



# Selvitys tiedon tietoturvalliseen hyödyntämiseen liittyvistä lainsäädännön vaatimuksista ja reunaehdoista

Turun kaupunki,  
Konsernihallinto, Integraatiotoiminto, Asiakasohjaus



# Sisällys

<b>1 Johdanto</b>	<b>3</b>
<b>2 Sääntelyn haasteet julkisella sektorilla</b>	<b>4</b>
2.1 Henkilötietojen käsittelyn oikeusperusteet.....	5
2.2 Tulkinnan vaikeus .....	6
<b>3 Kolmen tason tarpeita tilanteen selkeyttämiseksi</b>	<b>8</b>
3.1 Lainsäädännön taso .....	8
3.2 Käytännön taso.....	9
3.3 Eettinen taso.....	11
Lisätietoa selvityksestä .....	11
Kirjoittajat .....	11

**Selvitys tiedon tietoturvalliseen hyödyntämiseen liittyvistä  
lainsäädännön vaatimuksista ja reunaehdoista**

**Raportin tuottaja:** Konsernihallinto, Integraatiotoiminto, Asiakasohjaus

**Taitto:** KMG Turku

**Kansikuva:** Turun kaupunki, Valentino Valkaj

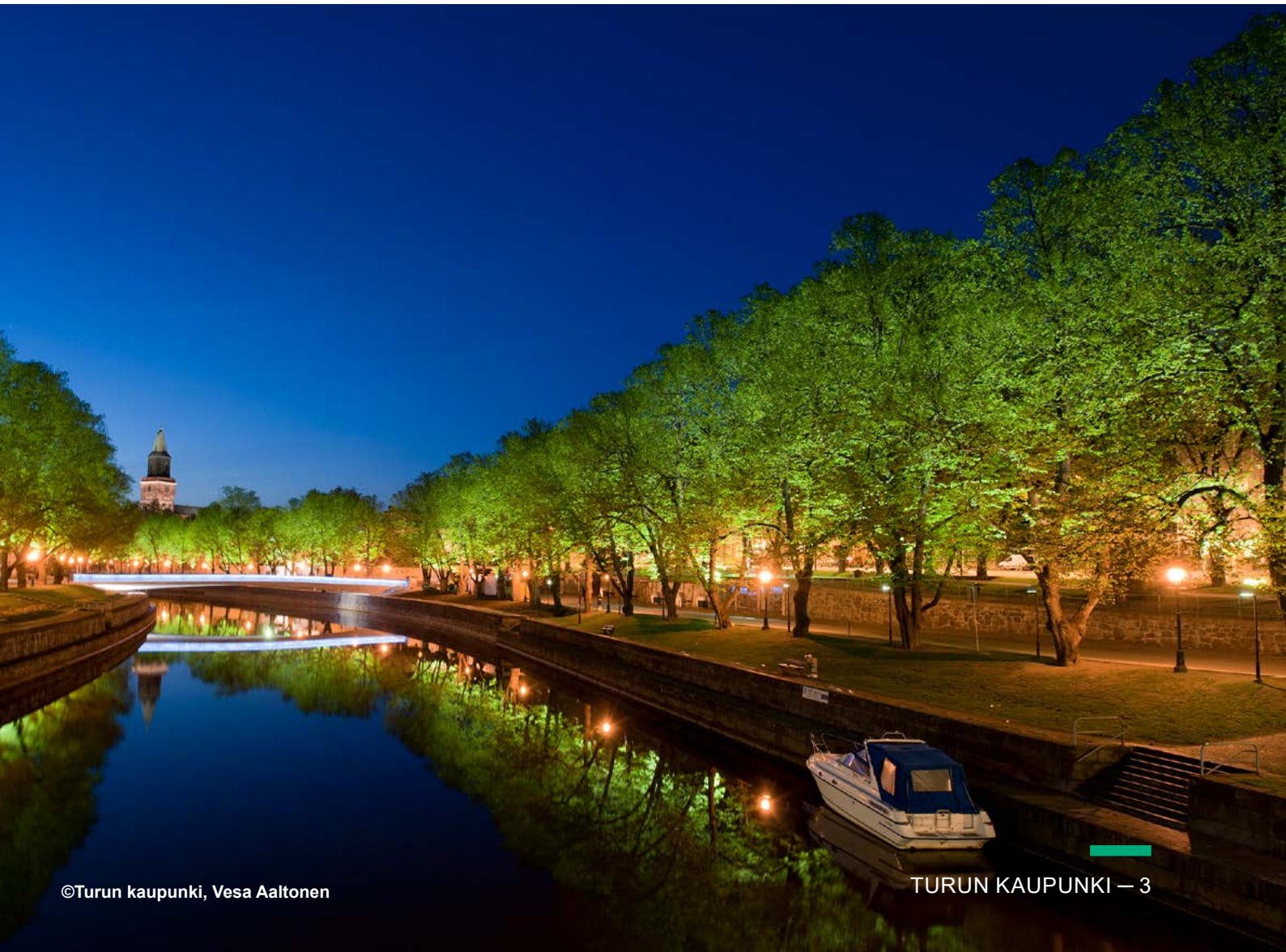
