

Asia: VN/26111/2023

Tietosuojalainsäädännön kokonaisuudistuksen koordinaatioryhmän väliraportti

TIETOSUOJAN YLEISSÄÄDÖKSET (EU:n yleinen tietosuoja-asetus ja tietosuojalaki)

Onko tietosuojan yleissäädösten yleisen tietosuoja-asetuksen tai tietosuojalain soveltamiseen koettu liittyvän haasteita tai epäselvyyksiä, jotka voisivat vaikeuttaa julkisen palvelun järjestämistä?

Kyllä

Jos on, minkälaisista haasteista tai epäselvyyksistä on tarkalleen ottaen kyse?

Suostumus käsittelyperusteena

Raportti käsittelee yleistä etua käsittelyperusteena viranomaistoiminnassa ja yleiseen etuun liittyviä epäselvyyksiä. Raportista ulkopuolelle jäävä kysymys on suostumuksen käyttäminen henkilötiedon käsittelyperusteena viranomaistoiminnassa.

Suostumus käsittelyperusteena kuntien palvelukehityksessä aiheuttaa nykyisellään hämmennystä ja kuntien välillä toisistaan poikkeavia tulkintoja. Useat kunnat ovat sitoutuneet OmaData-periaatteiden toteuttamiseen, ja suostumusta hyödyntämällä kuntien olisi mahdollista tarjota e-lakisääteisiä palveluita entistä kohdennetummin ja personoidummin sekä mahdollistaa uudenlaisia palveluja ja palvelupolkuja. Suostumuksen käytöstä viranomaistoiminnassa tulisi kuitenkin linjata kansallisesti nykyistä selkeämmin, jotta tulkintavastuu ei tässäkään asiassa jäisi yksittäiselle organisaatiolle. Tämä olisi syytä tehdä yhteistyössä kuntien ja muiden sidosryhmien kanssa linkittyen mm. meneillään olevaan digilompakkokehittämiseen sekä hallitusohjelmassakin mainittuihin kansallisiin suostumuksenhallintaratkaisuihin liittyvään pohdintaan. Muun muassa DVV on vastikään selvittänyt suostumuksen hyödyntämisen selkeyttämistarvetta Rekisteritiedon luovuttaminen suostumukseen perustuen. Käyttötapauksia ja asiakasymmärrystä -raportissa.

Lähtökohtaisesti tietosuoja-asetuksessa suostumuksen edellytykset on 7 artiklassa kirjoitettu selkeästi. Tietosuoja-asetuksen perustelukappaleessa 43 on kuitenkin asetettu viranomaistoimintaa

koskeva käyttörajoitus ”Jotta voidaan varmistaa, että suostumus on annettu vapaaehtoisesti, suostumuksen ei pitäisi olla pätevä oikeudellinen peruste henkilötietojen käsittelylle sellaisessa erityistilanteessa, jossa rekisteröidyn ja rekisterinpitäjän välillä on selkeä epäsuhta. Tämä koskee erityisesti tilannetta, jossa rekisterinpitäjänä on viranomainen ja jossa on sen vuoksi epätodennäköistä, että suostumus on annettu vapaaehtoisesti kaikissa kyseiseen tilanteeseen liittyvissä olosuhteissa.”

Rajoitus on kirjoitettu jyrkästi ja sekoittaa 7 artiklan tulkintatilanteita. Kohta ei sulje pois aidon suostumuksen käyttöä viranomaistoiminnassa, mutta antaa kuvan siitä, ettei se olisi mahdollista. Viranomaistoiminnassa on esimerkiksi salassa pidettävien tietojen osalta kuitenkin varsin tavallista, että niiden luovutus toiselle viranomaiselle ja käsittely muuhun kuin alkuperäiseen käyttötarkoitukseen on mahdollista vain rekisteröidyn suostumuksella. Tällainen tilanne voi tulla kyseeseen esimerkiksi silloin, kun rekisteröity antaa suostumuksensa luovuttaa potilastietojaan poliisille esitutkintaa varten.

Kuitenkin käytännön palveluita kehitettäessä on epäselvää, voiko suostumusta käyttää käsittelyperusteena tilanteissa, joissa on kyse ns. lisäpalveluista eli esimerkiksi kunnan tarjoamista, yksilölle vapaaehtoisista asiointia tai tiettyä asiointikokonaisuutta helpottavista palveluista. Nk. omadata-periaatetta noudattavat, datan liikkumiseen perustuvat uudenlaiset palvelut jäävät siis toistaiseksi oikeudellisesti epävarmalle pohjalle ja niiden kokeilu ja toteuttaminen ovat siten vaikeaa. Suostumuksen käyttöä viranomaistoiminnassa koskevaa sääntelyä olisi siis joko asetuksen tai kansallisen lainsäädännön tasolla selkeyttää.

EU:n datanhallinta-asetuksen määrittelemät datanvälityspalvelut sekä EU:n datasäädös tulevat jo lähitulevaisuudessa haastamaan tilannetta entisestään. Julkinen viranomainen voisi teoriassa toimia sekä datan haltijana, että datan vastaanottajana yksilön suostumukseen perustuvissa, uudenlaisia palveluita luovissa dataekosysteemeissä, mutta asia vaatisi tietosuojakysymysten osalta tarkempaa selvennystä. Aiheeseen tulisi kansallisesti perehtyä tarkemmin ja tarkastella asiaa myös suhteessa muiden EU-maiden tulkintoihin ja käytäntöihin, erityisesti huomioiden uusi EU-lainsäädäntö.

Muut käsittelyperusteet

Tietosuojalain 4 § 1 momentin 2 kohdan mukaan henkilötietoja saa käsitellä tietosuoja-asetuksen 6 artiklan 1 kohdan e alakohdan mukaan, jos käsittely on tarpeen ja oikeasuhtaista viranomaisen toiminnassa yleisen edun mukaisen tehtävän suorittamiseksi. Tätä kohtaa olisi tarpeen täsmentää, koska on käytännössä epäselvää, millaisissa tilanteissa kyseisen käsittelyperusteiden käyttäminen on mahdollista.

Raportissa nostetaan esiin, että osa koordinaatioryhmän kuulemista viranomaisista on pitänyt tietosuojalain 4 §:n 2 kohdan soveltamisalaa epäselvänä suunnittelu- ja selvitystehtävien osalta.

Vaikka viranomaisen suunnittelu- ja selvitystehtävä mainitaan nimenomaisena esimerkkinä lainkohdan perusteluissa, sitä on toivottu huomioitavaksi myös säännöksessä. Raportin mukaan suunnittelu- ja selvitystehtävästä ei välttämättä säädetä erikseen viranomaisen tehtävänä, mutta arvioitava kysymys on, onko sellaisesta ylipäättään tarpeen säätää. Sama koskee esimerkiksi palveluiden kehittämistehtävää.

