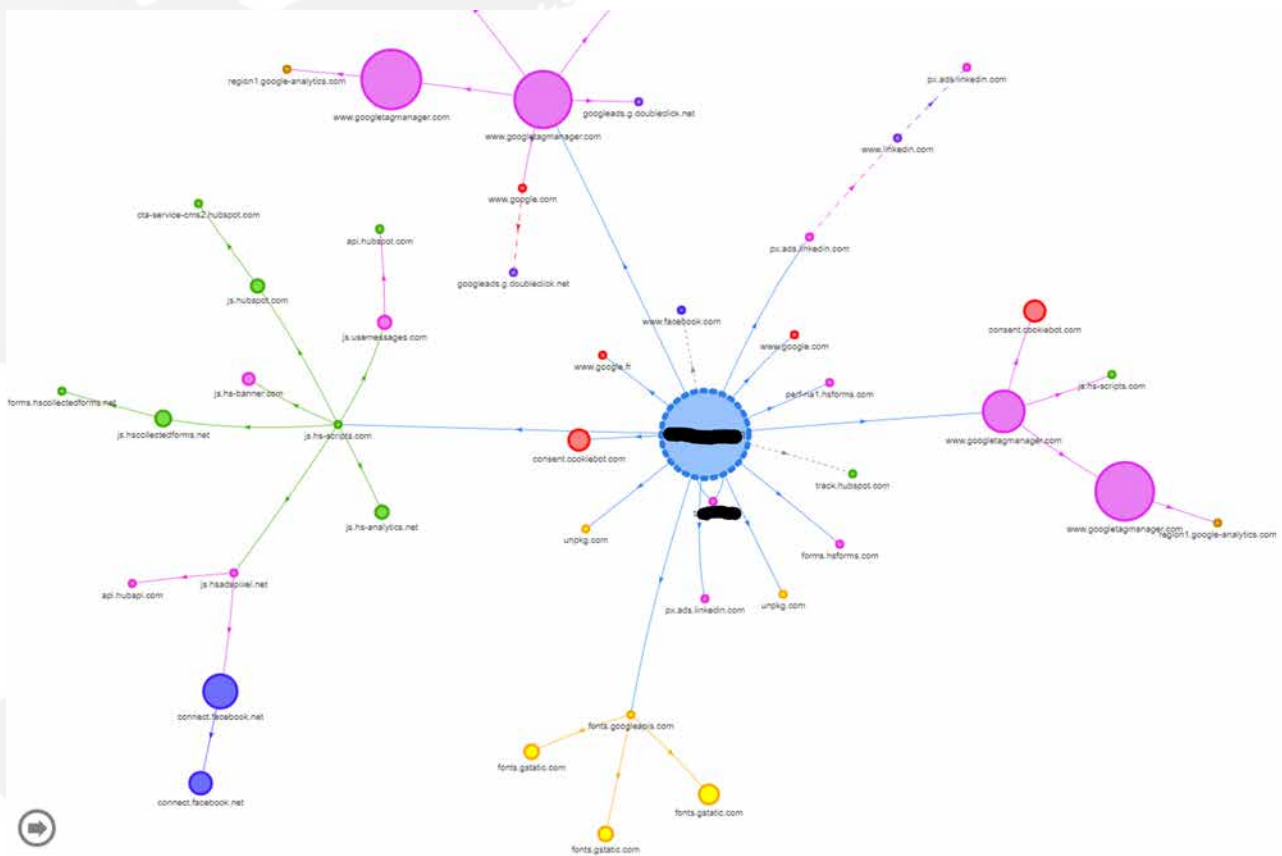
- Onko toimittajan kanssa solmittu tietojenkäsittelysopimus?

#### 3. Toimittajan sijainti:

- Missä maassa toimittaja sijaitsee?
- EU:n sisällä tietojen siirto on yleensä laillista, kunhan kohdemaan tietosuojataso on riittävä EU GDPR:n mukaisesti.

#### 4. Toimittaja EU:n ulkopuolella:

- Onko kohdemaalle myönnetty päätös tietosuojan riittävydestä? Katso lista maista!
- Jos riittävyttä koskevaa päätöstä ei ole, onko käytössä muita asianmukaisia suojatoimenpiteitä? Esimerkkejä näistä:
  - Sitovat yrityssäännöt
  - Euroopan komission hyväksymät vakiosopimuslausekkeet
  - Sertifiointimekanismit
- Erikoistapauksissa saattaa olla mahdollista käyttää poikkeuksia, kuten yksilön antamaa suostumusta.





Tämän listauksen avulla voit helposti varmistaa, että organisaatiosi tietojen käsittely noudattaa voimassa olevia tietosuojalakeja ja -säädöksiä.

### Maat, jotka ovat saaneet EU:n tunnustuksen tietosuojan riittävydestä

Euroopan komissio on tunnustanut seuraavat maat ja alueet tarjoamaan riittävää tietosuojaa GDPR:n mukaisesti syyskuussa 2023. Nämä maat ja alueet ovat saaneet hyväksynnän siitä, että ne tarjoavat riittävän tason tietosuojan Euroopan unionin standardien mukaisesti: Andorra, Argentiina, Etelä-Korea, Färsaaret, Guernsey, Iso-Britannia, Israel, Japani, Jersey, Kanada (kaupalliset organisaatiot), Mansaari, Sveitsi, Uruguay, Uusi-Seelanti ja Yhdysvallat (kaupalliset organisaatiot, jotka ovat liittyneet DPF-sopimuksen alaisuuteen).

### Vinkit tehokkaaseen tietosuojatyöhön

- Varmista toimijan asema DPF-listalla: [www.dataprivacyframework.gov/s/participant-search](https://www.dataprivacyframework.gov/s/participant-search)
- Pidä silmällä toimijoiden listaa säännöllisesti, sillä sen sisältö päivittyy ja muuttuu

- Jatka DPIA:n (Data Protection Impact Assessment) ja TIA:n (Transfer Impact Assessment) toteuttamista. Laadi suunnitelma ja harkitse varasuojatoimia mahdollisen DPF:n kumoamisen varalle.
- Merkitse DPIA:han DPF:n voimassaolon ajankohta ja määritä itsellesi aikataulu sen tarkistamiselle. Jos toimittajasi ei uusi DPF-osallistumistaan, toimintasi voi olla ristiriidassa vaatimusten kanssa.

### Tietosuojan jatkuva merkitys organisaation toiminnoissa

Tietosuojan vaatimukset edellyttävät jatkuvaa valppautta ja säännöllisiä tarkastuksia. Olipa tietosuojavastaava sisäinen tehtävä tai ulkoistettu, hänen vastuullaan on varmistaa tietosuojan noudattaminen kaikissa organisaation osa-alueissa, erityisesti hankinnoissa ja IT-toiminnoissa. DPF-sopimuksen mahdollinen kumoaminen tulevaisuudessa korostaa sopimusten ajantasaisuuden ja vaikutustenarviointien (DPIA) merkitystä.

Tehokkain tapa vähentää riskejä on integroida tietosuojanäkökulma organisaation perusprosesseihin, kuten hankintoihin. Tämä varmistaa, että mahdolliset riskit, olivatpa ne sitten toimittajaan tai alustaan liittyviä, havaitaan ajoissa.

ACTIVE

INACTIVE

Q vimeo

Advanced Search

1010data

New York, New York

Inactive

> Covered Entities (7)

Framework

EU-U.S. Data Privacy Framework

Swiss-U.S. Data Privacy Framework

?

 Questions or Complaints

**Esimerkki:** Verkkosivullasi näkyvät videot pyörivät teknisesti Vimeo-alustan kautta. Tarkastaessasi Vimeon tilaa DPF-hyväksyntälistalta, huomaat, ettei toimija ole aktiivinen jäsen. Käytön jatkamista on siis syytä punnita tarkkaan ja voi olla järkevää harkita toisen alustan käyttöönottoa.

**Huomio:** Jos et löydä toimittajaa aktiivisista jäsenistä, älä unohda tarkistaa myös ei-aktiivisten listaa.

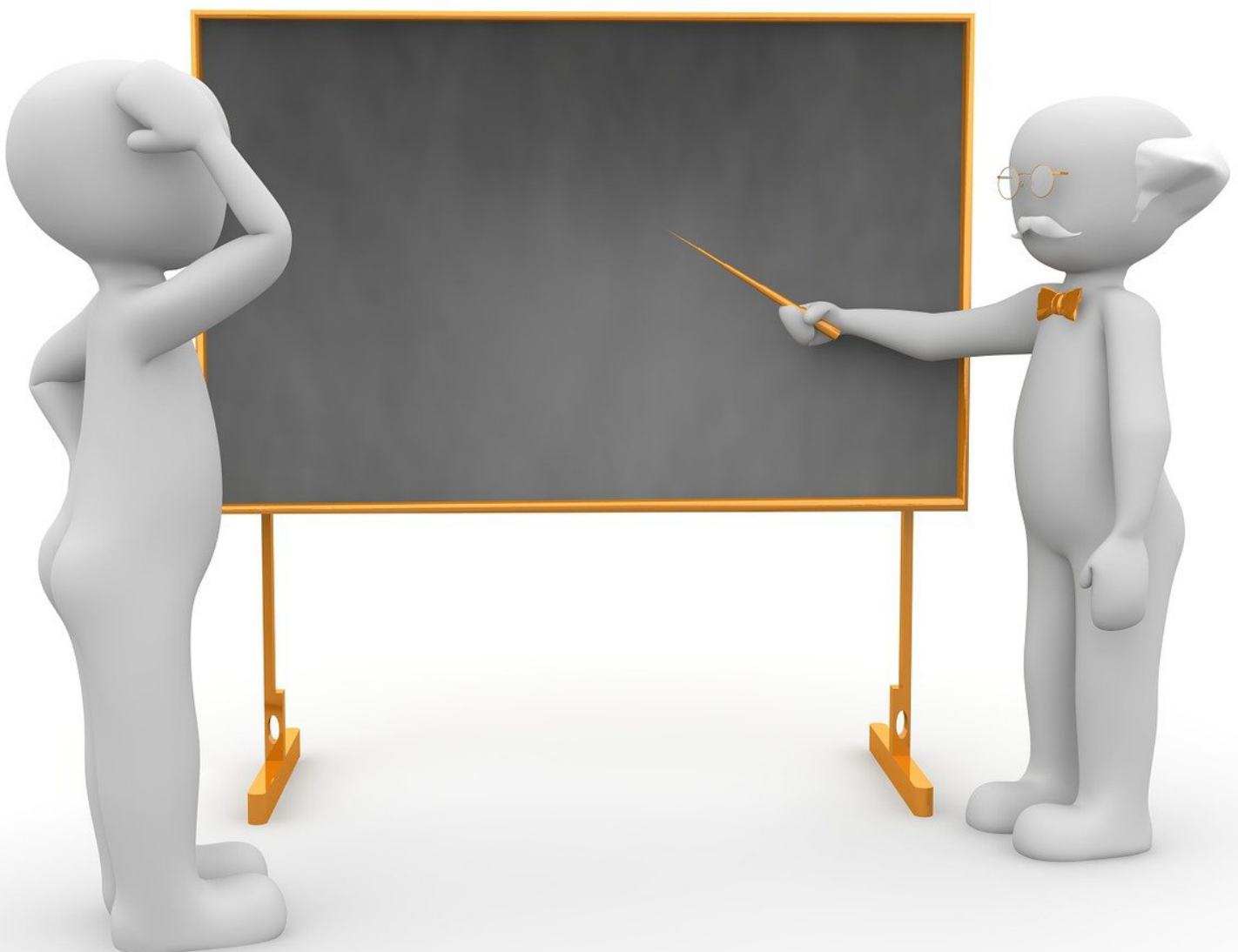
Sytyke 3/2023 • 13



## Ari Andreasson

Kirjoittaja on Tampereen kaupungin tietosuoja- ja tietokirjailija.

# Kohti tarkempia tietosuojaohjeita





Laskin tänään, että Tampereen kaupungilla on 26 erilaista dokumenttia ja ohjetta liittyen tietosujoaan ja tietoturvaan. Yleisemmin ja kategorisimmin voidaan puhua digiturvaohjeista. Perehdytyksen kannalta oleellisia ovat Tietojen ja tietojärjestelmien käyttö- ja salassapitositoumus, joka laukaistaan teknisesti kaikille uusille henkilöille, jotka saavat kaupungin Windows-tunnukset. Lisäksi sitoumus jaellaan kaikkien hyväksyttäväksi aika-ajoin, vähintään silloin, kun siihen tehdään sisällöllisiä päivityksiä johtuen esimerkiksi lainsäädännön muutoksista.

### Lähtökohtaisesti asiat ovat kohtalaisen hyvällä mallilla

Uusi työntekijä ei pääse aloittamaan Windowsin käyttöä ennen kuin hän on ”skrollannut” tekstin loppuun ja laittanut hyväksymisrastin ruutuun. Tämän jälkeen tietokone jatkaa käynnistymistään. Osalta työntekijöistä tämä sitoumus otetaan edelleen paperiversiona, mutta se on poikkeuksellista. Sähköisestä hyväksynnästä jää loki-tieto, josta voidaan jälkikäteen tarkistaa millä hetkellä ja minkä sisältöinen sitoumusteksti on hyväksytty työntekijän toimesta.