**Julkaistu:** 11/2023

# 1 Johdanto

Laki digitaalisten palvelujen tarjoamisesta asettaa kunnille velvoitteita sähköisten palveluiden toteuttamiseksi<sup>1</sup>. Digitalisaatio nähdään edellytyksenä, jotta kunnat ja muut julkisen sektorin toimijat voivat selvitä näistä velvoitteista. Samaan aikaan kun kuntien, kansallisella ja EU:n tasolla luodaan uusia ja kunnianhimoisia data- ja digitalisaatiostrategioita, on edistys käytännön projekteissa usein hidasta monimutkaisesta ja epäselvästäkin regulaatiosta johtuen. Käytännön haasteita aiheuttavat lisäksi kuntien riittämättömät tietosuojaresurssit tai riittämätön osaaminen. Toisaalta nopea teknologinen kehitys tarjoaa jatkuvasti uusia mahdollisuuksia ja toisaalta nostaa esiin uusia lainsäädännön haasteita.

---

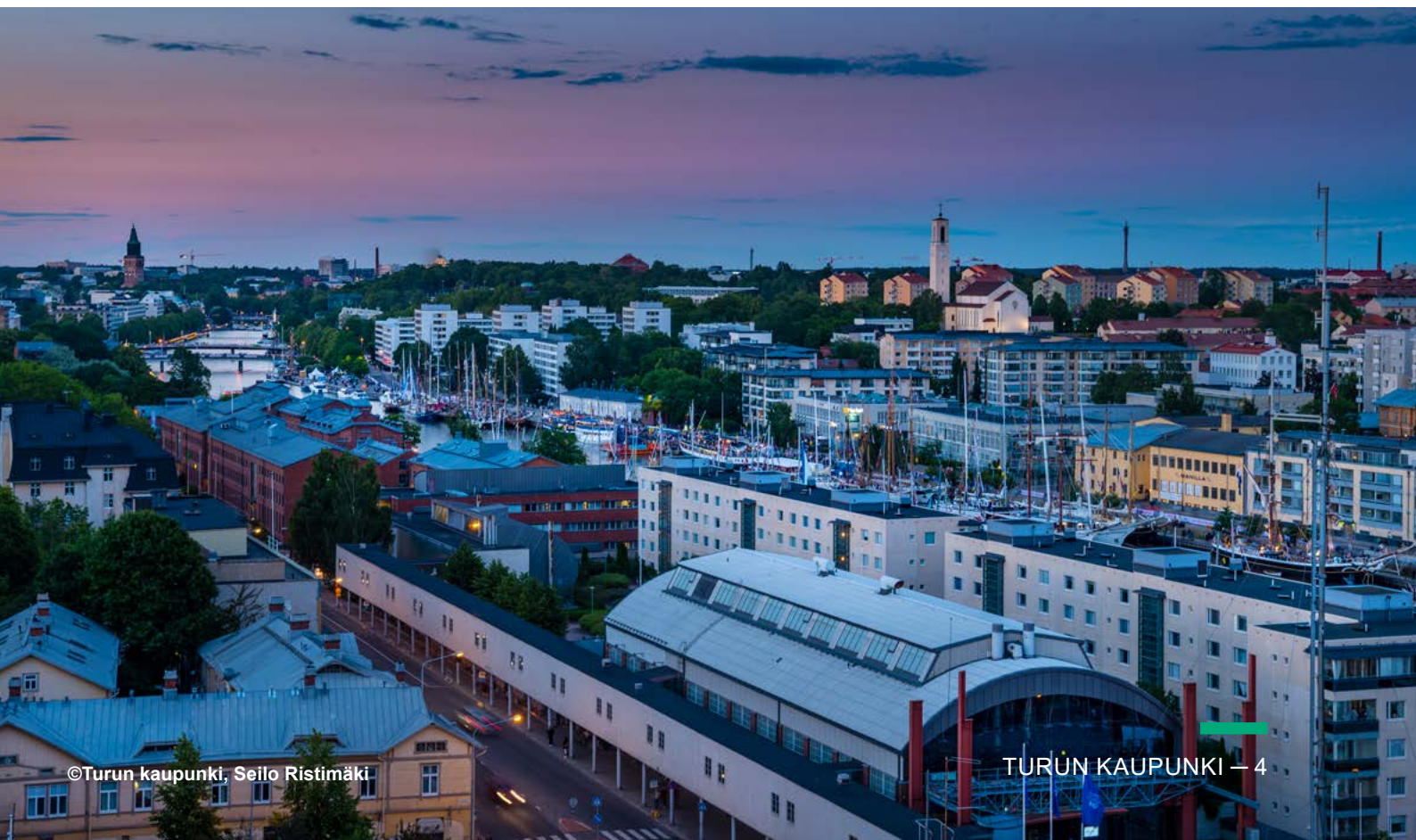
<sup>1</sup> Laki digitaalisten palvelujen tarjoamisesta (306/2019). <https://www.finlex.fi/fi/laki/alkup/2019/20190306>