Lisäksi käytännön toiminnassa on havaittu aika ajoin haasteita sen osalta, milloin käsittelyperuste pohjautuu lakisääteiseen velvoitteeseen ja milloin yleiseen etuun. Näiden kahden perusteen rajanvetoa olisikin tarpeen selkeyttää. Epävarmuutta on sen osalta, että jos viranomaisessa tahdotaan tehdä tietojen käsittelyä, joka ei rajaudu täysin lakisääteisen velvoitteen täyttämiseksi tarpeelliseen käsittelyyn, voiko viranomainen tällöin nojautua käsittelyssään yleiseen etuun, ”laajentaen” tällöin sitä, mitä viranomaisen on mahdollista henkilötietojen käsittelyn puitteissa tehdä pelkästään lakisääteisen velvoitteen nojalla.

Lisäksi epäselvää on se, mikä on henkilötietojen käsittelyperuste perusopetuksessa käytettävien digitaalisten työvälineiden käytön yhteydessä. Tästä kaupunki lausui laajemmin tammikuussa ja lausunto sisältyy sellaisenaan Kuntaliiton tammikuussa oikeusministeriölle antamaan muistioon.

Onko jonkin yleisen tietosuoja-asetuksen tai tietosuojalain säännöksen havaittu estävän viranomaisen tiedon liikkumisen tai julkisen palvelun järjestämisen tarkoituksenmukaisella tavalla? Onko tietosuojan yleissäädösten havaittu estävän tai rajoittavan tiedon tai henkilötietojen hyödyntämistä tai käsittelyä tarkoituksenmukaisella tavalla?

Ei

Jos on, mistä säännöksistä on tarkalleen ottaen kyse ja miten ne estävät tai rajoittavat tiedon käsittelyä?

-

VIRANOMAISTEN HENKILÖTIETOJEN KÄSITTELYÄ KOSKEVA KANSALLINEN ERITYISSÄÄNTELY

Onko kansalliseen erityissääntelyyn, jossa on kyse viranomaisten suorittamasta henkilötietojen käsittelystä (mukaan lukien henkilötietojen luovuttamisesta), koettu liittyvän haasteita tai epäselvyyksiä?

Kyllä

Jos on, minkälaisista haasteista ja epäselvyyksistä on tarkalleen ottaen kyse?

Henkilötietojen käsittely toissijaista tarkoitusta varten

Raportti nostaa esiin myös, että tietojen luovuttamista tai saamista koskevien säännösten osalta osa kuulluista viranomaisista nosti esiin tarpeen säätää viranomaisten oikeudesta käsitellä tietoja muihin

kuin alkuperäisiin käyttötarkoituksiin (niin sanottuun toisiokäyttöön), kuten viranomaisen tutkimus- tai selvittämistarkoituksiin tai palveluiden kehittämistarkoituksiin.

Käytännössä ”toisiokäyttö” aiheuttaa nimenomaan haasteita soveltajille, kun kyse on palveluiden kehittämistarkoituksesta ja palveluiden tarjoamisesta uusilla tavoilla, joissa hyödynnetään dataa ja mahdollisesti uutta teknologiaa (automaatio, tekoäly jne.) perinteisemmän asioinnin rinnalla. Tämä näkökulma puuttuu raportin tarkastelusta lähes täysin. Erityisesti näissä tilanteissa tietosuojakysymyksiin liittyy usein erittäin suurta epävarmuutta ja epäselvyyttä.

Henkilötietojen käsittely palvelun kehittämistä varten

Monet viranomaiset käyttävät tällä hetkellä sähköisiä palveluja, joilla pyritään siirtämään asiakkaan palvelu verkkoympäristöön. Esimerkiksi Omavero on tällainen sähköinen viranomaispalvelu, jota Verohallinto ylläpitää. Henkilötietojen käsittelyn peruste kyseisessä palvelussa on viranomaispalvelujen toteuttaminen.

Olenaisena kysymyksenä tällaisessa sähköisessä palvelussa on, että voiko Verohallinto käsitellä Omaveron käyttäjien henkilötietoja sähköisen palvelun kehittämistä ja parantamista varten esimerkiksi tietoturvan osalta. Verohallinnolla voi olla tarve käyttää käyttäjiensä tietoa, jotta palvelusta saadaan kaikille loppukäyttäjille turvallisempi. Laista ei kuitenkaan löydy suoraan perustetta, jolla viranomaiset voivat käyttää sähköisten järjestelmien käyttäjien henkilötietoja kyseisten sähköisten palvelujen kehittämiseen.

Opetuskentällä problematiikka koskettaa myös ei-viranomaistahojen sähköisiä palveluja. On epäselvää, saako esimerkiksi Wilmajärjestelmää kehittää toimivammaksi ja turvallisemmaksi työntekijöiden tai järjestelmään rekisteröityjen lasten tietojen käsittelyllä.

Tällä hetkellä viranomaisten suorittamaa henkilötietojen käsittelyä sääntelevä lainsäädäntö ei näytä mahdollistavan sitä, että viranomaiset käyttävät rekisteröityjen henkilötietoja palvelujensa kehittämiseen. Tämä tulkinta johtaa siihen, että sähköiset palvelut eivät voi kehittyä asianmukaisesti. Lainsäädäntöön olisi siten lisättävä viranomaisille mahdollisuus käyttää rekisteröityjen dataa vähintäänkin viranomaisten omien sähköisten palvelujen kehittämiseksi.

Sähköisten palvelujen kehittäminen käyttäjien henkilötietoja hyödyntämällä katsotaan yleisesti kuuluvan rekisterinpitäjän oikeutetun edun piiriin käsittelyperusteista puhuttaessa. Julkisella sektorilla oikeutettu etu ei lähtökohtaisesti ole käytettävissä ja oikeuskirjallisuudessa (ks. Tomi Voutilainen: Digitaalisten palvelujen sääntely 2023, s. 91) on katsottu, että muun muassa viranomaisen käyttämän palvelun kehittäminen hyödyntämällä palveluun kuuluvia henkilötietoja

kuuluisi 6(1)(e) artiklan mukaisen yleistä etua koskevan tehtävän suorittamisen piiriin. Tämä ei kuitenkaan ilmene suoraan laista tai sen esitöistä ja on sen vuoksi altis erilaisille tulkinnoille.

Esimerkiksi tietosuojalain 4 §:n 1 momenttiin olisi syytä kirjata mahdollisuudesta hyödyntää viranomaisten asiakkaiden henkilötietojen käyttämisestä sähköisten palvelujen kehittämiseen. Tämä selkeyttäisi vallitsevaa oikeustilaa.