Sitoumus on osa Tampereen seudun tietoturva-politiikkaa, joka on käsitelty myös YT-ryhmässä. Sinänsä hyväksyminen ei ole vapaaehtoista vaan mikäli kysyttävää löytyy, pitää asia käydä välittömästi esihenkilön kanssa läpi. Muutenkin kaupungin suositus on se, että teksti käydään perehdytysvaiheessa ensimmäisten asioiden joukossa yhteisesti perehdytettävän kanssa läpi, jonka jälkeen vasta tekninen hyväksyntä suoritetaan.

Henkilöstön tietoturva- ja tietosujoapas on toinen keskeinen ohjeemme. Se on jaeltu tiedostona tietokoneen työpöydälle. Täten opas on käytettävissä vaikka verkkoyhteyttä ei laitteella olisi ja se on muutenkin helposti löydettävissä eikä sitä tarvitse lähteä intranetin syövereistä etsimään. Nyt syksyllä on pohdittu myös toisen turvallisuuteen liittyvän oppaan eli Turvaoppaan jakelua vastaavalla tavalla kaikille käyttäjille. Tämä on nopea ja helppo tapa saattaa ohjeet todistettavasti työntekijän saataville.

Lähtökohtaisesti asiat ovat siis ohjeistuksen osalta kohtalaisen hyvällä mallilla, mutta tosiasiasa koulutuksissa ja niiden palautteissa tulee toistuvasti esille se, että työntekijät eivät tiedä mistä ohjeet löytyvät tai he eivät ole niitä sisäistäneet. Ohjeita pidetään osin vaikeatulkintaisina tai liian ylätasoisina, joka on tunnistettu ongelma. Sama pätee verkkokoulutusmateriaaleihin, jotka on laadittu lippalakeista tunnetulla ”yksi koko sopii kaikille” -periaatteella.

### Julkisen sektorin tietosuojan palvelukeskus

Ohjeiden ajan tasalla pitäminen on myös haaste, johon tarvitaan jatkuvasti apua lakimiehiltä, toiminnan johdolta sekä tietoturva- ja tietosuoja-asiantuntijoilta niin organisaation sisältä kuin usein myös ulkopuolelta. Suomessa on monia ohjaavia virastoja, joiden linjauksia, määräyksiä tai ohjeita pitää pystyä seuraamaan, jotta omat ohjeistukset pystytään päivittämään. Toisaalta ohjaavilta virastoilta tarvittaisiin tarkempia linjauksia, jotta organisaatio- ja rekisterinpitäjätasolla pystyttäisiin anta-





maan tarkkoja soveltamisohjeita eri toimialoille, joita esimerkiksi kunnan toiminnassa on useita.

Tämä vaatii mielestäni myös eri ministeriöiden ja virastojen välillä vuoropuhelun kehittämistä ja selkeämpiä toimintatapoja mistä tietoturva- ja tietosuoja-asioihin saa ohjausta ja neuvontaa. Tällä hetkellä tilanne vaikuttaa epäselvältä. Suomeen kaivattaisiin myös jonkinlainen tietosuojan (osaa-mis)palvelukeskus, joka voisi olla julkisen sektorin ylläpitämä. Tällainen malli on ainakin Hollannissa toteutettu. Keskus voisi pitää usein esitettyjen ky-symyksen kysymys-vastaus palvelua sekä heiltä voisi tilata kouluttajia eri tilaisuuksiin. He voisivat toimia myös yhteyspisteenä eri ohjaavien virastojen ja tietosuojavaikuttetun välillä. Kuntapuolella myös Kuntaliitto kuntien etujärjestönä olisi luonnollinen osa ohjeiden jalkauttamista ja kaipaankin itse takavuosien tapaa, jolla Kuntaliitto ohjeisti eräänlaisilla yleiskirjeillä keskeisiä lakimuutoksia ja ohjeisti kuntia oikeiden toimintatapojen suuntaan.

### Palvelualuekohtaiset tietosuojaohjeet

Yksi käytännön toimenpide, jota jokaisen organisaation kannattaa pohtia, on tietosuojaohjeiden laatiminen palvelualue- ja mahdollisesti jopa toimintokohtaisesti. Jostain pitää aloittaa ja kartoittaa ensimmäisenä mitä omia ohjeita palvelualueilla mahdollisesti on ja ovatko ne ajan tasalla. Oman kokemukseni sekä sen mukaan, mitä olen kuullut myös tietosuojavaikuttavien verkostoissani, tilanne on kuitenkin se, että palvelualueet eivät juurikaan itse ole laatineet henkilötietojen käsittelyyn ja sitä kautta tietosuojaan liittyviä ohjeita, vaan niiden oletetaan tulevan jostain ylempää.

Ylemmällä tasolla ohjeet jäävät valitettavasti yleensä myös konkreettisesti ylätasoisiksi. Tunnistan tämän vaikkapa laatimani Henkilötietojen käsittelyn yleisohjeen osalta. Tästä syystä Tampereen kaupunki on alkanut valmistelevaan vastaavan tasoisia tarkempia henkilö/asiakastietojen käsittelyohjeita, kuin mitä sosiaali- ja terveystietojen

osalta lakisääteisesti oli velvoitettu toiminnan johtajan kirjallisesti antamaan. Ensimmäinen laajempi ohjeuudistus käynnistyi nyt perusopetuksen ja tietohallinnon yhteistyönä. Sisäisesti asiasta keskustuamme päädyimme ratkaisuun, että otamme ohjeen laadintaan mukaan ulkoisen konsultin, joka valikoitui olemaan Harto Pönkä. Harto on käynyt Tampereen seudun opetushenkilöstölle luennoimassa tietosuojasta ja hän on aiemminkin tuottanut kirjallista materiaalia opetushenkilöstölle suunnattuna kuten yhteistyössä Docendo-kustantamon kanssa julkaistun opetuskäyttöön sallitun maksutoman Open somekirjan. Harton kanssa pohdimme teemoja, joita ohjeessa on syytä käsitellä.

Teemoina tulevassa ohjeessa ovat tällaiset asiat:

1. Keskeinen terminologia
2. Ohjaava lainsäädäntö
3. Mikä on salassa pidettävää, mikä lähtökohtaisesti julkista
4. Rekisterinpito kaupungilla
5. Rekisteröidyn oikeudet ja niiden toteuttaminen (taustaa voi avata esim. minkäikäinen lapsi itse voi toteuttaa oikeuksia ja milloin huoltaja ja mistä huoltajuuden voi varmistaa.
6. Käyttötapaesimerkkejä tietojen luovuttamisesta sivullisille (myös poliisille)
7. Turvakielto -mikä se on? Miten sen alaisia tietoja käsitellään
8. Markkinointiviestintä (mitä huomioda mm. suostumukset)
9. SOMEn käyttö (suostumukset) ja mitä palveluita saa käyttää ja mihin (linjaukset)
10. Kuvausluvut ja kuvamateriaalin julkaisu
11. Tekoälyratkaisut ja niiden käyttö opetuksessa
12. Keskeiset tietosuojariskit opetuksessa
13. Tietosuojavaikuttamista ilmoittaminen ja jatkotoimet

Ajatuksemme on se, että ohjeessa olisi keskeiset asiat esitetty käytännön esimerkein. Ohjeen

muotona on helposti selailtava diaesitys, jossa tietosuojaan liittyvät ohjeet esitetään selvästi ja yksinkertaisesti. Mielestämme tämä on paras tapa tuoda konkretiaa käytännön arjessa pohdittaviin asioihin. Monesti itselleni on tullut koulutuksissa vastaan esimerkiksi sellainen kysymys, että ”mistä voin tarkistaa, onko henkilö oikeasti lapsen lailinen edustaja kuten huoltaja?” Muutoinkin kysymys-vastaus-tyyppinen lähestymistapa tuo vaikeaksi mielletyt tietosuoja-asiat työntekijöille ymmärrettävästi esiin.

Ohjeen osalta Tampereen kaupungilta minä sekä opetuspalveluihin perehtynyt lakimies käymme Harton tekemän osuuden läpi ja lisäämme sisäisiä asioita kuten mistä löytyy tietosuojaselosteet ja kuka niiden päivityksestä vastaa ja esimerkiksi miten ja kenelle tietosuojapoikkeamista ilmoitetaan.

Tavoiteaikataulu on saada ohje valmiiksi lokakuun aikana, mutta siihen keskeisesti vaikuttaa Opetushallituksen lupaama ohjeistus, jota on nyt odoteltu loppukeväästä lähtien. Tämä ei ole varsinainen kritiikki, mutta mikäli Opetushallitus ei pysty itsekkään olemassa olevan lainsäädännön puitteissa antamaan kovin nopeasti vastauksia esitettyihin kysymyksiin, kuten opetuksen ja hyvinvointialueiden väliseen tietojen käsittelyyn, niin ei mikään ihme, ettei tarkkoja ohjeita ole voitu myöskään yksittäisten opetuksen järjestäjien toimesta laatia.

Opetushallituksella on itsellään joitakin tietosuojaoppaita, joita käytämme myös oman ohjeemme lähteenä. Näitä oppaita kannattaa jaella opetushenkilöstölle lukuun. Tällöin toiminnan johto osaltaan täyttää osoitusvelvollisuuttaan siihen, että ohjeistuksia on toimitettu toimintaan perehdyttäväksi. Oppaat löytyvät täältä. [Tietosuojaopas](https://www.opetus.fi/tietosuojaopas) | [Opetushallitus](https://www.opetus.fi/opetushallitus) (oph.fi)

Kun Tampereen kaupunki saa oman ohjeensa opetuksen osalta valmiiksi, voidaan sitä tarjota muillekin organisaatioille hyödynnettäväksi. Tämä on hyvä alku, mutta toimialoja on monia ja jokaisen suhteen on tehtävä vastaavanlaiset juuri kyseiseen toimintaan sovellettavat ohjeet.







## Paula Miinalainen

Paula Miinalainen on moniosaaja; projektit, yritysarkkitehti, Scrum Product Owner. Hänen painopistealueenaan on järjestelmien kokonaisvaltainen laatu ja testaus sekä GDPR ja tietosuojat. Paulan yritys on Oy Arbor Vitae-Finland Ltd.

[www.arborvitae.fi](http://www.arborvitae.fi),  
[paula.miinalainen@arborvitae.fi](mailto:paula.miinalainen@arborvitae.fi)

# Yhdistyslaki ja GDPR yhdistystoiminnassa

Suomessa oli rekisteröityjä yhdistyksiä 108 146 kappaletta Patentti- ja rekisterihallituksen (PRH) rekisterissä 31.8.2023. Yhdistyslain mukaan (pykälä 11) yhdistys on lakisääteisen jäsenrekisterinsä tietosuoja-asetuksen tarkoittama rekisterinpitäjä ja rekisterinpitäjälle kuuluvista tehtävistä vastaa rekisteröidyn yhdistyksen hallitus.

Pieni laskutoimitus: Oletetaan, että keskimäärin yhdistyksen hallituksessa on puheenjohtaja ja neljä jäsentä. Jäsenrekisteritiedoista vastaavia henkilöitä on siis  $108\,146 \times 5 = 540\,730$  eli yli puoli miljoonaa hallitusvastuuta - henkilöitä vuorineuvoksista koululaisiin. Osalla yhdistyksistä on rekisteriasiat kunnossa, mutta mietittäväksi jää kuinka monelta puuttuu resurssit hoitaa luottamustehtäväänsä lain mukaan oikein - sakkoja pelkäämättä. Seuraavassa luotaan taustoja siitä, mitä lakien ja asetusten säätämiä velvoitteita yhdistyksen hallituksella on.

## Yhdistyslaki

Lähdetään liikkeelle yhdistyslain pykälästä 11. Se velvoittaa yhdistyksen pitämään jäsenluetteloa eli jäsenrekisteriä, jossa on jäsenen kotipaikka ja koko nimi. Lisäksi pykälässä määritellään, että yhdistys on jäsenluettelon EU:n yleisen tietosuoja-asetuksen (GDPR = *General Data Protection Regulation*) tarkoittaman rekisterinpitäjä ja edelleen, että GDPR:n asettamista rekisterinpitäjän velvoitteista vastaa yhdistyksen hallitus. Yhdistyksen

hallituksella on osoittamisvelvollisuus siitä, että asetuksen rekisterinpitäjälle asettamat tehtävät ovat suoritettu asetuksen mukaisesti.

On tärkeätä huomata, että laissa mainittu kotipaikka on oma käsitteensä. On olemassa kotipaikkalaki, joka on noussut viime aikoina tiedotusvälineissä esille ukrainalaisten sotapakolaisten yhteydessä. On ollut keskusteltua siitä ketkä saavat ja milloin saavat anoa Suomesta kotipaikkaa. Kotipaikka on siis aivan eri asia kuin postitoimipaikka, johon se useasti sekoitetaan. Koko nimi taas tarkoittaa, että mukaan tulee myös kaikki etunimet.