## 2 Sääntelyn haasteet julkisella sektorilla

Julkisen sektorin toimintakenttä on perustavanlaatuisesti erilainen kuin yksityisen tai kolmannen sektorin, koska erityiset lakisääteiset vaatimukset rajoittavat toimintamahdollisuuksia. Valtiolle muodostuu yhtenäisiä käytäntöjä, koska toimintamalli ja prosessit (esim. Valtorin rooli) ovat yhtenäisempiä. Kunnat ovat itsevaltaisempia, mikä tarkoittaa, että lakisääteisten velvoitteiden tulkinta voi hajautua kuntakohtaisesti, eikä yhteneväisiä käytäntöjä synny yhtä helposti. Tämä johtaa ongelmiin ja keskusteluihin ”miten pitäisi toimia”, mutta ei kannusta kokeilevaan kulttuuriin lain tulkinnassa, esimerkiksi yleisen edun hyödyntämisessä palveluita kehitettäessä tai tiedolla johtamisessa.

Esimerkiksi henkilötietojen käyttö muuhun kuin alkuperäiseen tarkoitukseen on ollut haasteellista ja myös sääntelyn estämää. Tämä asettaa haasteita, kun halutaan kehittää täydentäviä lisäpalveluja, jotka ylittävät lakisääteiset velvoitteet. Kunnissa tämä korostuu edelleen, koska niille on asetettu laissa määritettyjä velvoitteita, joihin yksittäisillä kunnilla ei ole mahdollisuutta vaikuttaa. Valtionhallinnolla on kuntiin verrattuna myös enemmän mahdollisuuksia vaikuttaa lainsäädännön kehittämiseen.



## 2.1 Henkilötietojen käsittelyn oikeusperusteet

EU tietosuoja-asetus (GDPR) on EU:n pakottavaa lainsäädäntöä ja luo siten laillisen perustan henkilötietojen käytölle unionin jäsenvaltioissa<sup>2</sup>. Tietosuoja-asetuksen tavoitteena on helpottaa henkilötietojen käsittelyä, kun siihen on kansalaisten näkökulmasta katsottuna selkeä tarve ja peruste. Lisäksi tarkoituksena on, että tietosuoja-asetusta tulkitaan jäsenvaltioissa yhdenmukaisesti, eli tulkinta harmonisoidaan.