Ennakoiva palveluiden tarjoaminen

Ennakoiva oppilashuolto on esimerkki tilanteesta, jossa palvelun perustavoitteena on tukea oppijoiden hyvinvointia ennakkolisella toiminnalla, jota voitaisiin nykyistä vahvemmin tukea dataa hyödyntäen. Opetus- ja kulttuuriministeriön toimeksiantona valmistuneessa tuoreessa Sujuva kasvatusta- ja koulutustietojen hyödyntäminen -raportissa suositellaankin selvitettäväksi konkreettiset tilanteet, joissa lasten ja oppijoiden tietojen profilointi olisi perusteltua oppimisen arvioinnissa ja ohjaamisessa, sekä konkreettiset kohteet, joissa lasten, oppilaiden ja opiskelijoiden tietoja on tarpeen käsitellä profiloinnin avulla sekä arvioida, sisältyykö siihen tietosuoja-asetuksen tarkoittamaa automaattista päätöksentekoa. Ko. raportti ehdottaa myös tehtäväksi tarvittavat käsittelyn mahdollistamiseksi tarkoittavat muutokset lainsäädäntöön siltä osin kuin kysymys on muusta kuin hallintoasiassa tehtävästä automaattisesta ratkaisusta. (Sujuva kasvatusta- ja koulutustietojen hyödyntäminen - selvitysryhmän loppuraportti; Jaakko Kauko, Jaakko Penttinen, Maarit Rötö, Tomi Voutilainen, Opetus- ja kulttuuriministeriön julkaisu: 2024:17)

Varhaiskasvatuspalveluiden ennakoiva tarjoaminen on ei ole tietosuojanäkökulmasta ongelmatonta. Toisin kuin perusopetus, joka on oppivelvollisuuteen perustuvaa, varhaiskasvatukseen osallistuminen ei ole velvoittavaa pakollista esiopetusta lukuun ottamatta. Se, että millä käsittelyperusteella Helsingin kaupunki voi ennakoivasti ottaa yhteyttä lapsiperheisiin ja ilmoittaa esimerkiksi lähitöillä olevista päiväkodeista tai niiden vapaista paikoista ei ole yksiselitteistä. Samalla kuitenkin tästä palvelusta on monille vanhemmille hyötyä – etenkin jos vanhemmat ovat maahanmuuttajataustaisia ja Suomessa toteutettava varhaiskasvatus ei ole kaikilta osin selvää.

Varhaiskasvatusta koskevassa erityislainsäädännössä olisi siten hyvä säätää myös kuntien mahdollisuudesta tarjota varhaiskasvatuspalveluja ennakoivasti, jotta tämän hyödyllisen palvelun henkilötietojen käsittely olisi yksiselitteisesti sallittua.

Toisilaki

Laki sosiaali- ja terveystietojen toissijaisesta käytöstä on kokonaisuutena haastava lain soveltajalle. Laki ei ole sisällöllisesti tai käsitteiltään täysin johdonmukainen ja lakia on muutettu

valiokuntavaiheessa niin merkittävällä tavalla, että sen sisällön ymmärtämiseksi tulee lain lisäksi lukea sitä koskevaa hallituksen esitystä sekä valiokunta-asiakirjoja ristiin. Toisiolaki on tarkoitukseltaan hyvä, mutta se tulisi ottaa kokonaisuudessaan uudelleen tarkasteltavaksi sen sisäisen epä johdonmukaisuuden ja tulkinnanvaraisuuden vuoksi.

Lakiin on kirjoitettu tietolupaviranomaisen ja omien tietojensa osalta lupia myöntävien rekisterinpitäjien veloitteita samoihin pykäliin osin eri tavoin myös niissä kohdissa, joissa edellä mainittujen tulisi toteuttaa samaa tehtävää. Ks. esim. toisiolain 14 §:n 1 ja 2 momentit. Samaa tehtävää tai toimintoa koskevaa sääntelyä on myös hajautettu lain eri lukuihin. Esimerkiksi toisiolain 14 § ja 51 §, jotka molemmat säätelevät osiltaan tietojen esikäsittelyä, mutta eivät viittaa toisiinsa. Laissa tulisi selkeästi eritellä tietolupaviranomaisena toimivan Findatan ja yksittäisen rekisterinpitäjän tehtävät, oikeudet ja velvollisuudet sekä keskittää määrättyä säänneltävää teemaa koskevat pykälät samoihin lukuihin, jotta lain ymmärrettävyys parantuisi. Tässä yhteydessä myös lain perustelut tulisi selkeyttää.

Lokitetöjen käsittelyä koskeva 19.3 § on kirjoitettu käytännössä saman sisältöiseksi kuin asiakastietolain lokitetöjen sisältöä koskevat pykälät, mikä muodostuu ongelmalliseksi tietojen käyttötarkoitusten ollessa selvästi erilaiset. Erityisesti tietojohdantarkoituksissa voidaan käsitellä suuren henkilömäärän tietoja, jolloin lokitiedostot kasvavat kooltaan ja menettävät informaatioarvoaan. Esimerkiksi selvitetessä määrätyn terveysaseman potilaiden profiilia esimerkiksi perussairauksien osalta käsitellään useiden henkilöiden tietoja koneellisesti, ilman että ihminen niihin perehtyisi tuotettuja lokirivejä syntyy lukuisia. Toisio laissa ei myöskään säädetä rekisteröidyn oikeudesta omien sosiaali- ja terveydenhuollon asiakastietojensa käsittelystä koskevien lokitetöjen tarkastamiseen eksplisiittisesti.

Erityisen haastavaksi on koettu 41 §:n tietojohdantamista koskeva sääntely. Tulkintahaasteita on aiheuttanut erityisesti se, miten tulisi käsitellä tietojohdantamisen perusteella syntyviä tietoaineistoja, jotka ovat syntyneet tunnistettavia tietoaineistoja käsittelemällä tietojohdantamisen tarkoituksessa, mutta joiden lopputuloksena on anonymisoitua tietoa/aggregoitua tilastotietoa. Tällaisten tietojen hyödyntämiselle ja jakamiselle on usein käytännön toiminnassa tarvetta. Epäselvää on ollut, tuleeko tällaista tietoa käsiteltäessä edelleen huomioida toisiolain sääntely ja luovuttaa tällainenkin aineisto Findatan anonymisoitavaksi jos sitä halutaan jakaa organisaation ulkopuolelle, vai voidaanko katsoa, ettei kyseinen tieto ole enää henkilötietoa siten, kuin tietosuojasetuksessa määritellään, jolloin tiedon käsittelyyn ei enää sovellettaisi tietosuojasetusta. Yleisesti ottaen toiveena olisi, että toisiokäytön osalta enemmän vastuuta voitaisiin antaa rekisterinpitäjälle, ja pienentää Findatan roolia. Rekisterinpitäjän pitää voida tuottaa anonymisoituja aineistoja itse, joita voidaan julkisuuslain mukaisesti jakaa organisaation ulkopuolelle. Jos rekisterinpitäjälle annetaan enemmän roolia, toisiolaki istuu paremmin yhteen myös julkisuuslain systematiikan kanssa. Jos kaikessa sote-sektorin henkilötietojen anonymisoinnissa/aggregoinnissa tulee mennä Findatan kautta, tulee prosessista usein liian raskas, kallis ja aikaa vievä. Viranomaisen tulisi voida julkisuusperiaate huomioiden tuottaa esim. erilaisia tietoaineistoja ja tilastoja julkisesti jaettavaksi myös sotesektorilla.