Sanotaan, että Suomi on yhdistysten luvattu maa. Yhdistyksen perustamiseen on hyvin matala kynnyks, mutta nämä muutamat edellä mainitut asiat hallituksen kuitenkin tulee tehdä. Yhdistyksen hallituksen tulee lisäksi hyväksyä yhdistyksen uudet jäsenet, ellei sen säännöissä ole toisin määrätty ja toteaa eroamiset. Jäsenrekisterissä tulee olla siis jäsenen yhdistykseen liittymispäivämäärä sekä eroamispäivämäärä.

**Suomi on yhdistysten  
luvattu maa!**





### **EU:n yleinen tietosuoja-asetus (GDPR) ja yhdistyksen säännöt**

Yhdistyksen säännöissä määritellään yhdistyksen tarkoitus ja toiminta. Ne määrittelevät, mitkä tiedot jäsenistä tarvitaan yhdistyksen toimintaa varten. GDPR vaatii, että kunkin tiedon tarpeellisuus tulee arvioida erikseen, henkilöstä ei saa kerätä turhaa tietoa, eikä tietoa voida kerätä varastoon tulevaa mahdollista tarvetta varten.

Henkilön osoitetietoja tarvitaan jäsenmaksujen hoitoa varten, jäsenpalvelujen järjestämiseen, tiedottamiseen jne. Yhdistyksen jäsen toimintaa on tapahtumat, matkat, koulutus, kilpailut, leirit jne. Näitä varten tarvitaan jäsenenestä tietoja, joihin on hyvä pyytää suostumus ilmoittautumisen yhteydessä. Samalla on hyvä kysyä, mihin muihin käyttö tarkoituksiin henkilö antaa suostumuksensa. Kukin käyttötarkoitus tulee kysyä erikseen ja ymmärrettävässä muodossa.

### **Yhteistyö keskusjärjestön kanssa**

Yhdistys voi olla keskusjärjestön jäsen, jolloin yhdistyksen henkilöjäsenet ovat yhdistyksen jäseniä eivätkä keskusjärjestön jäseniä. Yhdistyslaki velvoittaa yhdistystä pitämään jäsenluetteloa. On tavanomaista, että keskusjärjestö hoitaa jäsenyhdistysten puolesta jäsenrekisterin hallinnoinnin ja siihen liittyvät tietojenkäsittelypalvelut. Palvelu voi olla jäsenmaksujen hoito, jäsenetujen hoito, uusien

jäsenten ja jäsenyyden lopettaneiden raportointi sekä jäsenkehityksen raportointi yleensäkin. Näitä tehtäviä varten keskusjärjestö tarvitsee jäsenten yhteystietoja. Jotta keskusjärjestö voi käsitellä yhdistyksen jäsenten henkilötietoja niin käsittelystä tulee tehdä kirjallinen sopimus (GDPR: Artikla 28 kohdat 3 ja 9). Sopimuksessa on yhdistys rekisterinpitäjä (yhdistyslaki 11) ja keskusjärjestö on GDPR:n tarkoittaman tietojen käsittelijä (toimeksisaaja).

**Yhdistyksen hallituksella on osoittamisvelvollisuus siitä, että asetuksen rekisterinpitäjälle asettamat tehtävät ovat suoritettu asetuksen mukaisesti.**





### Jäsenten välinen yhteydenpito

Yhdistyksen toiminnan toteutukseen voi kuulua jäsenten keskinäinen yhteydenpito. Tämä tulee ilmetä yhdistyksen säännöistä, jotta henkilöiden tietoja voidaan antaa yhdistyksen puolelta jäsenten keskinäiseen käyttöön ja jäsentietojen antamisen on oltava yhteensopivaa tiedoille määritellyn käyttötarkoituksen kanssa. Jäsenille on annettava etukäteen tieto siitä, että tietoja annetaan muille jäsenille. Tämä on tärkeää myös siksi, että henkilöllä saattaa olla turvakielto tai hän ei muutoin halua tietojaan jaettavan muille.

Yhdistystoiminnassa syntyy yhteistyöryhmiä, projekteja, harrasteryhmiä ym., joissa on tarpeen ja mielekästä pitää ryhmää koskevaa yhteistä yhteystietopankkia. Tässä tapauksessa on helpointa kysyä tähän suostumus ryhmään liittymisen yhteydessä.

**Tietosuojaseloste  
on myös oiva  
markkinointiväline!**

### Rekisteröidyn oikeudet.

GDPR määrää, että henkilörekisterinpitäjällä on todistettava eli osoittamisvelvollisuus siitä, miten se rekisterinpitäjänä toteuttaa asetuksen vaatimia. Keskeinen vaade on vaalia rekisteröidyn oikeuksia asetuksen vaatimalla tavalla. Kertauksena luettelo GDPR:n mukaisista rekisteröidyn oikeuksista.

1. Oikeus tarkastaa omat tietonsa.
2. Oikeus pyytää korjausta tietoihinsa.
3. Oikeus vaatia tietojensa poistamista ts. vaatimus tulla unohdetuksi.
4. Oikeus siirtää tiedot johonkin toiseen järjestelmään, silloin kun tiedot ovat rekisteröidyn itsensä toimittamia ja tietojen käsittely perustuu suostumukseen tai sopimukseen.
5. Oikeus kieltää suoramarkkinointi tai rajoittaa kiistanalaisten tietojen käsittelyä, kunnes asia saadaan ratkaistua.
6. Oikeus vastustaa henkilötietojensa käsittelyä, jos on sitä mieltä, että tietoja on käsitelty lain vastaisesti tai rekisterinpitäjällä ei ole oikeutta käsitellä niitä.
7. Oikeus tehdä valitus henkilötietojensa käsittelystä valvontaviranomaiselle.
- 8.



## Tietosuojaseloste

Rekisterinpitäjällä on velvollisuus antaa rekisteröidylle tietoja hänen henkilötietojensa käsittelystä. Tämän informaation tulee olla helposti saatavilla, helposti ymmärrettävää, läpinäkyvää ja tiivistä. On tärkeää ilmaista käsittelyn tarkoitus selkeästi, sillä tietoja voidaan käyttää vain tässä määriteltuihin tarkoituksiin.

Kannattaa tutustua taulukkoon: [Informointivelvoitteen edellyttämät tiedot](#), joka on Tietosuojavaltuutetun sivuilta kohdasta <https://tietosuoja.fi/rekisteroidyn-informointi>.

Tietosuojaselosteen pohjaa on hyvä käyttää vaiheittain siten, että täyttää siitä ensin ne kohdat, jotka ovat tiedossa ja etenee sitä mukaan, kun asiat valmistuvat tai selkeytyvät. Silloin se ohjaa työn etenemistä.

Kun suunnittelet uutta henkilörekisteriä, niin pohja toimii heti suunnittelun alusta lähtien muistilistana asioista, jotka tulee huomioida.

Tietosuojaseloste on myös oiva markkinointiväline! Sen avulla voi kertoa jäsenille ja myös suurelle yleisölle, miten juuri tässä yhdistyksessä huolehditaan jäsenen/yhteistyökumppanin henkilötiedoista, miten heitä arvostetaan ja kunnioitetaan jne. Tämä on vihje tehdä hyvästä henkilötietojen hallinnosta osa yhdistyksen julkisuuskuva. Tähän kannattaa paneutua ja tehdä rekisteröidyn informoinnista juuri oman yhdistyksen näköinen.

## Prosessikuvaukset eli rekisterien käsittelykuvaukset

Tee kustakin rekisteristä henkilötietojen käsittelyn kuvaus! Kuvauksella ei ole määrämuotoa. Se voi olla hyvinkin yksinkertainen, mutta se pitää olla olemassa. Kuvaa: kuka tekee, mitä tekee, miksi tekee ja missä tekee. Kuvaa lisäksi millaiset oikeudet kullakin tekijällä on henkilötietojen käsittelyyn. Saako katsoa tiettyä tehtävää varten, saako muuttaa, poistaa tietoja ja millä perusteella.

Henkilötiedot on hävitettävä heti silloin, kun käsittelyn perustetta ei enää ole eivätkä tiedot ole toiminnan kannalta enää tarpeellisia. Jäsenen erotessa tiedot on hävitettävä sen jälkeen, kun jäsenyysasioiden hoito ei enää edellytä tietojen säilyttämistä. On kuitenkin huomioitava, että tietojen säilyttämistä saatetaan edellyttää laissa määrätyn ajan kuten kirjanpitoa laissa.

Tarkista vielä, että prosessikuvauksessa on mukana kaikki rekisteröidyn oikeudet. Tarkista, että kaikki oikeudet voidaan toteuttaa. Käy nämä läpi myös atk-palvelutoimittajan kanssa. Heillä on mitä toden näköisemmin jo ratkaisut näiden oikeuksien toteuttamiseen.

Monissa organisaatioissa on jo olemassa prosessikuvausdokumentit. Tällöin riittää, kun tarkistaa ne ja tekee tarvittavat muutokset. Tarkastelun yhteydessä saattaa löytyä päällekkäisyyksiä ja monimutkaisia käytäntöjä. Tässä yhteydessä on hyvä tilanne sujuvoittaa toimintoja.





## Risto Nevalainen (TkL)

Risto on kokenut IT-järjestelmien laadun ja mitaamisen asiantuntija. Hän oli Tieke:n toiminnanjohtaja 1989-1995. Vuosina 1979-1980 hän oli Valtioneuvoston kansliassa Teknologiakomitean pääsihteerinä. Standardoinnissa hän on ollut mukana reilut 30 vuotta.

Nevalainen on ollut mukana ydinturvallisuuden kansallisessa tutkimusohjelmassa SAFIR, ja on ollut luomassa Nuclear SPICE mallia digitaalisten järjestelmien kelpoistamiseen ja toimittajien arviointiin.

# Tietojärjestelmien sääntelyn rajat ja reunaehdot

## Hieman historiaa

Kehittyneissä yhteiskunnissa on sääntelyä, kun jokin asia aiheuttaa uhkaa, väärinkäyttöä tai kärsimystä. Hyviä esimerkkejä ovat ydinvoima ja lääkkeiden luvitus. Sääntelyä on myös pakon edessä, kun torjutaan rikollisuutta ja yhteiskunnan perusarvojen loukkauksia. Sääntelyä on varsin monenlaista, rajoittavasta sallivaan ja edistävään.

Lienee hyvä, jos ja kun sääntelyä ei tarvita lainkaan. Liberaalin talousjärjestelmän ihannetilassa kukin toimija hoitaisi osansa, ja jo riskienhallinnan takia ehkäisisi epäonnistumiset ja väärinkäytökset. Näin ei tietysti ole oikeasti. Sääntelyä voidaan tarvita myös, kun jonkin asian tasoa halutaan nostaa vaatimalla sitä enemmän. Yksityisyyden suoja on tästä hyvä esimerkki, sitä tarvitaan tietoyhteiskunnassa enemmän kuin ennen.

Tarvitaanko tietojärjestelmien sääntelyä? Tässä artikkelissa pohdimme asiaa enimmäkseen yhteiskunnan muuttuvien tarpeiden eli tulevaisuuden näkökulmasta. Sääntelyähän on varsin vähän tällä hetkellä. On totuttu valvomaan ja reguloimaan yksittäisiä laitteita, etteivät ne aiheuttaisi vaaraa käyttäjälleen. Digitaalisissa laitteissa ja niiden muodostamissa järjestelmissä on tietysti ohjelmistoja, mutta ne on käsitelty siinä sivussa.

Kun rakennusten tasoa haluttiin nostaa ja vähentää onnettomuuksia, syntyi rakennusvalvonta ja rakennuslupamenettely. Se on hyvä esimerkki win-win asetelmasta, jossa sekä yhteiskunta että kansalainen hyötyy – kun homma toimii niin kuin pitäisi. Rakennuslupa on nykyään sisällytetty myös yhteiskunnan uusia tavoitteita, kuten energian säästö ja asumisen terveys.

Autokatsastus syntyi, kun kulkuneuvojen rikoutumiset aiheuttivat onnettomuuksia ja kuolemia. Syntyi varsin keskitetty valvontajärjestelmä tyyppihyväksyntöineen ja vuositarkastuksineen.

Nyttemmin sitä on kevennetty sallivammaksi, kun autotkin ovat parantuneet.

Sähkölaitteille kehitettiin CE-merkintä. Sillä haluttiin parantaa käyttöturvallisuutta, esim. estää sähköiskuja. Sähkölaitteet ovat muuttuneet digitaalisiksi, eli on yksi osa ohjelmistojen tarkastusta. Terveystieteiden standardeissa on sovittu, että ohjelmisto voi olla ”medical device” eli se voidaan tarkastaa ja sille voidaan myöntää sertifikaatti.

Pisimmällä sääntely lienee ydinvoima-alalla. Kaikki lähtee turvallisuudesta eli lähinnä onnettomuuksien ehkäisystä. Käytämme tästä termiä käyttöturvallisuus. Olennaista on järjestelmien luotettavuus ja kyky estää tai rajata erilaisia onnettomuuksia. Turvallisuuden eri vaatimustasoille on tiukka luokitus asianmukaisine vaatimuksineen, ohjeistoineen ja standardeineen. Hyvin on toiminut, täten on saatu aikaan luottamusta ydinvoimaan kansalaisten keskuudessa.