Julkisissa palveluissa tiedonkäyttö perustuu pääosin Artiklan 6 (1c) **antamaan oikeuteen käyttää tietoja lakisääteisen velvoitteen toteuttamiseksi**. Samaan aikaan henkilötietojen käsittely tulee minimoida ja varmistaa, että niitä ei käytetä muuhun kuin lakisääteisen palvelun toteuttamiseksi. Keskeistä on, että henkilötietoja sisältävän datan käytön tarve tulisi aina kyseenalaistaa. Toisin sanoen on arvioitava, voitaisiinko palvelu tarjota käyttämällä vähemmän sensitiivisiä henkilötietoja tai ylipäättään vähemmän tietoja. Mikäli palvelun järjestämiseen on useita vaihtoehtoja, tulee valita se, missä käytetään vähiten (sensitiivistä) tietoa. GDPR edellyttää myös riittäviä suojatoimia etenkin erityisiä henkilötietoryhmiä käsitellessä. Datan käsittelyn huolellinen suunnittelu ja selkeä informointi (mm. mitä, miksi, mistä, mihin, milloin, miten ja miten pitkäksi aikaa, mitkä ovat mahdolliset hyödyt ja vahingot) on aina tarpeen kansalaisten oikeuksien toteuttamiseksi. Minkään teknologian käyttöä ei sinänsä rajoiteta, kunhan tietosuojasäädösten vaatimukset täyttyvät.

<sup>2</sup> Ks. European Union (2016). Regulation (EU) 2016/679 of the European parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation). Official Journal of the European Union. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

### Euroopan parlamentin ja neuvoston asetus (EU) 2016/679

Käsittely on lainmukaista ainoastaan, jos ja vain siltä osin kuin vähintään yksi seuraavista edellytyksistä täyttyy:

- rekisteröity on antanut suostumuksensa henkilötietojensa käsittelyyn yhtä tai useampaa erityistä tarkoitusta varten;
- käsittely on tarpeen sellaisen sopimuksen täytäntöön panemiseksi, jossa rekisteröity on osapuolena, tai sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä;
- käsittely on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi;
- käsittely on tarpeen rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaamiseksi;
- käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi;
- käsittely on tarpeen rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi, paitsi milloin henkilötietojen suoja edellyttävät rekisteröidyn edut tai perusoikeudet ja -vapaudet syrjäyttävät tällaiset edut, erityisesti jos rekisteröity on lapsi.

Ensimmäisen alakohdan f alakohtaa ei sovelleta tietojenkäsittelyyn, jota viranomaiset suorittavat tehtäviensä yhteydessä.

Kuntien peruspalveluissa perusteet tietojen käytölle ovat siis vahvat ja lakiin perustuvat, mutta silti rajoitetut. **Suostumus on käsittelyperusteena vallan epätasapainosta johtuen haasteellinen. Sitä tulisikin käyttää käsittelyperusteena vain tarkasti harkiten.** Suostumuksen todellinen vapaaehtoisuus on siis aina varmistettava.

Kuten Euroopan tietosuojaneuvosto toteaa suostumusta koskevissa suuntaviivoissaan (05/2020), tilanteissa, joissa vallan epätasapaino on ilmeinen, suostumus voi tulla kyseeseen, jos suostumuksen epäämisen tosiasiallisena seuraamuksena ei ole kansalaiselle syntyvä haitta<sup>3</sup>. Jos palveluja voidaan käyttää vain sillä edellytyksellä, että henkilötietoja käsitellään, ei suostumus tule kyseeseen. Jos suostumusta halutaan käyttää, tulee siis varmistaa, että suostumuksen vapaaehtoisuus pystytään osoittamaan. Niille, jotka kieltäytyvät tästä suostumuksesta, palvelu tulee voida toteuttaa myös ilman suostumusta, esimerkiksi asioimalla henkilökohtaisesti kaupungin toimipisteessä.

Lakisääteisiä palveluja täydentävissä **lisäpalveluissa** olisi jopa suotavaa hyödyntää suostumuksen pyytämistä toiminnan eettisyyden vahvistamiseksi, samalla kun datan käyttöperusteena on lakisääteisen palvelun järjestäminen (yleinen etu on mahdollinen lisäperuste). Tällainen toimintatapa on jo käytössä esimerkiksi lakiin perustuvissa terveystietopalveluissa (huom. näihin kohdistuu erillinen lainsäädäntö), joissa kansalaisella on oikeus päättää, suostuuko hän tarjottuihin tutkimuksiin ja hoitoihin vai haluaako hän kieltäytyä niistä.