Potilastietojen käsittelystä tietojohdamisessa säädetään toisiolain 41.3 §:ssä. Kyseinen sääntely asettaa Helsingin kaupungin ja Uudenmaan hyvinvointialueet eriarvoiseen asemaan muihin hyvinvointialueisiin nähden, koska toisin kuin muut hyvinvointialueet, ne eivät voi tehdä tietojohdamista koko maakunnan alueen tiedoilla. Uudenmaan alueen tietojen käyttäminen on välttämätöntä, jotta voidaan toteuttaa Uusimaalain 1.2 §:ssä julkituotu lain tarkoitus edistää ja ylläpitää väestön hyvinvointia ja terveyttä sekä varmistaa yhdenvertaiset, yhteen toimivat ja kustannusvaikuttavat sosiaali- ja terveydenhuollon palvelut Uudellamaalla.

Tietojen luovuttaminen tieteelliseen tutkimukseen ja tilastointiin toisiolain perusteella edellyttää tietolupaa. Jos tietolupahakemus vastaa vain yhden rekisterinpitäjän tietoja, vastaa rekisterinpitäjä tietolupapäätöksestä. Tietolupahakemuksen koskiessa usean rekisterinpitäjän tietoja tietolupapäätöksen tekee Findata. Tiedot luovutetaan käsiteltäväksi aina tietoturvalliseen käyttöympäristöön – ensisijaisesti Findatan ylläpitämään käyttöympäristöön. Mikäli tiedot luovutettaisiin anonymisoituina, vastaa Findata aina anonymisoinnista ja tietojen luovuttamisesta.

Käytäntö on osoittanut, että Findatan rooli tietolupa perustuvien tietojen luovuttamisessa hidastaa ja estää lääketieteellistä tutkimusta sekä nostaa merkittävästi lääketieteellisen tutkimuksen kustannuksia. Toisiolakia tulisi muuttaa siten, että yksittäinen rekisterinpitäjä voi arvioida tutkijan käyttämän järjestelmän turvallisuuden, voi tehdä tietolupapäätöksen omien tietojensa osalta myös, kun tietolupa koskee useiden rekisterinpitäjien tietoja ja anonymisoida tiedot tarvittaessa itse.

Hallitusohjelmassa toisiolain osalta on asetettu seuraava tavoite: ”Ratkaistaan sote-tiedon toisiolain ja -käytön haasteet niin, että voidaan edistää Suomessa tehtävää tutkimusta ja mahdollisuutta hyödyntää tietoa. Arvioidaan Findatan rooli.” On ehdottoman tärkeää, että toisiolain ongelmat ratkaistaan hallitusohjelmassa asetetun tavoitteen mukaisesti osana tietosuojalainsäädännön kokonaisuudistusta.

Hätäkeskustoiminnasta annetun lain mukainen rekisterinpitäjä

Yksittäisistä lainkohdista lain soveltajan näkökulmasta monimutkaisiksi on koettu esimerkiksi asiakastietolain 16 § (rekisterinpitäjän vastuut palvelunantajan toiminnan päätyttyä) ja hätäkeskustoiminnasta annetun lain 16a §, joka koskee rekisterinpitäjyyttä ja vastuunjakoa. Myös julkisuuslain uudistuksessa on ehdotettu käytännössä hankalasti toteutettavia säädöksiä, kuten omia tietoja koskeva sääntely ja hätäilmoitustallenteita koskeva ehdotus.

Käsite ”henkilörekisterit”

Kansallinen erityislainsäädäntö nojaa usein ”henkilörekistereihin”. Tietosuoja-asetuksen systematiikassa ”rekisterit” ovat puolestaan marginaalissa asetuksen keskittyessä säätelemään henkilötiedon käsittelyä eri tarkoituksiin. Rekisteri-ajattelu voi aikaansaada usein tilanteen, että etsitään ”rekisteriä” ja kun sitä ei ole löydettävissä ymmärretään, ettei tietosuojalainsäädäntö sovellu, vaikka tosiasiasa henkilötietoja käsitellään tietosuoja-asetuksen määrittelemällä tavalla.

Onko kansallisen erityislainsäädännön henkilötietojen käsittelyä koskevien säännösten havaittu estävän tietojenvaihdon sellaisten viranomaisten (tai julkista hallintotehtävää hoitavien) välillä, jotka tarvitsevat tietoja lakisääteisten tehtäviensä hoitamista tai julkisen palvelun tarjoamista varten?

Kyllä

Jos on, mistä säännöksistä on tarkalleen ottaen kyse ja miten ne estävät viranomaisten välistä tietojenvaihtoa?

Sosiaali- ja terveydenhuollon tietojen luovuttaminen poliisille

Sosiaalihuollon asiakastietojen luovuttamisesta poliisille säädetään uuden asiakastietolain 63.2 ja 63.3 §:ssä. Terveydenhuollon potilastietojen luovuttamisesta poliisille on sen sijaan säädetty esitutkintalain 7 luvun 8 §:ssä, jossa on viitattu oikeudenkäymiskaaren 17 luvun 14 §:ään, jossa säädetään lääkärin ja muun terveydenhuollon ammattihenkilön todistamiskiellosta. Selvyyden vuoksi olisi syytä säätää potilastietojen luovuttamisesta poliisille asiakastietolaissa samassa yhteydessä kuin sosiaalihuollon asiakastietojen osalta. Nykyinen malli, jossa tiedonsaantioikeus on yhdentyypisten tietojen osalta sijoitettu yhteen lakiin ja toisen toiseen, on omiaan johtamaan epäselvyyteen lain sisällöstä. Esimerkiksi Korkein hallinto-oikeus on katsonut ratkaisustaan, että terveydenhuollon asiakkaana olevan henkilön henkilöllisyys on salassa pidettävä, sillä se paljastaa potilassuhteen.

Olisi myös syytä selvyyden vuoksi säätää laissa erikseen potilaan hoidosta kertyvien lokitietojen luovuttamisesta poliisille saman sisältöisesti kuin niin sanottujen varsinaisten potilas- ja asiakastietojen osalta. Sääntelyn tulisi olla lähtökohtaisesti yhdenmukaista potilastietoja koskevien tietojen luovutusten kanssa, sillä lokitiedoista paljastuu tietoja annetuista palveluista.