Tietojärjestelmät olivat alkuun tukitoiminnon asemassa. Rutiinimaista tiedonkäsittelyä tehostettiin teknologian antaessa varsin tiukat rajat. Vähi-tellen atk:sta tuli nykyistä IT:tä, digitalisaatiota. Se on nykyisin liiketoiminnan ydintä ja keskeinen osa sen uudistamista kaikilla toimialoilla. Tehokkuusvaatimuskin on oleellinen, kun IT on kilpailutekijä. Sen johtaminen on osa liiketoiminnan johtamista. IT on tullut monimutkaisemmaksi, eikä mikään osapuoli hallitse tai tee kaikkea.

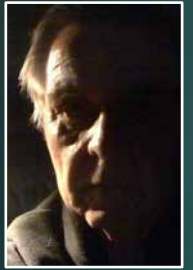
Yhteiskunnan vaatimukset ovat lisääntyneet ja muuttuneet. Sääntelyä tuli ensin aloille, joissa oli selkeä turvallisuusuhka. Turvallisuus voi olla sekä käyttökäsitteistä tuoteturvallisuutta (*safety*) että uudenlaista tietoturvaa (*data security*) ja verkkoturvaa (*cybersecurity*). Nyt vaatimuksena on lisäksi ilmastonmuutoksesta johtuvaa säästämistä Green IT nimissä ja monenlaista uudenlaisten riskien torjuntaa, resilienssiä. Alkuaikojen tyypillisiä säädeltyjä toimialoja ovat olleet terveydenhoito, energian



## Heikki Uusitalo (LuK)

Heikki on nähnyt tietojärjestelmien kehittymisen reikäkorttien aikakaudelta nykyiseen netti-  
aikauteen useiden sovellusalueiden kautta useissa  
eri tehtävissä. Pankkisektorilta kokemusta on  
maksuliikennejärjestelmistä, asiakaspäätepalve-  
luista, rahamarkkina-, valuuttakauppa- ja rahoitusinstrumenttien sijoitusjärjestelmistä.

Elintarvikesektorille hän on kehittänyt omavalvontajärjestelmiä. Hän on lisäksi testannut terveydenhuollon potilasmonitorijärjestelmiä.



tuotanto, maksuliikenne, poliisitoimi, hätäkeskukset ja rajojen ulkovalvonta. Näilläkin aloilla sääntely on muuttumassa, kun IT on tullut niiden keskeiseksi osaksi.

### Onko sääntely tarpeen?

Nykyhetkessä voimme nähdä sääntelylle uudenlaisia tarpeita:

- Kasvava riippuvuus IT-järjestelmistä voi heikentää yhteiskunnan turvallisuutta ja huoltovarmuutta. Näin ei välttämättä tapahdu, mutta hereillä on syytä olla. Esimerkiksi energian jakeluverkko voi vahingoittua tahallisesti, suuronnettomuuden tai poikkeavan säätötilan johdosta. Maksuliikenteen riippuvuus mobiili-verkoista voi sekoittaa kaupankäyntiä. Etähoitot voivat heikentää vanhusten kokemaa turvallisuutta, kun kotona käymistä vähennetään. Pilvipalvelu voi hukata tietoja ja menettää saavutettavuuttaan.
- Kasvava rikollisuus ja haitanteko. Verkkorikollisuudesta ennustetaan jopa uutta toimialaa (FBI). Järkyttävä esimerkki saatiin Vastaamon tietomurrosta. Yrityksen liiketoiminta kärsi johtaen lopulta konkurssiin. Yrityksen asiakkaat kärsivät ja tulevat edelleen kärsimään. Yhteiskuntakin kärsi, pelkästään välittömät ja välilliset kustannukset ovat mittavat. Henkisten kärsimysten määrä on lähes mittaamaton.
- Alustatalouden isot toimijat pyrkivät monopolin ja rajoittamaan kilpailua. Se voi olla kansallisen tai EU-lainsäädännön vastaista, mutta ainakin kehitystyötä rajoittavaa ja kansalaisen kannalta näkymätöntä.
- Tekoäly on nyt hypen huipulla, ja voi johtaa huonoon tilaan, jos ja kun sille annetaan päätösvaltaa. Esimerkiksi erilaisista avustuksista

päätäminen, veron määrääminen, linnatuomion antaminen ja lainan myöntäminen sopii tekoälylle mainiosti. Jossain vaiheessa koputellaan sallittavan ja hyväksyttävän rajoja.

Yhteiskunnassa ollaan kohtalaisen hyvin tietoisia tietojärjestelmien sääntelyn tilanteesta. Mutta monenlaisia hidastavia voimia on. Kansalaisetkin ovat jakaantuneet aikaisiin omaksujiin, seurailijoihin ja IT:n ulkopuolella pysyviin. Varsinkin kansalaisten käyttöön tarkoitetuissa IT-järjestelmissä (eli IT-palveluissa) on vaikea päästä yhtenäisratkaisuun. Sen on vaikkapa SOTE-järjestelmien kirjavuus jo osoittanut.

Sääntelystä voi olla myös haittaa. Se voi rajoittaa innovointia lukitsemalla nykytilan. Sääntely voi olla myös verraten kallista, joten vain muodon vuoksi sitä ei kannata tehdä. Hintaa kertyy etenkin raskaassa sertifiointissa. Pitää olla osapuolten yhteinen tahtotila, mikä on järkevää.

### Millaista sääntely voisi olla?

Tässä artikkelissa on varsin laaja näkemys sääntelystä ja sen tarpeesta. Ehkä kaikkea jo toimivaa käytäntöä ei edes koeta sääntelyksi, siihen on totuttu ja se hyväksytään. Mielessämme on seuraavanlainen asteikko ja eräänlainen tasoajattelu sääntelyn eri muodoista:

- ”nollataso”, eli sääntelyä ei ole lainkaan eikä siihen ole tarvetta. Suurin osa IT-alan asioista on tätä, ei sääntelyä.
- Omavalvonta ja itsesääntely, eli kukin toimija tekee sääntelyä oman näkemyksensä mukaan. Apuna voi olla esimerkiksi oman toimialan ohjeistoja, kuten maksuliikenteen valvonta ja rikollisen rahan pois siivoaminen. Monissa yrityksissä tällainen toiminta on yhdistetty



laatujohtamisen kanssa.

- Toimialakohtainen viranomaissääntely, esimerkiksi vaatimus terveydenhuollon tietojen siirrettävyydestä järjestelmien välillä. Tietoturvaa voidaan vaatia esimerkiksi GDPR-direktiivin mukaisesti.
- Valtakunnallinen yhtenäisratkaisu, useimmiten valtiovallan avulla tai kansainvälisin sopimuksin. Kaikki hyväksyvät, että sähköä siirretään kansallisesti ja yli rajojen samalla tavalla. Sääntely siis hoituu melko lailla itseksensä. Ei se kuitenkaan ongelmatonta ole, kuten olemme huomanneet sähköpörssin toimimattomuuden osalta. Monopolikin vaatii siis valvontaa loppujen lopuksi...
- Sertifiointi, eli järjestelmälle annettava (laatu)todistus. Siinä osapuolet vakuuttavat riippumattoman tarkastuksen perusteella, että järjestelmä täyttää nimetyt vaatimukset, esimerkiksi haluttu luotettavuustaso. Saavutettu SIL-luokka on esimerkki laajalti hyväksytystä sertifikaatista, ja sen variaatioita on käytössä esimerkiksi autojen IT-järjestelmissä.
- Käytön ennakkoluvitus, eli järjestelmän käyttöönotto vaatii (yleensä viranomaisen) ennakoluvan. Kaikki tiedämme tämän ydinvoimaloista. Yleensä ennakkoluvitus huomioidaan pitkän kehitysvaihetta vaatimuksista alkaen, jotta ei tulisi yllätystä ja käyttö lupaa ei saataisikaan. Luvitus sisältää myös mahdollisuuden kieltää järjestelmän käyttö.

Luokituksemme on osapuilleen (heikko) järjestysasteikko. Kaikkein vahvin sääntely eli ennakkoluvitus sisältää kaikki muutkin sääntelyn muodot. Kevyempi sääntely on yleensä varsin konsultoivaa ja win-win tilanteeseen perustuvaa. Silloin kaikki osapuolet ovat siihen hyvin sitoutuneita. Tarkastuspainotteinen ja reguloiva sääntely voi olla erillistä itse kehitystyöstä. Puhutaan riippumattomasta V&V-toiminnasta, esimerkiksi hyväksytyn laboratorion tekemistä erillistesteistä.

Varmaankin suurin osa sääntelyn tulevaisuudesta on omavalvonnan tyyppistä. Se perustuu palveluntuottajan omaan näkemykseen ja suunnitelmaan. Laatujohtajien auditoinnissa olemme jo tottuneet tämännäköiseen toimintaan. Johdon asema on keskeinen. Sen tulee vaatia ja valvoa omavalvonnan toimivuutta ja tehokkuutta. Aika vähällä voi saada paljon hyötyä toiminnan tason ja riskittömyyden nostona. Vähitellen omavalvonnasta tulee IT:n johtamiskäytännön (*IT Governance*) vakio-osa.

Kun järjestelmän kehittämistyössä on käytössä vankka linkkaarimalli, sen osana on jo monenlaista läpikäyntiä, katselmointia, testausta ja auditointia. Skaalautuvan ketteryuden malleissa tälle on paikkansa, ja on usein melko riittävää sääntelyn kannalta. Riippumattomuus on monien toimialojen lisävaatimus, ihan aina ei voi luottaa vain palveluntuottajan sanaan ja raportteihin.



### Esimerkkinä esteettömyys

Maankäyttö ja rakennuslaki määrää esteettömyydestä. Liikkumis- ja toimimiseisillä henkilöillä tarkoitetaan henkilöitä, joiden kyky liikkua tai toimia itsenäisesti on korkean iän, sairauden, vamman tai muun syyn takia heikentynyt väliaikaisesti tai pysyvästi. Liikkumiseisillä henkilöillä ovat mm. pyörätuolin ja pyörillä varustetun kävelytelineen tai muun liikkumisen apuvälineen käyttäjät sekä henkilöt, joilla on rajoitteita käsien käytämisessä. Liikkumisen apuväline voi olla käsi-käyttöinen tai sähkökäyttöinen. Toimimiseisillä ovat mm. henkilöt, joilla on näkemisen, kuulemisen, muistamisen, ymmärtämisen tai hahmottamisen haasteita.

Miten tietojärjestelmien pitäisi suhtautua tähän? Esteettömyysasetus perustelumuiotioineen ja sen ohje ovat osa vammaisten henkilöiden oikeuksista tehdyn YK:n yleissopimuksen kansallista toteutusta. Vammaisyleissopimus ja sen valinnainen pöytäkirja tulivat Suomessa voimaan vuonna 2016. Toistaiseksi on pärjätty kohtalaisen hyvin erilaisilla IT:n korvaavilla ratkaisuilla, kuten virkailijapalvelut, puhelinpalvelu, läheisten antama apu ja uudet tekniset ratkaisut.

### Sääntelyn järki

Jotta sääntely on hyväksyttävää, sen pitää perustua laajalti hyväksyttyyn ja ammatillisesti kunnianhimoiseen normistoon (referenssi). Referenssi voi olla monenlaista edellä kuvatun sääntelyn tason mukaan. Itsesääntelyn normi voi olla itse tehty tai usein toimialalla vakiintunut tapa.

Rakennukset ja niiden rakentaminen perustuu paljolti standardeihin: paljonko katto kestää lumi-kuormaa, alalla on tästä pitkät kokemuspohjaiset perinteet. Portaissa nousemiseen vaikuttaa kaksi tekijää, nouseminen ja eteneminen. Jos niiden suhde ei ole oikea, niin portaat ovat liian jyrkät tai loivat, eikä liikkuminen ole miellyttävää. Portaat ovat osa rakennuksen käyttöliittymää. Porraskaitteiden väliin ei saa mahtua päätä, muuten joku ve-



## Jotta sääntely on hyväksyttävää, sen pitää perustua laajalti hyväksytyyn ja ammatillisesti kunnianhimoiseen normistoon

kara keksii sen ja joutuu vaaraan.

Yhteiskunnalle tärkeissä IT-järjestelmissä referenssin on syytä olla vahva. Historiassamme referenssi on perustunut yleensä käyttöturvallisuuden (*safety*), tietoturvaan (*data security*) tai verkkoturvaan (*cybersecurity*). Kuten huomaamme, edes terminologia ei ole kovin vakiintunutta. Esi-isämme eivät tällaista asiaa ehkä osanneet kaivata, se on tullut tarpeeseen vasta digitalisaation ja tietoyhteiskunnan kehittymisen mukana. Viime vuosina IT-järjestelmän yleiseksi vaatimukseksi on lisätty yksityisyyden suoja (*data privacy*).

Kansainvälinen standardi olisi paras referenssi, kun se on huolella tehty ja laajasti hyväksytty. Jokin estää kuitenkin standardien laajamittaisen käytön, ehkä siksi kun ne ovat väkisin melko yleisellä tasolla. Referenssin olisi hyvä olla tarkka ja helppokäyttöinen, mutta todellisuus ei sitä ole. Se on monimutkainen, tulkinnanvarainen ja ristiriitainen. Muutamalta osin standardit toimivat, esimerkiksi ISO9001. Systeemyön viralliset ”de jure” standardit ovat usein menetelmälähtöisiä suosituksia, joita ei ole tehtykään normiksi vaan pikemmin best practice-tyyppiseksi ohjeeksi. Tekniset standardit ovat usein ”de facto”-tyyppisiä, esimerkiksi jonkin konsortion tekemiä. Esimerkiksi käytettävyyden on hankala mitattava, kuten myös tiedon laatu. Tuoteturvallisuuden mittaamisessa ollaan onneksi pidemmällä, samoin tietoturvan tason tarkastamisessa.