Myös yleinen etu on laillinen peruste, johon perustuen henkilötietoja voitaisiin periaatteessa julkisella sektorilla käyttää. Ongelmaksi yleisen edun kohdalla on noussut tiukka tulkinta välttämättömyydestä. Päätöksissä on korostettu, että tiedon käytön on oltava aivan välttämätöntä<sup>4 5</sup>. Välttämättömyyden osoittaminen ei ole helppoa, mikä käytännössä poissulkee yleisen edun käytön laillisena perusteena henkilötietojen käsittelyssä.

## 2.2 Tulkinnan vaikeus

GDPR rajoittaa henkilötietojen käyttöä muuhun kuin alkuperäiseen tarkoitukseen. Digi Távközlési és Szolgáltató Kft. -tapauksessa (C-77/21)<sup>6</sup> EU-tuomioistuin katsoo, että kansallisten tuomioistuinten on määriteltävä, kuuluuko henkilötietojen edelleen käsittely ”tarkoituksen rajoitusperiaatteen” piiriin, käytettäessä artiklan 6 (4) mukaisia kriteerejä. EU-tuomioistuimen ohjeet siihen ovat kuitenkin vähäiset. Tuomioistuin toteaa vain, että tietorekisterin kopio virheiden tarkistamiseksi ei näytä rikkovan tarkoituksen rajoitusperiaatetta, mutta ei anna lisäohjeita tarkoituksen rajoitusperiaatteen tarkemmasta tulkinnasta.

<sup>3</sup> European Data Protection Board. (2020a). Guidelines 05/2020 on consent under Regulation 2016/679. [https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679\\_en](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en)

<sup>4</sup> Euroopan Unionin tuomioistuin. *Vyriausioji tarnybinės etikos komisija (C-184/20)*. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62020CJ0184>

<sup>5</sup> Euroopan Unionin tuomioistuin. *Luxembourg Business Registers (C-37/20)*. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62020CA0037&qid=1685513172580>

<sup>6</sup> Euroopan Unionin tuomioistuin. Digi Távközlési és Szolgáltató Kft (C-77/21). <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62021CJ0077>

GDPR:n lisäksi julkista sektoria ja erityisesti kuntia rajaa monimutkainen sääntely-ympäristö, jonka puitteissa uusien digitaalisten palvelujen kehittäminen on vaikeaa, kun kehitettävien palveluiden lainmukaisuudesta ei voida olla varmoja <sup>7</sup>. Silloin palvelujen kehittäminen usein pysähtyy tai jo käytössä olevia palveluja joudutaan muuttamaan tai lopettamaan, esimerkiksi Tietosuojavaltuutetun tai oikeuden päätöksellä tiedonkäytön perusteen oikeellisuudesta.

<sup>7</sup> Koskinen, J., Knaapi-Junnila, S., Kuusniemi, L. & Karilahti, A. (2022). Henkilötietoja sisältävän datan eettinen hyödyntäminen kuntapalveluissa edellyttää tukea säädösten yhtenevään tulkintaan. Turun kaupunki, tutkimuskatsaus 5/2022. [https://www.turku.fi/sites/default/files/atoms/files/tutkimuskatsauksia\\_5-2022.pdf](https://www.turku.fi/sites/default/files/atoms/files/tutkimuskatsauksia_5-2022.pdf)



# 3 Kolmen tason tarpeita tilanteen selkeyttämiseksi

## 3.1 Lainsäädännön taso

Lainsäädännön ja sen tulkinnan selkeyttäminen tukisi julkisen sektorin mahdollisuutta kehittää digitaalisia palveluja. **Ensimmäinen** tavoite on mahdollisuus käyttää yleistä etua laillisena perusteena, mikä vaatii välttämättömyysperusteen avaamista ja arviointia niin kansallisella kuin EU-tasolla. **Toiseksi** tulisi saada selkeä tulkinta siitä, miten suostumusta voitaisiin käyttää julkisella sektorilla –vallanalaisuuden aiheuttama problematiikka huomioiden. Kun kyse ei ole lakisääteisistä palveluista, on suostumukseen periaatteellinen oikeus, sillä antamalla suostumus kansalaisen on mahdollista saada hyödyllisiä lisäpalveluja. Myös suostumuksen käänteinen käyttö (käytön kieltäminen) olisi mahdollista, jos henkilötietojen käyttöön perustuvalla digitaalisella palvelulla olisi myös vaihtoehtoinen toteutustapa. Tällöin yksilöllä olisi mahdollisuus valita toinen palvelukanava ja hän voisi halutessaan kieltäytyä digitaalisesta palvelusta. Samalla suostumus (tai tiedon käytön kieltäminen) noudattaisi GDPR:n tavoitetta. **Kolmantena** tarpeena on GDPR:n tulkinnan harmonisaation lisääminen, joka ei nyt käytännössä ole toteutunut unionissa<sup>8</sup>.