Tietojen luovuttaminen Helsingin sosiaali- terveys- ja pelastustoimialan ja HUSin välillä

Uudellamaalla HUS-yhtymä vastaa erikoisairaanhoidon järjestämisestä. Uudenmaan erilliskäyttöön perustuva lainsäädäntö antaa potilaalle mahdollisuuden kieltää tietojensa luovuttaminen Helsingin sosiaali- terveys- ja pelastustoimialan ja HUSin välillä. Tämä asettaa Helsingin eriarvoiseen asemaan Uudenmaan ulkopuolisten hyvinvointialueiden kanssa, sillä em. hyvinvointialueilla ei tällaista kieltä oikeutta perusterveydenhuollon ja erikoisairaanhoidon välillä ole. Saumattomien hoitoketjujen ja potilasturvallisuuden takaamiseksi Helsingin sosiaali- terveys- ja pelastustoimialalla on oltava

mahdollisuus käsitellä myös erikoissairaanhoidon tietoja hoidon edellyttämässä laajuudessa ilman kiello-oikeutta, kuten muillakin hyvinvointialueilla.

Laki eläinten hyvinvoinnista

Uusi laki eläinten hyvinvoinnista sisältää seuraavan ristiriidan. Lain 80 §:n mukaan valvontaviranomaisella on oikeus saada salassapitosäännösten estämättä eläinten hyvinvointisäädösten valvonnan suorittamiseksi välttämättömät, eläinten pitoon tai kohteluun liittyvät tiedot ja asiakirjat eläinten omistajalta ja pitäjältä sekä muulta, jota tässä laissa tai Euroopan unionin lainsäädännössä säädettyt velvoitteet koskevat.

Lain 107 §:ssä on lueteltu ne asiat, jotka valvontatilanteessa saa tallentaa rekisteriin. Ristiriidan 80 §:n kanssa aiheuttaa 107 §:n kohta 8: muut sellaiset 1–7 kohdassa tarkoitettuja tietoja vastaavat eläinten hyvinvointisäädösten mukaiset valvonnan kannalta välttämättömät tiedot, jotka eivät sisällä luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 2016/679 (yleinen tietosuojasetus) 9 tai 10 artiklassa tarkoitettuja tietoja.”

Valvontatoimessa on välttämätöntä kirjata tietyissä tilanteissa esimerkiksi henkilön terveyntilaan liittyviä tietoja. Tällä hetkellä laki kuitenkin kieltää sen. Asiaan on tiedusteltu kantaa ministeriöstä, eivätkä heidän asiantuntijansa osanneet sanoa, miksi tällainen rajausta on tehty ja myönsivät, että tällaisia tietoja on tarpeen käsitellä. Tähän siis kaivattaisiin nopeaa muutosta.

Laki Kansallisesta koulutuksen arviointikeskuksesta

Opetuksen järjestäjä on veloitettu osallistumaan järjestämänsä koulutustoiminnan arviointiin. Lainsäädännöstä ei kuitenkaan ilmene, saavatko tiedot jäädä KARVI:lle (Kansallinen Koulutuksen Arviointikeskus) kuinka pitkäksi aikaa käsittelyn jälkeen ja muodostuuko niistä rekisteri, josta KARVI on rekisterinpitäjä.

Kansallisesta koulutuksen arviointikeskuksesta annetun lain 6 §:ssä säädetään, kansallisen koulutuksen arviointikeskuksen (Karvi) oikeudesta saada salassa pidettäviä henkilötietoja muun muassa varhaiskasvatuksen ja koulutuksen tuottajilta. Samassa pykälässä myös säädetään Karvin oikeudesta säilyttää tietoja korkeintaan yksi vuosi siitä, kun tietoja ei enää tarvita arviointitoimintaan. Samassa laissa myös säädetään Karville tietojen käsittelyyn liittyviä tehtäviä, kun taas edellä mainittujen tietojen luovuttajien ainoa tehtävä on luovuttaa tietoja Karvin käyttöön. Tähän viittaisivat myös lain esityöt (ks. SiVM 1/2020 vp, s.3), missä henkilötietojen käsittelyn käsittelyperusteen katsotaan olevan Karvin lakisääteisen veloitteen. Tämä viittaisi siihen, että Karvi

toimii itsenäisenä rekisterinpitäjänä, jonka tehtävät on säädetty laissa. Kuitenkin lain 7 b §:ssä säädetään yhteisrekisterinpitäjyydestä varhaiskasvatuksen laadunarviointijärjestelmään tietoja luovuttavan tahon ja Karvin välillä. Lain esitöistä (ks. HE 99/2019 vp, s. 12) voisi päätellä, että tämän yhteisrekisterinpitäjyyden olisi tarkoitus kattaa myös muut opetuksen järjestäjät, sillä nämä on perusteluissa mainittu yhteisrekisterinpitäjyyttä koskevassa kohdassa.

Olisi selvyuden ja rekisteröityjen oikeuksien tehokkaan toteuttamisen vuoksi perusteltua säätää, että henkilötietojen käsittely Karvin toiminnassa tapahtuu Karvin lakisääteisiä tehtäviä varten Karvin ollessa rekisterinpitäjä Karville luovutettujen tietojen osalta.

Onko kansallisessa erityislainsäädännössä tunnistettu muita esteitä julkisen palvelun tarkoituksenmukaiselle järjestämiselle?

Ei

Jos kyllä, mistä säännöksistä on tarkalleen ottaen kyse ja miten ne estävät julkisen palvelun tarkoituksenmukaista järjestämistä?

-

YLEISEN TIETOSUOJA-ASETUKSEN SALLIMAN KANSALLISEN SÄÄNTELYLIKKUMAVARAN KÄYTTÖ

Onko yleisen tietosuoja-asetuksen sallimaa kansallista sääntelyliikkumavaraa käytetty tarkoituksenmukaisella tavalla viranomaisen tiedon liikkumisen tai julkisen palvelun järjestämisen näkökulmasta?

Ei

Jos ei, tulisiko kansallista sääntelyliikkumavaraa käyttää enemmän?

Jos kyllä, miltä osin ja miten liikkumavaraa tulisi käyttää nykyistä enemmän julkisen palvelun järjestämisen näkökulmasta?

Edistyneen analytiikan hyödyntäminen henkilötiedon käsittelyyn ja ennakoivaan toimintaan

Hallintolakiin ja tiedonhallintalakiin tehdyt muutokset, jotka mahdollistavat automaattiset hallintopäätökset asioissa, jotka eivät edellytä viranomaisen harkintaa, ovat hyvä uudistus. Automaattiset hallintopäätökset mahdollistavat erilaisten massapäätösten tuottamisen tehokkaasti ja säästää henkilöstöresursseja asioihin, joissa tosiasiaa tarvitaan ihmisen työpanosta.

Automaattisia hallintopäätöksiä on kuitenkin mahdollista käyttää ainoastaan niissä asioissa, joissa päätöksen tuottaminen voidaan pelkistää kerran hyväksytyiksi käsittelysäännöiksi. Lisäksi käsittelysääntöjen dokumentointiin ja julkaisuun liittyvä velvoite on luonteeltaan raskas menettely ja nämä velvoitteet rajaavatkin automaattisten hallintopäätösten käyttöalaa. Tämä sulkee erilaisten

koneoppimiseen perustuvien ratkaisujen käytön automaattisten hallintopäätösten ulkopuolelle. Helsingin kaupunki pitää perusteltuna, että oikeusministeriö selvittää koneoppimiseen perustuvien ratkaisujen mahdollistamista automaattisessa päätöksenteossa, sillä koneoppimisella olisi suuri potentiaali tehostaa hallintotoimintaa ja automaattista päätöksentekoa.