Järkeä tarvitaan myös tekijöiden osaamisessa.

Verrokkina voisi mielestämme toimia journalistin ohje. Journalistin ohjeiden noudattamista valvoo kustantajien ja muiden sidosryhmien muodostama Julkisen sanan neuvosto, eli kyse on itsesääntelystä. Ohjeen ensimmäinen kohta on: ”*Journalisti on vastuussa ennen kaikkea lukijoilleen, kuulijoilleen ja katselijoilleen. Heillä on oikeus saada tietää, mitä yhteiskunnassa tapahtuu.*”. IT-alallakin on paljon julkaisemista ja sisällön tuottamista!

IT-ammattilaisten eettisiä ohjeita on laadittu vuosien varrella, mutta ovat painuneet unholaan. ISO/IEC 7000 on standardimuotoinen esitys IT-alan etiikasta, siitä voi aloittaa. Eettisiin ohjeisiin sitoutuminen parantaa ammattilaisen itseohjausta, kun hän noudattaa yleviä periaatteita ja uskaltaa tuoda myös havaitsemiaan ongelmia yhteiseen keskusteluun.

Esimerkkinä hyvästä IT-ammattilaisuudesta on ISTQB-yhteisön myöntämä pätevyyssertifikaatti. Siinä on monta tasoa. Ei kuulosta hassummalta, jos yhteiskunnan kriittiset IT-järjestelmät hyväksyisi lopuksi tunnustetun ammattipätevyyden omaava henkilö. Projektinhallinnan osalta on voimassa IPMA:n normistoon perustuva pätevyyssertifikaatti, ja se nosti ammatin arvostusta.

Sääntelyn järkeen voisi lisätä kustannustason. On käynnissä lukuisia hyvin kalliita järjestelmähankkeita, ja entistä huonompaan suuntaan ollaan menossa. Kaikkien etua tavoittelevassa ennakoivassa sääntelyssä voitaisiin valvoa myös hallintamenettelyjä ja päätöksentekoa kaikkien osapuolten eduksi. Ongelmana on, että yhteistä referenssiä hyväksyttävälle kustannustasolle ei ole, eivätkä tilaajat sen kummemmin kuin toimittajatkaan tiedä oman toimintansa tehokkuutta eikä tuottavuutta. Tässä asiassa on siis merkittävän kehitystyön ja osapuolten sitouttamisen haaste.

IT-ala on sittenkin kovin nuori. Vakiintuneimilla toimialoilla on luokiteltuja pätevyysvaatimuksia, esimerkiksi hitsauksessa, autonkuljetuksessa ja terveydenhoidossa.

Yhteiskunnassa on yhä enemmän haasteita, jotka koskettavat IT-järjestelmiä. Ovathan ne tietoyhteiskunnan kivijalka. Pitäisi noudattaa hyviä johtamistapoja (*governance*), olla valmiina uudenlaisiin kriiseihin (*resilienssi*) ja puolustaa kestävyyttä (*sustainability*). Sellaista yksittäistä toimijaa ei olekaan, joka pystyisi vastaamaan kaikkiin haasteisiin yksin. Vaaditaan siis laaja-alaista yhteistyötä ja ammatillisesti vakavaa pohdintaa uusien sääntelytarpeiden edessä.

Uutena ja hankalana sääntelyn tarpeena on tekoäly. Sen sääntelyn normistoa voisi kait sitten kutsua tekojärjeksi? EU on tässä asiassa liikkeellä likimain ajoissa. Tekoälyä sisältävien järjestelmien ja tuotteiden sääntely hakee muotoaan vielä vuosikausia. Yksi sääntelyn työmaista on tekoälyn etiikka. Meidän on syytä keskustella myös Sytykkeen piirissä, millaista sääntely voisi olla. Toivottavasti saadaan järjellistä lainsäädäntöä kehitystyön pohjaksi.





## Tuula Seppo (KTM, YTM)

Kirjoittaja, toimii johtavana asiantuntijana Digi- ja väestötietovirastossa ja on tietoturvallisuus- jaoston sihteerinä ollut tekemässä hankintasuositusta sekä aikaisempia suosituksia Julkrista, turvallisuusluokitelluista asiakirjoista ja salassa pidettävistä asiakirjoista. Hän on aktiivinen kouluttaja tiedonhallinnan, tietosuojan ja hallinnollisen tietoturvan osa-alueilla. Hänellä on laaja kokemus kuntien tietohallinnosta ja toiminut mm. tietohallintopäällikkönä ja tietosuojavastaavana.

# Tietoturvallisuus- vaatimukset hankinnoissa

Tietoturvallisuusvaatimusten määrittely on yksi keskeisimmistä vaiheista hankinnan turvallisuuden varmistamisessa. Tietoturvallisuusvaatimukset tulee määritellä riskilähtöisesti riittävän tiukoiksi välttämällä tarpeettoman korkeita vaatimuksia ja niihin liittyviä ylimääräisiä kustannuksia. Tiedonhallintalautakunta on julkaissut julkishallinnon käyttöön suosituksen koskien hankintojen tietoturvallisuusvaatimuksia. Suositus ei sisällä yleisiä hankintoihin liittyviä vaatimuksia, vaan näkökulma on tietoturvallisuus ja miten se tulee huomioida hankinnan kohteen vaatimuksissa ja miten tietoturvallisuuden säilymisestä huolehditaan koko hankinnan elinkaaren ajan.

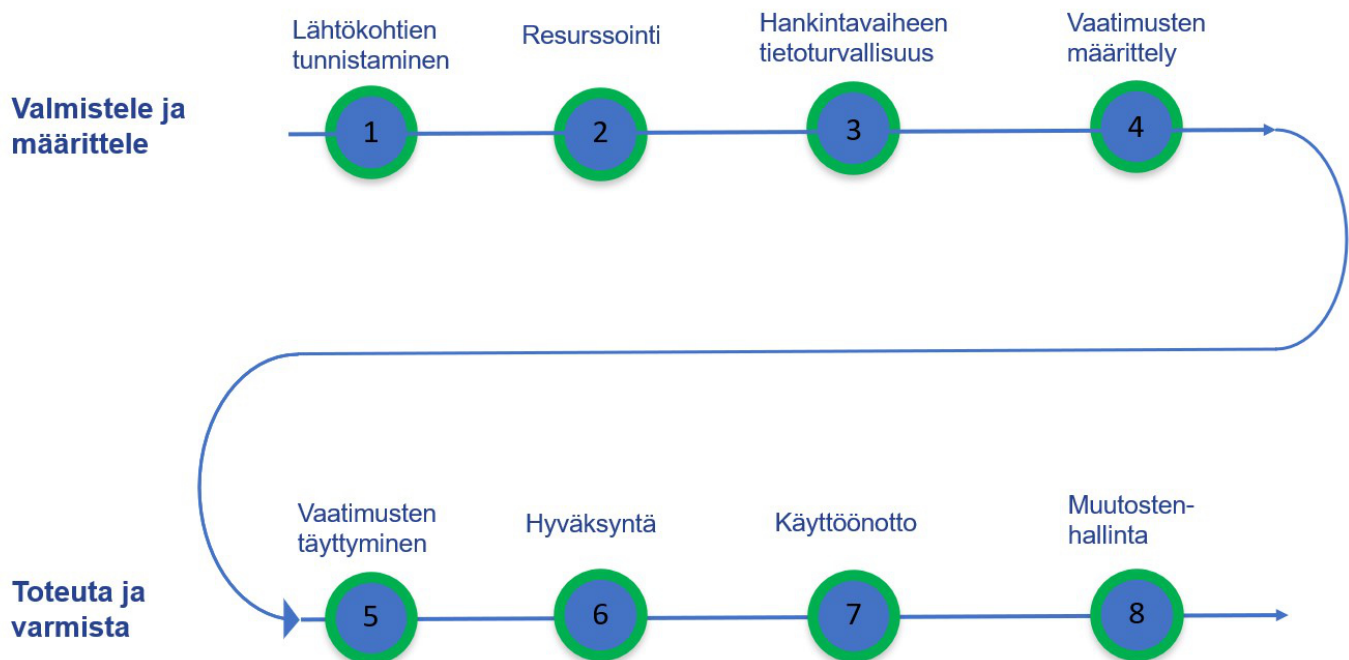
Suosituksen sisältyvien liitteiden avulla on mahdollista muodostaa tietoturvallisuusvaatimukset toimittajille, esimerkiksi osana hankintadokumentaatiota. Suositus sisältää pääsopimukseen kirjattavat asiat sekä liitteinä suppeat ja laajat tietoturvallisuusvaatimukset, hankintaehtotyökalun yksityiskohtaisempien tietoturvallisuusvaatimusten määrittelyyn ja erillisenä VAHTI-toiminnassa julkaistut tietosuojaliitteet.

## Kenelle suositus on tarkoitettu

Suositus on tarkoitettu viranomaisille ja erityisesti hankintayksiköille tietojärjestelmien ja soveltuvin osin muiden palveluiden hankintoihin liittyvien tietoturvallisuusvaatimusten määrittelyyn sekä niiden täyttymisen varmistamiseen. Myös toimittajia suositellaan perehtymään suositukseen.

## Tietoturvallisuuden varmistamisen prosessi

Suosituksessa on kuvattu tietoturvallisuuden varmistamisen prosessi. Se sisältää ne vaiheet, joiden avulla voi suunnitella ja varmistaa hankinnan tietoturvallisuuden sekä huolehtia, että tietoturvallisuus säilyy koko hankinnan elinkaaren ajan. Valmistelu- ja määrittelyvaiheessa korostuu lähtökohtien tunnistaminen, tarvittavien osaamisten ja resurssien varaaminen sekä vaatimusten määrittely. Toteutus- ja varmistusvaiheessa tulee huolehtia vaatimusten täyttymisestä, johdon hyväksynnästä sekä käyttöönotosta. Käyttöönotto tulee suunnitella huolellisesti varsinkin suurissa ja kriittisissä hankinnoissa. Lopuksi on tärkeä huolehtia muutosten-



Kuva 1. Tietoturvallisuuden varmistamisen prosessi.

hallinnasta, joka pitää sisällään ylläpidon ja palvelun käytön päättämiseen liittyviä näkökulmia.

### Suosituksen sisältyvät liitteet ja niiden käyttötarkoitukset

#### Pääsopimukseen kirjattavat asiat

Pääsopimuksessa olisi hyvä huomioida, että seuraavat tietoturvaluusnäkökulman asiat ovat mukana:

- Oikeus tarkastaa kohteen kannalta riittävät tietoturvaluusjärjestelyt
- Tietoturvaluuden vastuuhenkilöt yhteystiedoissa
- Sopimuksen ja liitteiden soveltamisjärjestyksen huomiointi (erityisesti tietoturva- ja tietosuojaliitteet)
- Riittävät sakko- ja vahingonkorvauslausekkeet (myös tietoturvaluus- ja tietosuojavaatimukseen liittyvissä poikkeamisissa)
- Millainen purku- tai välittömän irtisanomisen ehto liittyy tietoturvaluusliitteen velvoitteiden rikkomiseen
- Tietojen sijainti tai käsittely Suomessa tai

ETA-alueella

- Mahdollisten yrityskauppatilanteiden huomiointi

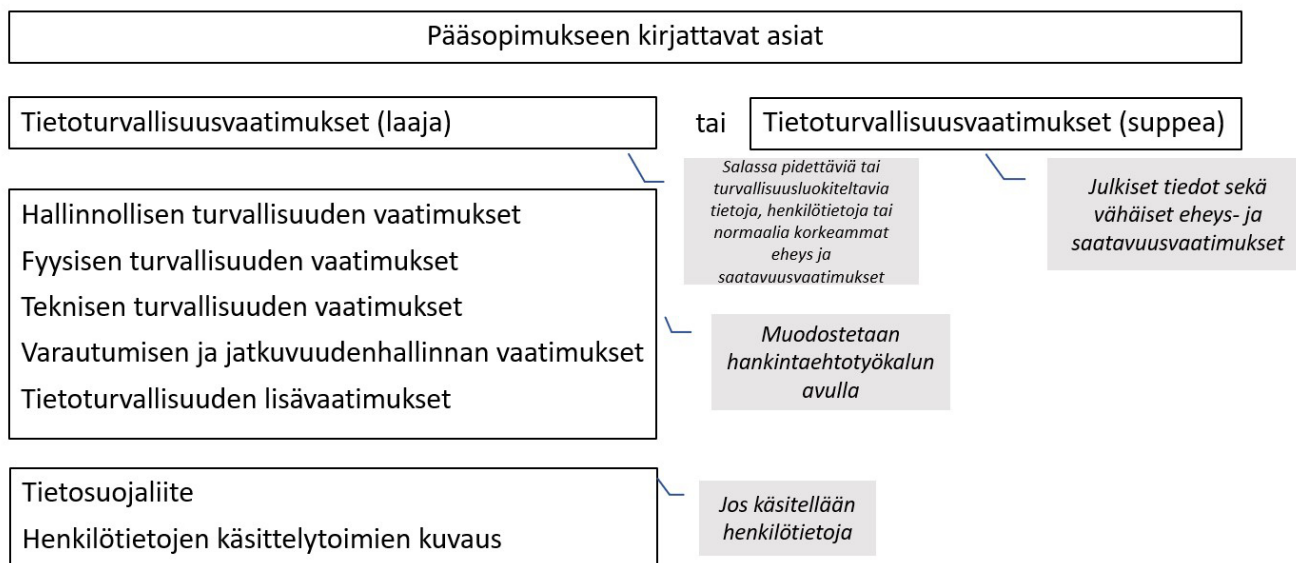
#### Suppeat tietoturvaluusvaatimukset -liite

Suppeita tietoturvaluusvaatimuksia voi käyttää osana sellaisia hankintoja, joissa käsitellään vain julkista tietoa ja tiedon eheyteen sekä saatavuuteen ei kohdistu normaalia korkeampia vaatimuksia. Näitä vaatimuksia voidaan käyttää myös tilanteissa, joissa käsitellään vain vähäisessä määrin muita kuin julkisia tietoja ja joiden paljastumisen aiheuttama vahinko on vähäinen.