**Neljäntenä** tarpeena hyvinvointialueiden synnyn myötä, toisiolakia tulisi päivittää erityisesti sote-datan käytön osalta. Toisiolaki on osa lainsäädäntökokonaisuutta, joka koskee asiakastietojen sekä eräiden muiden terveyteen ja hyvinvointiin liittyvien henkilötietojen käsittelyä. Toisiolaki täydentää osaltaan yleistä tietosuojasetusta (GDPR).

Kunnilla on edelleen velvoite vastata kuntalaisten hyvinvoinnista ja siihen tarvittaisiin hyvinvointialueelle siirtynyttä sote-dataa. Hyvinvointialueen palvelut voivat käyttää dataa omien palveluidensa kehittämiseen, mutta samaa tietoa ei voida käyttää kunnissa hyvinvoinnin edistämiseen (esim. segregatio, syrjäytymisriski, häiriökäyttäytymisellä oireilevat nuoret). Palveluiden kehittämiseksi kuntalaisten tarpeita haluttaisiin tunnistaa mahdollisimman hyvin, mikä mahdollistaisi esimerkiksi liikuntapalveluiden proaktiivisen tarjoamisen riskiryhmille. Jos tähän olisi käytössä riittävästi dataa, loisi se mahdollisuudet luoda kokonainen ekosysteemi, joka voisi tarjota relevantteja palveluja.

Työllisyyspalvelut ja kotoutumispalvelut ovat kohtaamassa samanlaisia haasteita. Tämä osoittaa, että toisiolaki ei ole vain sote-dataan liittyvä ongelma, vaan ilmiö on laajempi, ja kattaa koko julkisen sektorin. Lainsäädännön tulisivin luoda mahdollisuuksia toiminnan ja palveluiden kehittämiseen.

<sup>8</sup> Ks. esim. Vlahou, A., Hallinan, D., Apweiler, R., Argiles, A., Beige, J., Benigni, A., ... others (2021). Data sharing under the general data protection regulation: time to harmonize law and research ethics? *Hypertension*, 77(4), 1029–1035. <https://doi.org/10.1161/HYPERTENSIONAHA.120.16340>

## 3.2 Käytännön taso

**Ensinnäkin** yksi käytännön ratkaisu olisi erottaa ohjaus- ja valvontavalta kahdelle erilliselle kansalliselle viranomaiselle. Tällä hetkellä tietosuojavaltuutetun toimisto voi antaa vain yleisiä ohjeita, koska he samanaikaisesti valvovat tietosuojan toteutumista. Uusi kansallinen ohjausviranomainen voisi sen sijaan antaa yksityiskohtaisia ohjeita GDPR:n toteuttamiseksi, mikä auttaisi pitämään tietosuojavaltuutetun erillään ohjaavasta viranomaisesta. Ohjaus- ja valvontavallan eriyttäminen varmistaisi myös sen, että organisaatio ei valvo itseään. Tiedonhallintalautakunnan tyyppinen ohjauselin olisi suositeltava myös tietosuoja-asioiden edistämiseen.

Tiedonhallintalautakunta on monialaiseen asiantuntijayhteistyöhön perustuva viranomainen, joka toimii valtiovarainministeriön yhteydessä. Tiedonhallintalautakunnassa on edustus valtakunnallisesti eri organisaatioista, myös kunnista ja se tarjoaa suosituksia, jotka ovat yleensä ohjauskeinoina käytännössä riittäviä. Olisi hyvä, jos tietosuoja-asioihin voitaisiin perustaa tiedonhallintalautakuntaa vastaava toimija, siis ”tietosuojalautakunta”.