Esimerkiksi palvelutarvetta arvioivien tai ennakoivien, proaktiivisesti tarjottavien julkisten palveluiden kehityksessä on jo Helsingin kaupungillakin törmätty kansallisen lainsäädännön osalta haasteeseen erityisesti automatisoituihin yksittäispäätöksiin liittyen (ks. esim. apulaistietosuojavaltuutetun päätös 6482/186/2020). Asian automaattinen käsittely, kuten profilointi, voidaan mahdollistaa paitsi rekisteröidyn suostumuksella, myös kansallisella lainsäädännöllä rekisteröidyn oikeudet huomioiden.

Ennakoivilla palveluilla olisi merkittävä potentiaali paitsi palveluprosessien sujuvoittamiseksi asiakkaiden näkökulmasta palveluiden saatavuuden ja saavutettavuuden helpottamiseksi sekä kaupungin näkökulmasta palveluiden kustannusvaikuttavuuden kehittämiseksi. Aivan erityisen suuri kustannusvaikuttavuuspotentiaali on terveystietosuojien ennakoivassa tarjoamisessa, mikäli tarvittavaa kansallista sääntelyä saataisiin asetettua. Sote-palveluiden ennakoivassa tarjoamisessa tämä vaatisi muutosta esimerkiksi asiakastietolakiin, jossa voitaisiin säätää tietosuojasetuksen 22 artiklan 4 kohdan edellyttämällä tavalla poikkeuksesta automatisoitujen yksittäispäätösten kieltoon.

Lisäksi olisi syytä tarkentaa toisilain sääntelyä siitä, miten rekisterinpitäjä voi käyttää omassa rekisterissään olevia tietoja koneoppivien algoritmien kouluttamiseen, sillä tällä on huomattava potentiaali parantaa ennakoivan terveydenhuollon toimintaa. Vastaava säännös tulisi ulottaa koskemaan myös muita julkisen sektorin hallussa olevia erityisiä henkilötietoja ja julkisuuslain mukaan salassa pidettäviä tietoja, sillä tämä mahdollistaisi kohdennetut palvelut myös muin muilla toimialoilla, kuten työllisyyspalveluissa ja oppilashuollossa.

Puuttuuko kansallisesta erityislainsäädännöstä säännöksiä, jotka mahdollistaisivat viranomaisten välisen tiedon liikkumisen siten, että julkinen palvelu voitaisiin järjestää tarkoituksenmukaisella tavalla. Jos kyllä, mistä puutteesta ja palvelusta on tarkalleen ottaen kyse?

Ei

Onko kansallisessa erityislainsäädännössä käytetty sääntelyliikkumavaraa tarpeettomasti? Jos on, miltä osin ja mistä säännöksistä on tarkalleen ottaen kyse?

Ei

YLEISET KOMMENTIT

Puuttuuko väliraportin liitteestä 1 lakeja, joita olisi hyvä arvioida kokonaisuudistuksen yhteydessä?

Työelämän tietosuojalaki

Väliraportissa ei mainita sanallakaan lakia yksityisyyden suojasta työelämässä. Tällä lailla on merkittävä vaikutus henkilötietojen käyttöön viranomaistoiminnassa, sillä jokainen maan virasto ja viranomaistaho ovat työnantaja.

Työelämän tietosuojalaki on kaksi vuosikymmentä vanha ja yhteiskunta, työnteon tavat sekä yleinen tietosuojalainsäädäntö ovat muuttuneet tuon kahden vuosikymmenen aikana laajasti. Olisikin hyvä, jos koko laki otettaisiin tarkasteluun sen ajantasaisuuden arvioimiseksi.

Esimerkkinä työelämän tietosuojalain tulkintavaikeuksia aiheuttavista kohdista voidaan mainita esimerkiksi se, että työelämän tietosuojalaissa asetetaan henkilötietojen käsittelyn edellytykseksi usein työntekijän suostumus, mutta yleisen tietosuoja-asetuksen mukaisen hankkiminen työntekijän asemassa olevalta henkilöltä ei vallitsevan tulkintakäytännön mukaan täytä suostumuksen vapaaehtoisuuden kriteeriä. Tätä työntekijän suostumuksen vaatimusta voisi selvyyden vuoksi tarkentaa lainsäädännössä. Suostumuksen käyttämisestä henkilötietojen käsittelyperusteena viranomaisen toiminnassa on lausuttu tässä lausunnossa jo ylempänä.

Lisäksi huumausainetestien teettämistä ja niistä työnantajalle tiedon antamista ja tiedon tallentamista koskeva sääntely olisi hyvä arvioida nyky maailman realiteetteja, kuten sähköinen tietojen käsittely huomioiden. Myös rikosrekisteritietojen käsittelyä koskeva sääntely olisi syytä uudistaa yhdessä lasten kanssa työskentelevien rikostaustan selvittämisestä annetun lain ja lasten kanssa toimivien vapaaehtoisten rikostaustan selvittämisestä lain kanssa sääntelyn yhteneväisyyden takaamiseksi.

Tarkasteltaessa työelämän tietosuojalakia tulisi se tehdä yhdessä myös sähköisen viestinnän palveluista annetun lain viestinnän välitystietojen käsittelyä koskevan sääntelyn kanssa.

Työnantajana toimivan yhteisötilaajan oikeus käsitellä viestinnän välitystietoja tietoturvaperusteella

Sähköisen viestinnän palveluista annetun lain 138 §:n ja 272 §:n mukaan viestinnän välittäjä ja lisäarvopalvelun tuottaja sekä niiden lukuun toimiva voivat käsitellä viestinnän välitystietoja viestintäverkkojen tietoturvan toteuttamiseksi. Yhteisötilaajalla ei kuitenkaan ole säädetty tätä oikeutta, vaan yhteisötilaaja voi sähköisen viestinnän palveluista annetun lain mukaan käsitellä viestinnän välitystietoja viestintäverkon käyttäjän väärinkäytöksen tai liikesalaisuuden paljastamisen ehkäisemiseksi. Yhteisötilaajan edellä mainittujen välitystietojen valvomista koskevien oikeuksien käyttäminen edellyttää laajan suunnittelu- ja huolellisuusvelvoitteen läpikäymistä, yt-menettelyä sekä ennakoilmoitusta tietosuojavaltuutetulle sekä lain tarkoittamia jälki-ilmoituksia.