#### Laajat tietoturvaluusvaatimukset -liite

Laajoja tietoturvaluusvaatimuksia suositellaan käyttämään hankintoihin, joissa käsitellään salassa pidettäviä tietoja, turvaluusluokiteltuja tietoja tai henkilötietoja. Lisäksi liite on tarkoitettu käytettäväksi sellaisissa tilanteissa, joissa palvelujen eheyteen tai saatavuuteen kohdistuu normaalia korkeampia vaatimuksia. Liitetä suositellaan käytettäväksi yhdessä hankintaehtotyökalun avulla muodostettavien osa-aluekohtaisten liitteiden sekä tietosuojaliitteiden kanssa.





Kuva 2. Sopimuksen tietoturvallisuusliitteet.

### Hankintaehtotyökalu - liite

Laajan tietoturvallisuusvaatimusliitteen kanssa suositellaan käyttämään Excel-pohjaista hankintaehtotyökalua. Työkalu helpottaa riskilähtöistä vaatimusten määrittelyä. Se pohjautuu Julkisen hallinnon tietoturvallisuuden arviointikriteeristöön, [Julkisiin](#). Julkin arviointikriteeristö on muokattu toimittajaa koskeviksi vaatimuskriteereiksi. Vaatimukset voidaan muodostaa eri osa-alueille, joita ovat hallinnollinen, fyysinen ja tekninen turvallisuus sekä varautuminen ja jatkuvuudenhallinta. Hankintayksikkö voi täsmentää ennalta määriteltäviä vaatimuksia sekä määrittellä lisävaatimuksia.

### Tietosuojaliitteet

Myös henkilötietojen käsittely on huomioitava hankinnan tietoturvallisuusvaatimusten määrittelyssä. Henkilötietojen käsittelyyn liittyvät vaatimukset voi huomioida hankintaehtotyökalun esiehdossa valitsemalla, että kohde sisältää henkilötietoja tai erityisiin henkilötietoryhmiin kuuluvia tietoja. Esiehtojen valinnalla hankintaehtotyökalu huomioi henkilötietoihin kohdistuvat tietoturva-vaatimukset osana vaatimusmäärittelyä.

Lisäksi VAHTI-toiminnassa on julkaistu erilliset tietosuojaliitteet ja henkilötietojen käsittelytoimien kuvaus. Liitteet löytyvät Digi- ja väestötietoviraston Digturvajulkaisut sivustolla kohdassa [Työkalut ja mallipohjat](#). Tietosuojaliite on tarkoitettu malliasiakirjaksi hankintoihin, joissa toimittaja tulee käsittelemään tilaajan henkilötietoja tilaajan lukuun. Henkilötietojen käsittelytoimien kuvaus on tarkoitettu malliasiakirjaksi, siihen mitä

tilaajan (rekisterinpitäjän) henkilötietoja toimittaja (käsittelijä) tai sen alihankkija käsittelee tuottaessaan sopimuksen mukaista palvelua.

### Loppusanat

Suositusta ja siihen liittyviä liitteitä työsti lukuissa määrää tietoturvallisuuden, tietosuojan ja hankinnan asiantuntijoita mukaan lukien Hansel ja Valtori. Tietoturvallisuusjaoston puheenjohtaja, tiedonhallintalautakunnan sihteeri Mika Kuronen valtiovarainministeriöstä johti suositusvalmistelua.

Tiedonhallintakunta hyväksyi suosituksen ja se julkaistiin 4.8.2023. Suosituksen ja sen liitteet löytyvät: <http://urn.fi/URN:ISBN:978-952-367-645-9>

Toivomme ja uskomme, että nämä suositukset ja siihen liittyvät liitteet helpottavat hankintayksiköiden työtä tietoturvallisuusvaatimusten määrittelyssä. Julkisen hallinnon käyttäessä samoja vaatimusmäärittelyitä myös toimittajien vaatimusmäärittelyihin vastaaminen yhdenmukaistuu ja helpottuu. Aina on mahdollista myös kehittää tehtyä työtä. Näitä toiveita ja käyttökokemuksia voi lähettää Tiedonhallintalautakunnalle ([tiedonhallintalautakunta\[at\]gov.fi](mailto:tiedonhallintalautakunta[at]gov.fi)). Suositus käännetään myös ruotsin kielelle. Kaikki versiot tulevat [Tiedonhallintalautakunnan verkkosivuille](#).

Olethan huomannut, että eOppivassa on julkaistu kaikille avoin koulutus [Julkista](#) sekä [salassa pidettävien tietojen käsittelystä ja suojaamisesta](#).



# Mallinnusilta 2.0!

Koko päivän seminaari arkkitehdeille  
Kokoushotelli Hanaholmen 9.11.2023

## Koko päivän liveseminaari arkkitehdeille, kokoushotelli Hanaholmen torstaina 9.11.2023

Viime vuonna KAOS järjesti ensimmäistä kertaa arkkitehdeille suunnatun, mallinnukseen keskittyvät koko päivän seminaarin. Seminaari onnistui yli odotusten ja sai tosi hyvät palautteet. Tämän innoittamana KAOS järjestää seminaarin myös tänä vuonna.

Kattaaksemme tilojen ja tarjoilujen kulut, tilaisuus on maksullinen. Seminaarin hinta on 160 € / 230 € riippuen valitsemastasi seminaaripaketista. Seminaari järjestetään, mikäli saamme riittävästi ilmoittautumisia 9.10. mennessä. Jos siis haluat mallinnuskarkeloiden toteutuvan tänäkin vuonna, niin toimi ripeästi!

Seminaari on suunnattu nimenomaan arkkitehdeille, joten ohjelmassa painottuvat erilaiset mallintamiseen liittyvät asiat; arkkitehtuurikuvausten hyödyntäminen, mallinnustyökalut ja arkkitehtien osaaminen.

Aamupäivällä on tiedossa kaksi puheenvuoroa, joiden aiheena ovat käytännön case-esimerkit kuvausten hyödyntämisestä sekä arkkitehtuurivälinetarjonta ja välineiden erityispiirteet. Lounaan jälkeen seminaarivieraat pääsevät osallistumaan mallinnusvälineiden demo-esityksiin (mm. BiZZdesign ja Sparx EA).

Demojen jälkeen on vuorossa puheenvuoro arkkitehtien osaamisesta. (Puhuja varmistuu myöhemmin, mahdollisesti kuulemme eräässä toisessa Pohjoismaassa lanseeratusta arkkitehdin osaamisprofiilista.)

Seminaarin virallisen ohjelman päättää paneelikeskustelu. Keskustelun teemaksi valikoitui 'kestävä arkkitehtuuri' – miten arkkitehtuuritoiminto saadaan pidettyä hengissä pidempään?

Seminaarin lisätiedot ja ilmoittautuminen:  
[www.sytyke.org/tapahtumat/mallinnusilta-2-0/](http://www.sytyke.org/tapahtumat/mallinnusilta-2-0/)

KAOS – Kokonaisarkkitehtuurin osaamisyhteisö





# Suomen Merenkulun Uusi Aikakausi

## Vähäpäästöisyys, Logistiikkakustannukset ja V

Suomen taloudellinen selkäranka on vahvasti kiinni merenkulussa. Yli 80 % maamme viennistä ja tuonnista kulkeutuu meriteitse, osoittaen alan kriittisen merkityksen kansalliselle hyvinvoinnille. Kuitenkin, kuten monet perinteiset teollisuudenalat, myös merenkulku seisoo historiallisen nopean muutosvaiheen kynnyksellä. Tämä muutostahti ei ole pelkästään teknologisen kehityksen seurausta, vaan yhä enenevissä määrin vastauksena kasvaviin regulaation ja asiakkaiden vaatimuksiin vähäpäästöisemmästä liikenteestä. Maailmanlaajuiset ilmastotavoitteet ja kuluttajien kasvava ympäristötietoisuus asettavat paineita alalle, joka on perinteisesti ollut riippuvainen fossiilisista polttoaineista.

Tämän haasteen edessä laivanvarustajat ja operaattorit kohtaavat kalliiden vaihtoehtoisten polttoaineiden dilemmaa. Vaikka nämä polttoaineet voivat tarjota ratkaisun päästöongelmiin, niiden

korkea hinta ja saatavuushaasteet tekevät niistä vaikeasti hyväksyttäviä lyhyellä aikavälillä. Itämeren alueella laivan käyttökustannukset koostuvat jo nyt jopa 80 % polttoainekuluista, mikä korostaa polttoainevalinnan taloudellista painoarvoa.

Näissä olosuhteissa parempi tilannekuva ja kyky optimoida toimintaa tulevat keskeisiksi tekijöiksi. Teknologian ja data-analytiikan rooli korostuu, kun etsitään ratkaisuja tehokkaampaan reittisuunnitteluun, polttoaineenkulutuksen vähentämiseen ja ylipäätään parempaan resurssien hallintaan.

On syytä huomata, että tämä ei ole pelkkä merenkulkuun liittyvä haaste tai mahdollisuus. Alhaisemmat logistiikkakustannukset vaikuttavat suoraan tuotteiden hintoihin kotimaassa. Lisäksi ne ovat avainasemassa, kun puhutaan Suomen viennin kilpailukyvyistä globalisoituneessa maailmantaloudessa. Jokainen säästetty euro logistiikassa voi



## Olli Soininen

Kirjoittaja toimii hankepäällikkönä Fintrafficin Meriliikenteenohjauksessa, missä hän on vastuussa Fintraffic VTS:n kehitys- ja investointihankkeiden johtamisesta sekä projektien sidosryhmäsuhteista ja kansainvälisistä kumppanuuksista. Hänellä on laaja, yli 20 vuoden kokemus järjestelmäkehityksestä, digitalisaatiosta ja automaatiosta. Ennen nykyistä rooliaan Fintrafficissa, Soininen palveli yli 20 vuotta merivoimissa eri tehtävissä. Vuodesta 2004 lähtien hän toimi järjestelmäkehityspäällikkönä, keskittyen johtamis- ja merivalvontajärjestelmien suunnitteluun ja kehitykseen.



## Liikennin Kilpailukyky

kääntä Suomen talouden eduksi, kun pyrimme säilyttämään ja kasvattamaan asemaamme kansainvälisillä markkinoilla.

Tulevaisuuden merenkulku vaatii adaptiivisuutta, innovaatiota ja sitoutumista kestäväan kehitykseen. Suomen kaltaiselle maalle, joka on syvästi sidoksissa meriliikenteeseen, tämä ei ole pelkästään haaste, vaan myös mahdollisuus määritellä tulevaisuuden suuntaa ja standardia alalla.

### Fintraffic VTS: Liikenteenohjauksen ja merilogistiikan digitalisaation edistäjä

Fintraffic VTS (Vessel Traffic Services) on osoittautunut paitsi kriittiseksi tekijäksi meriliikenteen sujuvuuden ja turvallisuuden varmistamisessa, myös merilogistiikan digitalisaation tärkeäksi fasi-

litaattoriksi Suomen vesillä. Fintraffic VTS ei vain seuraa ja ohjaa vesiliikennettä, vaan näyttää myös aktiivista roolia digitalisaation kehitysprosessissa, joka kohdistuu merenkulun ja satamatoimintojen alueelle.

Fintraffic VTS:n operatiivinen tietotaito ja teknologinen kapasiteetti ovat osoittautuneet korvaamattomiksi, kun on kyse modernien, digitaalisten ratkaisujen integroimisesta perinteisiin merenkulun ja logistiikan prosesseihin. Onnistuminen edellyttää työskentelyä tiiviisti muiden toimijoiden kanssa alalla, jotta digitalisaatioprojekteissa, kuten NEMO:ssa, voidaan hyödyntää parhaita käytäntöjä, data-analytiikan sovelluksia ja muita teknologisia innovaatioita.