Tietosuojalautakunnan tarjoamat yksityiskohtaiset ohjeet olisivat hyödyllisiä erityisesti tietojohdossa ja uusien digitaalisten palvelujen kehittäessä. Tällaisia ohjeita pidettäisiin hyväksyttävänä perusteena, johon paikalliset päätökset voisivat nojata. Näitä ohjeita noudattamalla paikalliset viranomaiset eivät syyllistyisi virheeseen, vaikka tietosuojavaltuutetun antama lausunto myöhemmin muuttaisi tietosuojalautakunnan alkuperäistä tulkintaa. Käytännöt tulisi korjata lausunnon mukaisesti, mutta alkuperäinen toiminta tulkittaisiin tehdyksi parhaimman tiedon nojalla, mikä loisi kannustavan mekanismin palveluiden kehittämiseksi.

Kunnilla on mahdollisuus tietosuojavaltuutetun ennakkokuulemiseen. Menettely on käytännössä hidas ja edellyttää tietosuojan vaikutustenarviointia. Ennakkokuuleminen ei myöskään sisällä (vaihtoehtoista) ratkaisuehdotusta, johon perustuen tiedonhallintaa ja palvelujen kehittämistä voitaisiin edistää.

GDPR:n One-Stop-Shop- periaatteen mukaan minkä tahansa EU-maan valvontaviranomaisten päätökset ovat sitovia kaikissa EU-maissa. Toisten EU-maiden valvontaviranomaiset eivät voi haastaa jonkun muun EU-maan valvontaviranomaisen päätöstä. Suomalaiset tietosuoja-asiantuntijat hakevat tietoa muiden maiden viranomaisten päätöksistä ja ohjauksesta antaakseen paikallista ohjausta. Ainakin merkittävässä päätöksissä olisi toivottavaa, että tietosuojavaltuutettu julkaisi päätöksestä suomenkielisen version ja toteaisi, että sitä on noudatettava. Tämä ei kuitenkaan poista sitä perusongelmaa, että ohjausta tarvitaan joko tietosuojavaltuutetun toimistolta tai erilliseltä uudelta ohjaavalta viranomaiselta. Tämä korostaa tarvetta, että ohjaus- ja valvontavalta eriytetään kahdelle erilliselle kansalliselle organisaatiolle.

**Toiseksi** tietosuojan tulee olla sisäänrakennettua ja oletusarvoista. Oletusarvon tulee kaikessa toiminnassa olla, että tietosuoja ja tietoturva huomioidaan riittävän varhaisessa vaiheessa ja riittävällä tavalla. Tietosuojaroolitus ja toimintamahdollisuudet tulee selkiyttää, dokumentoida ja hyväksyttää organisaation ylätasolla, ja roolituksia tulee noudattaa. Roolitusten osalta tulee

suunnitella mm. kuka johtaa tietosuojaa – onko se organisaation yleinen johto vai tarvitaanko asialle oma johtava resurssi (vertautuen esim. talousjohtajaan, henkilöstöjohtajaan jmv.). Edellä mainittu tukee hyvän tietosuojakulttuurin kehittymistä organisaatiossa. Sääntelyllä voidaan mahdollistaa henkilötietojen käsittelyä, mutta viimekädessä organisaatiokulttuuri määrittää riittävän tietosuojan tason (roolien selkeyttäminen, vastuunotto). Tietosuojan tulee olla osa arkipäivän johtamista ja siihen pitää olla tarjolla riittävästi asiantuntijatukea.

Laki velvoittaa perustamaan jokaiseen kuntaan **tietosuojavastaavan** tehtävän, mutta sitä hoidetaan usein käytännössä muun toiminnan ohella. Silloin tietosuojavastaava saattaa joutua rooliristiriitaan. Käytännössä esimerkiksi tilanteisiin, joissa henkilö jossain roolissa esittää ratkaisua, jonka myöhemmin hyväksyy tietosuojavastaavan roolissa. Myöskään tietosuojavastaavan osaamista ei ole selkeästi määritelty.

Käytännön kehittämisen näkökulmasta **tietosuoja-asiantuntijan** rooli on kunnissa tärkeämpi, koska tietosuoja-asiantuntija voi auttaa palvelujen kehittäjiä ratkomaan tietosuojaan liittyviä haasteita. Kunnissa ei kuitenkaan ole riittävästi tietosuoja-asiantuntijoita, ja heiltä puuttuu ohjaavan viranomaisen tuki. Tietosuoja-asiantuntijoille ei ole Suomessa selkeää omaa koulutusta, mikä tekee tilanteesta entistäkin haastavamman. Olisikin hyvä edellyttää vähintään esimerkiksi sertifikaatilla osoitettavaa muodollista pätevyyttä.