Olisi tarpeen säätää sähköisen viestinnän palveluista annetussa laissa myös yhteisötilaajalle mahdollisuus käsitellä viestinnän välitystietoja tietoturvapoikkeaman selvittämiseksi samaan tapaan, kuin viestinnän välittäjälle ja lisäarvopalvelun tuottajalle on säädetty. Tämä mahdollisuus toimisi varoventtiilinä, joka mahdollistaisi selkeiden tietoturvapoikkeaminen selvittämisen niissäkin tapauksissa, kun yhteisötilaaja ei ole suunnitellut viestinnän välitystietojen käsittelyä liikesalaisuuksien paljastamista tai viestintäverkon käyttäjän väärinkäytöksen paljastamisen vuoksi. Tämä olisi tarpeen, sillä nykyinen sääntely koskee erityisesti yhteisötilaajan tietoverkon luvallisten käyttäjien, monesti yhteisötilaajan työntekijöiden, valvontaa mutta tietoturvapoikkeaminen havaitseminen ja tutkiminen kohdistuvat lähtökohtaisesti luvattomaan järjestelmään tunkeutumiseen.

Koska kyse ei olisi yhteisötilaajan verkon käyttäjinä toimivien työntekijöiden valvonnasta, olisi tarpeen säätää, että tietoturvapoikkeamia koskevien viestinnän välitystietojen käsittely olisi perustellusta syystä mahdollista myös ilman ennakkollista työelämän tietosuojalain 21 §:n mukaista yt-menettelyä. Rekisteröidyn oikeuksia koskevana suoja-toimenpiteinä tulisi säätää tietoturvapoikkeamien selvittämisen jälki-ilmoitusvelvollisuus tietosuojavaltuutetulle sekä rekisteröidyille, joiden tietoja on mahdollisesti samassa yhteydessä käsitelty, samaan tapaan kuin nykyisessäkin laissa.

EIDAS-asetus

EIDAS-asetuksen mukaiset tunnistautumistavat aiheuttavat hankaluuksia henkilön tunnistamisessa ja tämän tunnistautuneen henkilön tietojen yhdistämistä tämän henkilötunnuksen alla oleviin tietoihin. Jotta EIDAS-asetuksen mukainen tunnistautuminen voidaan toteuttaa kuntasektorilla, on järkevämpää toteuttaa EIDAS-asetuksen mukaisen tunnistautumisen yhdistäminen suomalaisen henkilötunnukseen keskitetysti esimerkiksi Digi- ja Väestötietovirastossa tai muussa viranomaisessa sen sijaan, että jokainen rekisterinpitäjä on itse velvollinen tekemään tämän tunnistautumisen. Nykyinen lainsäädäntö, joka asettaa tämän velvoitteen yksittäisille rekisterinpitäjille johtaa päällekkäiseen työhön eri viranomaisissa eikä ota huomioon sitä, että kunnilla ei ole edellytyksiä sellaiselle tietotekniselle työlle, jolla EIDAS-asetuksen mukainen tunnistautumistapa saataisiin yhdistettyä henkilötunnukseen.

Vaikka EIDAS-asetuksen toimeenpano on erillinen kysymys tietosuojasta, on EIDAS-asetus silti huomioitava kokonaisuudistuksessa. EIDAS-asetuksen mukaiset tunnistautumiset tulevat ensisijaisesti kohdistumaan Suomessa viranomaisiin. Mikäli EIDAS-asetuksen mukaisen tunnistautumisen varmentaminen ja yhdistäminen henkilötunnukseen jää yksittäisten viranomaisten vastuulle, on olemassa merkittävä riski siitä, että rekisteröityjen oikeudet eivät tule toteutumaan.

Rikostaustan selvittämistä koskevat lait

Laki lasten kanssa työskentelevien rikostaustan selvittämisestä, laki lasten kanssa toimivien vapaaehtoisten rikostaustan selvittämisestä ja rikosrekisterilaki sisältävät sääntelyä työntekijöiden, viranhaltijoiden ja vapaaehtoisten rikostaustan selvittämisestä. Laissa ja sen esitöissä puhutaan rikosrekisteriotteen esittämisestä työnantajalle ja sen palauttamisesta, mikä viittaa paperiseen asiakirjaan eikä suoraan taivu sähköisten asiakirjojen käsittelyyn. Perusteluina on mainittu muun muassa se, että työntekijä voi tarvita todistusta toisessa hakuprosessissa (ks. HE 3/2002 vp, s 34). Lisäksi lainsäädännön esitöissä on esitetty, ettei työnantajalla ole kyseisen lain nojalla oikeutta käsitellä erityisiä henkilötietoja (HE 3/2002 vp, s. 44), joihin rikostaustaa koskeva tieto kuuluu. Sääntely on omiaan luomaan epävarmuutta siitä, onko rikosrekisteriotetta mahdollista saada työnantajan nähtäväksi sähköisesti, sillä tämä edellyttäisi yleisen tietosuojasetuksen mukaista henkilötietojen automaattista käsittelyä esimerkiksi rikosrekisteriotetta koskevan viestin välittämiseksi ja käsittelemiseksi.

Olisikin hyvä, että edellä mainitut lait arvioitaisiin kokonaan uudelleen 2020-luvun vaatimuksia vasten.

Muut lait

Lisäksi seuraavia lakeja tulisi arvioida kokonaisuudistuksen yhteydessä: Laki sosiaali- ja terveystietojen toissijaisesta käytöstä (552/2019) ja laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä (703/2023).

Muut kommentit

Tietosuojavastaava -termi

Data Protection Officer on suomennettu tietosuojasetuksessa ”tietosuojavastaavaksi”. Tämä on saanut aikaan yleistä käsitystä, että tietosuojavastaava vastaa organisaation tietosuojasta sekä antaa sitovia ohjeita ja määräyksiä ja tekee päätöksiä henkilötiedon käsittelyn suhteen. Tosiasiassa em. vastuu ja tehtävät kuuluvat tietosuojasetuksen mukaisesti rekisterinpitäjälle, jota ”tietosuojavastaava” asetuksen mukaisesti neuvoo ja valvoo. Sana ”tietosuojavastaava” sinänsä aikaansaa merkittävästi epäselvyyksiä ja haasteita siinä, kuinka julkisten palvelujen yhteydessä tapahtuva henkilötiedon käsittely järjestetään – mikä taho sitovasti ohjeistaa ja päättää henkilötiedon käsittelystä ja vastaa siitä. Vaikka tietosuojasetusta on sovellettu jo yli kuusi vuotta em. väärinkäsitys on yhä erittäin yleinen ja mikäli ko. termiä ei muuteta, jäänee se yleiseksi tietosuojatyötä perustavanlaatuisesti hankaloittavaksi seikaksi. Ruotsinkielisessä tietosuojasetuksessa Data Protection Officer on käännetty ”dataskyddsbudeten” ja rekisterinpitäjä puolestaan ”personuppgiftsansvarig”

Julkisuuslain ja tietosuojasääntelyn yhteensovittaminen

Henkilötietojen suojassa ei sinänsä ole kysymys tietojen salassapidosta, vaikka salassapidolla suojattava etu saattaakin yksityisyyden suojan osalta olla päällekkäinen henkilötietojen suojan kanssa. Salassapito voi liittyä henkilötietojen suojaan myös siten, että salassapito voi olla säädetty henkilötietojen käsittelyn mahdollistavaksi yhdeksi suojatatoimeksi. Käytännössä tietosuojaa on kunnan toiminnassa mahdoton toteuttaa tuntematta julkisuuslain ja erityislakien useita yksityisyyttä suojaavia salassapitosäännöksiä, joten pykälien sijoittuminen merkittävään määrään eri lakeja vaarantaa yksityisyyden suojan toteutumisen käytännössä.