Yksi Fintraffic VTS:n keskeisistä tehtävistä on varmistaa, että digitalisaation mahdollistama tiedonkulku sujuu tehokkaasti ja saumattomasti kaik-





kien osapuolten kesken, mikä puolestaan auttaa parantamaan reaktiokykyä ja ennakointia meriliikenteessä sekä hyödyntää dataa liiketoiminnassa. Fintraffic VTS toimii myös keskeisenä tukena ja neuvonantajana toimijoille, jotka ovat digitalisaatiomatkan eri vaiheissa, tarjoten asiantuntemusta ja näkemystä, joka auttaa navigoimaan kohti menestyksekkäitä ja kestäviä digitaalisia ratkaisuja merilogistiikassa.

### **Merenkulkua digitalisoimassa: NEMO tekee merilogistiikasta sujuvampaa**


Suomi on merellinen maa. Meri yhdistää meitä maailmaan, mahdollistaa viennin ja tuonnin, ja rannikkojemme satamat kuhisevat päivittäistä aktiiviteettia. Kuvittele noin sata alusta, jotka saapuvat päivittäin satamiimme. Jokainen niistä lähettää saa-

pumiseen ja lähtöön 6–12 lakisääteistä ilmoitusta, jotka liittyvät esimerkiksi miehistöön ja rahtiin. Se tarkoittaa lähes 800 000 ilmoitusta vuosittain.

Tämä herättää kysymyksen: Kuinka voimme tehdä tästä prosessista tehokkaamman, sujuvamman, ympäristöystävällisemmän sekä vähentää ilmoittajaan kohdistuvaa byrokratiaa? Tulevaisuus on vastauksessa, ja se tulee digitalisaation muodossa. Suomen merenkulku on ottamassa uuden digitaalisen askeleen NEMO-järjestelmän myötä.

Kansainvälisen merenkulkujärjestön, IMO:n, määräys edellyttää vuoteen 2024 mennessä jokaisesta maasta ottamaan käyttöön Maritime Single Window -järjestelmän (MSW), EU tasolla toteutetaan European Maritime Single Window joka on laajempikokonaisuus pitäen sisällään niin IMO:n, EU:n ja kansallisen lainsäädännön perusteella kerättävät tiedot. Tämä "yhden luukun" järjestelmä on suunn-





NEMO tekee enemmän  
kuin vain nopeuttaa  
ilmoitusprosesseja.  
Se antaa myös  
kokonaiskuvan alusten  
saapumisista, mikä  
mahdollistaa paremman  
suunnittelun ja resurssien  
jakamisen.

niteltu vähentämään byrokratiaa, jonka kanssa alukset kohtaavat saapuessaan satamiin. Suomen vastaus tähän on NEMO. NEMO, jota Traficom in toimeksiannosta kehittää Fintraffic yhdessä kumppaniensa kanssa, on paljon enemmän kuin pelkkä ilmoitusjärjestelmä. Se on kokonaisvaltainen digitaalinen alusta, joka tuo automaation ja tiedonvaihdon uudelle tasolle.

Yksi NEMO:n keskeisimmistä eduista on, että se nopeuttaa ja tehostaa tiedonkulkua viranomaisten ja alusten välillä. Kun laiva saapuu satamaan ja antaa ilmoituksen jätteen jättämisestä, tiedot ovat välittömästi saatavilla kaikille tarvittaville osapuolille. Mutta NEMO tekee enemmän kuin vain nopeuttaa ilmoitusprosesseja. Se antaa myös kokonaiskuvan alusten saapumisista, mikä mahdollistaa paremman suunnittelun ja resurssien jakamisen. Tämän lisäksi, kun tiedämme tarkalleen, milloin

alus saapuu, voimme optimoida sen kulkunopeuden, mikä voi vähentää päästöjä. Tämä on erityisen tärkeää, kun otetaan huomioon, että Itämerellä liikkuvien alusten polttoainekustannukset muodostavat suuren osan niiden kokonaiskustannuksista.

NEMO:n etuna ei ole vain sen tuoma tehokkuus ja ympäristöystävällisyys, vaan myös sen tarjoama helppous ja sujuvuus. Mikään ei kehity, jos toimija toimii uuden järjestelmän myötä kuin ennen. Prosesseja tulee muuttaa ja suoraviivaistaa. NEMO:ssa on kyse paljon enemmän kuin vain teknologiasta. Se on kulttuurinen muutos, joka vie Suomen merenkulun seuraavalle tasolle.

NEMO:n lanseeraus on merkittävä askel Suomelle, mutta se on myös mahdollisuus näyttää tietä muulle maailmalle. Monet maat eivät ole vielä aloittaneet omien MSW-järjestelmiensä kehittämistä, ja Suomi voisi olla edelläkävijä tällä alueel-





Kun tiedämme tarkalleen,  
milloin alus saapuu,  
voimme optimoida sen  
kulkunopeuden, mikä voi  
vähentää päästöjä.

la. Suunnitelmien mukaan NEMOsta voisi tulla vientituote, joka hyödyntäisi Suomen pitkää perinnettä merenkulun teknologiassa. Teknologia, olipa kyseessä sitten NEMO tai mikä tahansa muu innovaatio, on vain niin hyvä kuin me teemme siitä. Mutta jos Suomi jatkaa tällä tiellä, tulevaisuus näyttää valoisalta.

#### Satamasovellus: Uuden sukupolven digitaalinen alusta satamatoiminnalle

Kun laiva saapuu satamaan, sen ympärillä alkaa nopeasti vilkas toiminta. Lastaus ja purkaminen, kunnossapitotyöt sekä muut perustarpeet, kuten jätehuolto, polttoaineen toimitus ja tavaroiden hoitaminen, otetaan käsiteltäviksi. Myöhästymiset satamassa voivat aiheuttaa monimutkaisia aikatauluongelmia ja kustannuksia. Tähän haasteeseen vastaa, Port Activity sovellus

Kun laiva myöhästyy tai sataman laituri on varattu, se voi vaikuttaa monen toimijan aikatauluihin. Tiedonkulun parantaminen satamatoimijoiden välillä on ollut suuri haaste, koska aikataulutiedot ovat olleet hajallaan. Port Activityn avulla tämä ongelma on ratkaistu. Sovellus kokoaa reaaliaikaiset aikataulutiedot yhteen paikkaan, paran-



taen tehokkuutta ja säästämällä kustannuksia.

Yhteistyössä Rauman ja Gävlen satamien kanssa kehitetty pilottiversio on saanut suurta suosiota. Yli kaksikymmentä Suomen satamaa käyttää jo Port Activitya, ja sen suosio on kasvamassa myös Ruotsissa. Sovellus tukee kansainvälistä yhteistyötä, erityisesti vilkkaalla Itämeren alueella.

Tämä innovatiivinen sovellus on osa EU-rahoitteista STM EfficientFlow -projektia. Projektin tavoitteena on ollut meriliikenteen tehostaminen, turvallisuuden parantaminen ja päästöjen vähentäminen. Port Activity edustaa juuri tällaista uuden sukupolven ratkaisua, joka hyödyntää digitaalista tiedonjakoa. Port Activityn avoin lähdekoodi mahdollistaa sovelluksen mukauttamisen eri satamien tarpeisiin. Sovelluksen mobiili- ja työpöytäversiot varmistavat, että se on helppokäyttöinen missä tahansa, toimistosta satamalaituriin. Pilottiprojek-

tin menestys on osoitus siitä, että digitaalinen aikakausi on todella saapunut satamatoimintaan. Satama sovellus on osa NEMO ekosysteemiä ja tarjoaa näkymän Suomeen vierailevien alusten aikataulutietoihin ja niiden muutoksiin.

Viranomaisten keräämä ja tuottama data on molemmissa tapauksissa keskeinen elementti uusien palveluiden kehittämisessä. On selvää, että vaikka merilogistiikan ala on ollut hitaampi omaksumaan digitalisaation etuja, olemme nyt pisteessä, jossa toimialan tarpeet ja vaatimukset kohtaavat teknologisen osaamisen oikealla hetkellä. Digitalisaation ovi on vasta raollaan, eikä kenelläkään ole täyttä käsitystä siitä, mitä se tuo tullessaan. On kuitenkin varmaa, että muutos tapahtuu nopeasti ja meidän on oltava valmiita yllättäviinkin käänteisiin. On suuri etuoikeus olla osana tätä transformaatiota.



# TIEDON ELINKAARI HALLINTAAN

Julkishallinnon ja yksityissektorin organisaatioiden toimintaympäristö sähköistyy koko ajan: yhä uusia tietojärjestelmiä otetaan käyttöön ja järjestelmäintegraatiot yleistyvät. Sähköisessä toimintaympäristössä asiakirjallisten tietojen elinkaaren hallinta ja ohjaaminen sekä tietojen arkistointi edellyttävät suunnitelmallisuutta ja asiakirjahallinnollisten ominaisuuksien toteuttamista tietojärjestelmissä. Näiden ominaisuuksien avulla pystytään turvaamaan asiakirjallisen tiedon eheyteen, alkuperäisyyteen, luotettavuuteen ja käytettävyyteen liittyvät vaatimukset.

Asiakirjahallinnolliset ominaisuudet kytketään osaksi tietojärjestelmien toiminnallisuutta, jolloin tietojärjestelmät tukevat niihin sisältyvien tietojen luotettavaa ja aukotonta käsittelyä koko niiden elinkaaren ajan, varmistavat asiakirjallisten tietojen käytettävyyden ja säilymisen sekä mahdollistavat säilytysarvon määrittelyn ja tarpeetoman aineiston hävittämisen.

Asiakirjallisen tiedon elinkaarta hallitaan ja ohjataan pitkälti metatietojen avulla. Jotta edellä luetellut asiakirjallisen tiedon laatuvaatimukset sähköisessä ympäristössä voidaan toteuttaa ja taata, järjestelmän metatietomallin on tarkoituksenmukaista perustua joko arkistolaitoksen SÄHKE -metatietomäärittelyseen tai asiakirjojen kuvailun ja hallinnan metatiedoista annettuun julkisen hallinnon suositukseen JHS 143. Arkistolaitoksen metatietomäärittely on ensisijaisesti suunnattu asiankäsittelyjärjestelmiin, mutta se on sovellettavissa myös dokumenttienhallintajärjestelmiin. JHS 143 kohdentuu nimenomaan muihin tietojärjestelmiin kuin asiankäsittelyjärjestelmiin.

Metatietomäärittelykset sisältävät runsaasti metatietoelementtejä ja niiden tarkenteita. Luotettavan tiedonhallinnan näkökulmasta on ensiarvoisen tärkeää, että suurin osa vaadittavista metatietoelementtien arvoista tallentuu järjestelmään automaattisesti; käyttäjän tallentamat arvot on rajattava minimiin ja niiden tallentamista on tarkoituksenmukaista ohjata erilaisin valintalistoin. Esimerkiksi dokumenttienhallintajärjestelmässä metatietoelementin ”asiakirjatyypin” arvoa käyttäjä ei voisi vapaasti valita, vaan valittavissa olisivat ainoastaan ne asiakirjatyypit, jotka liittyvät käsiteltävään prosessiin.

Julkishallinnon organisaatioissa erinomaisena tietojärjestelmien metatietoarvojen lähteenä toimii järjestelmien taustalle integroitava arkistonmuodostussuunnitelma. Lisätietoja arkistonmuodostussuunnitelmasta metatietojärjestelmänä saa arkistolaitoksen SÄHKE-hankkeen kotisivuilta ([www.narc.fi/sahke](http://www.narc.fi/sahke)) sekä vuoden 2006 alussa julkaistavasta arkistolaitoksen asiankäsittelyjärjestelmiä ja sähköistä arkistointia koskevasta määräyksestä.

## TIETO KYTKETTÄVÄ PROSESSIIN

Tietojärjestelmissä käsiteltävät tiedot ja asiakirjatiedostot on kytkettävä aina laajempaan kokonaisuuteen. Dokumenttienhallinta järjestelmien kansiorakenteen tulisi perustua organisaation toimintaprosesseihin, ei organisaatioyksiköihin eikä asiakirjatyyppeihin. Jos kansiorakenne tehdään asiakirjatyypiperusteisesti, tallennetaan kaikki sopimukset yhteen kansioon, kaikki tarjoukset toiseen kansioon ja kaikki muistiot kolmanteen kansioon. Tällöin yksittäisen muistion yhteys siihen asiaan, mihin se liittyy sekä muihin samaan asiaan liittyviin asiakirjoihin, katoaa.

Kuvattu tilanne ei ole kestävä sähköisen arkistoinnin näkökulmasta. Asiakirjalliselle tiedolle määritellyt laatuvaatimukset täyttyvät vain, jos asiakirjan asiayhteys, prosessikytkös, säilyy.

Vastaava tilanne syntyy, kun sähköpostiviestit säilytetään joko sähköpostijärjestelmässä tai sähköpostien arkistointiin kehitetyissä järjestelmissä. Viestit ovat irti siitä käsittelyprosessista, mihin ne liittyvät. Sähköpostijärjestelmä tai sähköpostiarkisto ei ole dokumenttien- eikä asianhallintajärjestelmä.