**Kolmanneksi** tietosuojan arviointi tulisi integroida systemaattiseksi osaksi järjestelmien välistä tiedonsiirtoa julkisissa palveluissa. Tietosuojavaltuutetun toimisto tarjoaa nyt jo erinomaisen työkalun, joka on tietosuojan vaikutusten arviointiohjeen mukainen<sup>9</sup>.

Tietosuojan arviointijärjestelmä olisi hyvä toteuttaa kansallisena palveluna. Palvelussa olisi kuvattu, mitä henkilötietoja käsitellään tai siirretään<sup>10</sup> ja käsittely olisi mahdollista vain, jos vaikutustenarviointi olisi tehty. Silloin muodostuisi pohja data-arkkitehtuurin kuvaukselle, jossa myös tietosuoja olisi huomioitu.

<sup>9</sup> Tietosuojavaltuutetun toimisto. <https://tietosuoja.fi/vaikutustenarviointi>

<sup>10</sup> Tietojen siirtoon tehdään tietyissä tapauksissa transfer impact assessment (eri asia kuin DPIA), tämä tulee implementoida järjestelmään myös

## [Tietosuoja.fi](https://tietosuoja.fi)

Tietosuojavastaava on nimitettävä, jos:

- käsittelette laajamittaisesti arkaluontoisia tietoja,
- seuraatte ihmisiä laajamittaisesti, säännöllisesti ja järjestelmällisesti,
- organisaationne on julkishallinnon toimija (poislukien tuomioistuimet).

### 3.3 Eettinen taso

Eettisen teknologian käytön tavoittelu pysyy haastavana tehtävänä, koska teknologian kehitys avaa jatkuvasti ennakoimattomia tapoja toimia ja tehdä asioita. Siksi yhteiskunnassa tulisi toteuttaa jatkuvasti eettistä teknologian ja datan käytön tarkastelua. Eettisyyden tulisi ohjata sekä lainsäädäntöä että sen tulkintaa, jotta lainsäädännön oikeutuksen eettinen perusteltavuus säilyisi. Lainsäädännön ja sen tulkinnan lisäksi on tarkasteltava myös eettistä näkökulmaa. Lakien ja säännösten tulisi aina suojata tai edistää tavoiteltavaa hyvää.

GDPR on alkanut estää julkista sektoria palvelemasta kansalaisia, mihin tulee etsiä eettisesti kestäviä ratkaisuja. Vaikka yksityisyys on tärkeää, ei se ole ainoa yhteiskunnassa tavoiteltava asia. Erityisen ongelmallista on se, että nykyinen tietosuoja-asetus tuntuu kahlitsevan julkista sektoria enemmän kuin yksityistä, koska julkisella sektorilla ei ole ollut mahdollisuutta käyttää suostumusta kuten yksityisellä sektorilla. Riskinä on, että julkinen sektori ei pysty hyödyntämään digitalisaatiota, mikä rapauttaa muutenkin koetuksella olevaa yhteiskunnan taloudellista kestävyyttä.

On varmistettava, että julkinen sektori palvelee kansalaisiaan oikeudenmukaisesti ja samalla edistää yhteiskuntaa, joka ei perustu kansalaisten kontrollointiin valvontayhteiskunnassa. Tavoitteena tulee aina olla kansalaisten etu, mutta ei vain yksilöinä tai vain yhteisönä, vaan näiden välillä tasapainoillen. Tavoitteena on kansalaislähtöisyys, jossa lisätään kansalaisten osallisuutta ja päätösvaltaa digitaalisia palveluja kehitettäessä.

#### Lisätietoa selvityksestä

- arto.karilahti@turku.fi
- wilhelmiina.griep@espoo.fi

#### Kirjoittajat

##### Turun kaupunki

- Karilahti Arto
- Paara Kari
- Ritvanen Johanna

##### Espoon kaupunki

- Griep Wilhelmiina
- Kaukonen Katariina
- Pernilä Paula
- Wollstén Piia

##### Turun Yliopisto

- Koskinen Jani