Asiakirjallisten tietojen käsittelyyn liittyvät työnkulut on sidottava organisaation toimintaprosessien kehittämiseen. Järjestelmään on tallennuttava kattavat merkinnät tietojen käsittelyvaiheista. Aukoton käsittelyketju ja automaattiset tilasiirtymät takaavat omalta osaltaan järjestelmän tietosisällön luotettavuuden, eheyden ja alkuperäisyyden.

Asiakirjallisten tietojen tilasiirtymät määritellään prosessikuvausten yhteydessä: miten asiakirjallisten tietojen tilat muuttuvat prosessin edetessä, missä vaiheessa asiakirjaan ei enää voi tehdä muu-

# Historian havinaa



toksia? Tilasiirtymät automatisoidaan, jolloin prosessiin sisältyvän ennalta määritellyn toiminnallisuuden toteuttaminen järjestelmässä muuttaa asiakirjatiedoston tilaa.

## LOKI- JA MUUTOSHISTORIATIETOJEN TALLENTUMINEN

Tietojärjestelmän on automaattisesti tallennettava järjestelmän tietosisältöön kohdistuneet tapahtumat ja toimenpiteet lokitietoihin. Esimerkiksi dokumenttienhallintajärjestelmässä metatietoihin tehtävien merkintöjen ja muutosten sekä asiakirjallisten tietojen käsittelyyn liittyvien toimenpidetietojen on tallennuttava lokitietoihin. Asiakirjatiedoston sisältöön kohdistuvista muutoksista ja muutosten tekijöistä järjestelmän on kerättävä säilytyshistoriatietoa.

Loki- ja muutoshistoriatietojen tallentuminen ja niiden seuranta ja valvonta vastaavat omalta osaltaan asiakirjallisille tiedoille määriteltyihin laatuvaatimuksiin. Nämä vaatimukset vaikuttavat myös siihen, kuinka kauan lokitietoja järjestelmissä säilytetään.

## TIETOJÄRJESTELMÄN HÄVITYSTOIMINNALLISUUS

Nykyisten tietojärjestelmien määrittelyvaiheessa asiakirjallisen tiedon elinkaaren loppupää on valitettavan usein unohtunut. Järjestelmät palvelevat luonnollisesti organisaation operatiivista toimintaa, mutta toiminnan rationalisoinnin ja kustannustehokkuuden näkökulmasta pitäisi olla luonteavaa, että sähköisiin tietojärjestelmiin sisältyvät tiedot voidaan

säilyttää luotettavasti sähköisessä muodossa ja että tarpeettomaksi käyneet tiedot voidaan järjestelmästä hävittää.

Käytännössä tämä tarkoittaa sitä, ettei tietojärjestelmissä tuotettujen ja tietojärjestelmään tallennettujen tietojen säilyttämistä eikä hävittämistä ole juurikaan mietitty. Hävittäminen toteutetaan eräajoina siten, että kaikki tiettyä vuotta vanhemmat tiedot poistetaan järjestelmästä. Tämä ei vastaa asiakirjahallinnollisia vaatimuksia, sillä organisaation asiakirjallisten tietojen säilytysajat on määriteltävä prosessiperusteisesti: kaikkia muistioita ei säilytetä yhtä kauan, vaan säilytysaika päätetään niiden tietosisällön mukaan.

Metatiedot ohjaavat myös asiakirjallisten tietojen hävittämistä. Tämä edellyttää sitä, että järjestelmään tallennetuille tiedoille on etukäteen määriteltävä konkreettiset säilytysajat ja säilytysajan päättymisen laskentaperusteet. Laskentaperusteet sidotaan järjestelmän toiminnallisuuteen. Määritetyn toiminnallisuuden toteuttaminen tallentaa automaattisesti säilytysajan päättymisajankohdan asianomaiseen metatietokenttään. Järjestelmän hävitettäväksi esittämät tiedot on jonkun henkilön aina hyväksyttävä.

## ARTIKKELISTA

Artikkelin on kirjoittanut Päivi Happonen. Happonen työskenteli tuohon aikaan ylitarkastajana Kansallisarkiston asiakirjahallintoyksikössä.

Artikkeli on julkaistu ensimmäisen kerran Systeemyö -lehdessä 4/2005





KUUTAMOLLA

## TUKI VAI TAAKKA

Ilmiselvää on, että tällä hetkellä maailmassa eniten lisääntyvä asia on data. En muista tarkkoja lukuja, koska lehtemme tutkimusosaston analyttikot ovat juuri aloittaneet työnseisauksen ja lähteneet mielenosoituksellisesti Müncheniin ja aikovat kumota hallituksen aikomia jotain toimenpiteitä oktoberfest-tuoppi kerrallaan, mutta jos sata vuotta sitten tietoa kerääntyi kahvikupillisen verran vuodessa, niin kymmenen vuotta sitten määrä oli tankkerin verran ja nyt puhutaan pienemmän kokoluokan valtamereestä. Yhtäkkiä on keksitty, että on ääretömän tärkeitä laittaa kaikki mahdollinen asia muistiin. Olen ennenkin tainnut tällä paikalla kertoa, kuinka jo vuosia sitten jumbojetin yhdessä siivessä oli arviolta satatuhatta anturia keräämässä dataa. Lisäksi kellot, puhelimet, pyörät, hammas-harjat, uunit ja jääkaapit, autoista puhumattakaan, keräävät dataa jatkuvasti.

Totta kai tämä kerätty data on äärimmäisen tärkeää. Kuluttajan on ehdottoman tärkeää ymmärtää, kuinka nopeasti se lenkki tuli juostua (keskimääräinen nopeus kilometreinä tunnissa, keskimääräinen vauhti minuuteissa per kilometri, keskimääräinen kalorikulutus ja syke, sekä maksimit ja minimi kaikista ja trendit koko mittaushistorian ajalta ja toki voi liittyä isompiin porukoihin, jolloin saa vertaisryhmältä vertailtavaa dataa ja kilpailuhenkiset voivat yrittää päästä joka kategorian ykkösiksi), miten yö tuli nukuttua, miten paljon sähköä tuli kulutettua viime kuussa ja miten paljon

## Sytyke hallitus 2023



**Timo Piiparinen**  
Jyväskylän kaupunki  
puheenjohtaja, päätoimittaja  
040 770 1710  
timo.piiparinen[at]sytyke.org



**Janne Heinonen**  
Solable  
varapuheenjohtaja, talousasiat  
janne.heinonen[at]sytyke.org



**Jarkko Koistinaho**  
AtoZ  
jarkko.koistinaho[at]sytyke.org



**Maila Vienola**  
Telia  
maila.vienola[at]sytyke.org

rahaa. Pitkälle on tultu niistä ajoista, kun baarireisun reitti pääteltiin taskussa olevien kuittien perusteella. Silloinhan raha oli vain käteistä ja aina kaikki meni.

Kaikki tuo datamäärä, joka meistä kerätään ja jota meille analysoidaan ja lopuksi tuodaan pureskeltuna hienoksi visuaaliseksi esitykseksi, pyörähtää muuallakin kuin vain siinä analyysidataa tuottavassa värkissä. Ja sitä voidaan käyttää muuhunkin kuin vain meille tarkoitettuun lopputuotokseen. Sehän voidaan vaikka myydä ja sitä voidaan yhdistellä muihin datalähteisiin. Tarpeeksi kun on massaa, niin saadaan jo luotua todennäköisiä kaupallisia menestysmalleja. Esimerkiksi minkälaista kivennäisvettä noin 40-vuotias kolesteriarvoiltaan arveluttava Opel-merkkisellä autolla ajava kahden lapsen isä ostaa lähikaupastaan torstaisin. Tai mitä reittiä Helsingin Stockmannin tavaratalon (vielä kun se on) parkkihalliin pysäköivä menestynyt ja maksukykyinen Breitling-kelloja harrastava keski-ikäinen naisjohtaja kävelee tavatakseen tuttavansa Tornin kattoterassilla.

Massojen käyttäytymisen mallintaminen on kannattavaa puuhaa, kysykää vaikka myymäläsuunnittelijoilta. Yksittäisen, identifioitavan yksilön data sen sijaan ei sillä lailla ole kiinnostavaa, ellei sitten ole viihdelehtitoimittaja tai muuten vaan pahat mielessä. Ja monellahan on. Eikä asian tarvitse olla sen suunnitelmallisempaa kuin että joku vähän tylsistynyt henkilökunnan jäsen vähän se-

lailee asiakastietoja. Vaikkapa sairaalassa. Tai pankissa.

Henkilötietojen ja yksityisyyden suojaan tarkoitettu tietosuojasetus, GDPR, onkin yksi niistä yleisemmin ymmärretyistä ja tunnetuista regulaatioista, mutta voi herranpieksut niitä on vaikka kuinka paljon. GDPR:n yhdeksi ehkä suurimmaksi hienoudeksi on luettava sen lausuttavuus, suomeksi ja englanniksi. Jos vaikka vertaa IFRS:ään.

Nämä tällaiset erilaisten regulaattoreiden laatimat sääntelyyn, ohjaamiseen ja hallitsemiseen tarkoitetut regulaatiot luovat sen viitekehyksen, jossa kullakin alueella toimivat operaattorit voivat touhuta. Se, onko niistä enemmän hyötyä vai haittaa, voidaan jättää kunkin henkilökohtaiseksi mielipiteeksi. Varmaa on, että ne aiheuttavat paljon työtä. Kun sitä dataa niin mahdottoman innokkaasti kerätään, niin yritykset joutuvat jonkin verran pohtimaan, että mitäs sillä oikein tehdään ja miten sitä säilytetään ja sitten jossain vaiheessa ehkä tuhoaan.

Tämä kaikki on sellaista ihmisen itselleen itse keksimää ylimääräistä puuhaa. Ajatelkaa, miten paljon vähemmän olisi stressiä, korjattavia virheitä, rahaa syydettyä datanhallintajärjestelmiin ja konsultteihin, jos emme keräisikään mitään dataa. Keskityttäisiin vain kaikki omiin, oikeisiin töihimme. Tämä on aivan sama asia kuin se vanha totuus, jota aina välillä toistan: elämä olisi paljon helpompaa, jos ei olisi asiakkaita ollenkaan.



Kati Viik  
CGI  
kati.viik[at]sytyke.org



Reino Myllymäki  
Ketterät kirjat  
varajäsen  
reino.myllymäki[at]sytyke.org



Minna Oksanen  
Ari Hovi Oy  
varajäsen  
minna.oksanen[at]sytyke.org

Liittokokousedustajat  
Janne Heinonen  
Timo Piiparinen



Seuraavassa numerossa:

# PROJEKTIN HALLINTA – MINNE MENET?

70  
TIVIA



# systemAI

SytykeHybridinaari  
22.11.2023

Tekoäly systeemityössä klo 14-19 seminaari ja webinaari

- Webinaari
- Seminaari: Telia Finlandin tiloissa, Pasilan asema-aukio 1

Ohjelmassa mm.:

- KEYNOTE, Petteri Järvinen: Tekoäly ja työn tulevaisuus
- Sytyke ry:n syyskokous klo 19-20

Lisätietoja ja ilmoittautuminen:

- [www.sytyke.org/seminaari](http://www.sytyke.org/seminaari)

## SYTYTTÄÄKÖ? – Liity jäseneksi

Systeemityöyhdistys SYTYKE ry on Tieto- ja viestintätekniikan ammattilaiset TIVIAN suurin valtakunnallinen teemayhdistys. Sytyke on jo vuodesta 1979 lähtien kehittänyt tietojärjestelmäalan ammatillista osaamista. Sytyke yhdistää suomalaiset tietojärjestelmätyön ammattilaiset liiketoiminnasta teknisiin asiantuntijoihin.

Käsitlemme alan ajankohtaisia teemoja, keskustelemme ja opimme yhdessä – hypetystä tervejärkisesti. Sytykkeen osaamisyhteisöissä samoista teemoista kiinnostuneet verkostoituvat asiantuntijataapahtumissa.

Lisätietoja: [www.sytyke.org](http://www.sytyke.org)

Sytykkeen jäseneksi liittyminen onnistuu TIVIAN verkkosivustolla [www.tivia.fi](http://www.tivia.fi) ja sieltä valitsemalla Liity jäseneksi. Aukeavalta sivulta löydät Sytykkeen lisäksi muut TIVIAN alaiset jäsenyhdistykset. Painamalla Liity nyt -painiketta, pääset valitsemaan jäsenyytyypin. Tämän jälkeen valitse tiputusvalikosta yhdistys, jonka jäseneksi haluat liittyä. Poimi Systeemityöyhdistys SYTYKE ja lisää se ostoskoriin. Voit vielä tilata jäsenyydellesi lisäjäsenyyksiä tai -palveluja. Lopuksi valitse Jatka tilaamaan viimeistelläksesi jäsenyytilauksen.

Henkilöjäsenmaksu vuonna 2023 on 65€, eläkeläiset 44€ ja opiskelijat 20€ vuodessa. Nuorisojäsenyys (alle 23-vuotiaat) maksaa 10€ vuodessa. Jos ennestään olet jo TIVIAN jonkin toisen yhdistyksen jäsen, lisäjäsenyys Sytykkeessä maksaa vain 16€ vuodessa.

Lisätietoja: [www.tivia.fi](http://www.tivia.fi) ja [jasenasiat\[at\]tivia.fi](mailto:jasenasiat[at]tivia.fi)