Julkisuus- ja salassapitolainsäädäntö kaipaisi kokonaisuudistusta, jossa säädöksiä nykyaikaistettaisiin. Tällä hetkellä tietosuojaa, salassapitoa, tietojen luovuttamista ja teknisiä käyttöyhteyksiä koskeva lainsäädäntö on niin pirstaleista ja vaikeaselkoista, että sen hallitsemiseen ei monella organisaatiolla ole resursseja. Tämä näkyy erityisesti tietojärjestelmähankkeissa ja paitsi aiheuttaa kustannuksia ja viivästyksiä myös vaarantaa tietosuojan tosiasiallisen toteutumisen. Liian vaikeaselkoinen lainsäädäntö jää helposti noudattamatta. Myös terminologiaa tulisi yhdenmukaistaa. Pirstaleinen tietosuoja- ja salassapitolainsäädäntö koskee erityisesti arkaluonteisia henkilötietoja, vaikka perustuslakivaliokunnan lausuntojen (PeVL 14/2018 vp s.6 ja PeVL 71/2018 vp s.3) mukaan arkaluonteisten henkilötietojen käsittelyä koskevan sääntelyn kohdalla on syytä pyrkiä selkeään ja ymmärrettävään lainsäädäntöön.

Julkisuuslain 16 §:n 3 momentti, joka koskee tietojen luovuttamista viranomaisen henkilörekistereistä, aiheuttaa käytännön työssä tulkintaongelmia. Saman pykälän 4 momentti, jonka mukaan tietojen antamisesta teknisen rajapinnan ja katseluyhteyden avulla säädetään julkisen hallinnon tiedonhallinnasta annetussa laissa kuvastaa hyvin säädösten hajaantumista. Tietojen luovuttamista koskevia pykäläiä tulisi muuttaa siten, että niissä käytetään johdonmukaisesti yleisen tietosuojasetuksen ja tietosuojalain käsitteitä.

Nykyisen lainsäädännön mukaan esimerkiksi henkilön omia tietoja koskevia tietopyyntöjä on mahdollista tehdä viranomaiselle sekä julkisuuslain 12 §:n että tietosuoja-asetuksen 15 artiklan nojalla, jolloin tietopyyntöjä koskevat eri säännökset menettelyineen ja määräaikoineen. Määrätyillä toimialoilla erityislainsäädäntö mahdollistaa vielä muitakin perusteita omien tietojensa pyytämiseen. Viranomaisen on tarvittaessa selostettava tiedon pyytäjälle eri tiedonsaantioikeuksia koskevat säännökset sen selvittämiseksi, minkä säännöksen perusteella tietoja halutaan pyytää. Viranomaisen neuvontavelvollisuuteen kuuluu erojen selostus ja tiedonpyytäjälle edullisemman tiedonsaantioikeuden tarjoaminen. Asia on kuitenkin asiakkaalle vaikeasti ymmärrettävä eikä aina ole selvää kumpi tiedonsaantisäännös on edullisempi, koska asiakirjoista perittäviä maksuja ja muutoksenhakua koskevat määräykset ovat eri tapauksissa erilaisia.

Käynnissä oleva julkisuuslain päivitys tulisi kytkeä tiiviisti myös tietosuoja-sääntelyn kokonaisuudistukseen ja julkisuuslakia päivittää laajalti tarvittavin osin.

Ennakoivan palvelutuotannon mahdollistaminen

Julkisten palveluiden tuottajat kohtaavat haasteita myös erityisesti asiakaslähtöisten palveluiden kehittämisessä tilanteissa, joissa lainsäädäntöön pohjaavat siilomaiset palveluprosessit törmäävät tavoitteeseen kehittää asiakas (ei organisaatio) -lähtöisiä palvelupolkuja, joissa tieto liikkuu joustavasti. Erityisesti paljon palveluita käyttävien asiakkaiden asioinnin helpottaminen ja palveluiden oikea-aikainen tarjoaminen suhteessa asiakkaan tarpeeseen, voi muodostaa uudenlaisia palveluntarjoamisen polkuja ja kokonaisuuksia (esim. elämäntapahtumalähtöisyys) perinteisen asioinnin rinnalle. Esimerkkinä tästä voisi toimia työllisyys-, sosiaali- ja terveyspalveluiden yhteistyö asiakkaan monialaisiin tarpeisiin vastaamiseksi ja/tai viranomaisaloitteinen toiminta (ennakointi) asiakkaan tarpeisiin vastaamiseksi.

Seurauksena käytännössä on kuitenkin epäselvyyksiä lakien toimeenpanossa mm. tiedon liikkumisen ja -käsittelyn näkökulmasta, ja siten mahdollisuuksissa tarjota aidosti sujuvampaa palvelua asiakkaalle. Kyseisen kaltainen monialainen palvelutuotanto ja tarjonta (dataa ja mahdollisia uusia teknologioita hyödyntäen) vaatii lisäpanostuksia myös kansalliselta tasolta sääntelyn selkeyttämiseen ja toimeenpanoon liittyen.

Näistä syistä tietosuojalainsäädännön kokonaisuudistushanke tulisi tiukasti integroida osaksi mm. diginorminpurun valittuja teemoja (esim. automaation ja tekoälyn hyödyntäminen tai viranomaisaloitteinen toiminta) sen sijaan, että hanke rajaa nämä teemat tarkastelun ulkopuolelle.

Kansallinen ohjaus ja tukintojen yhdenmukaisuus

Kansallisesti ja julkishallinnolle olisi hyvä, että tietosuojaan muodostuisi kansallisten viranomaisten yhteistyömalli, joka tukisi palveluiden tarjoamista sekä kehittämistä. Viranomaistyönä tehtävät objektiiviset ennakkoarvioinnit laajalti käytetyistä palveluista tai muutoin merkittävistä ratkaisumalleista niin tietosuojan, tietoturvan kuin riskienhallinnankin näkökulmasta tulisivat tarpeeseen. Tällä toimintamallilla voitaisiin vähentää saman työn tekemistä ja parantaa arviointien laatua, koska kaikilla toimijoilla ei ole mahdollista saada erikoisosaamista arviointeihin.

Helsingin kaupunki on havainnut, että tietosuojavaltuutetun toimistosta on usein vaikea saada ohjausta lainsäädännön tulkintatilanteissa. Tietosuojaa koskevien vaikutusten arviointien ennakkokuulemiset tietosuojavaltuutetun toimistossa ovat usein venyneet tietosuojasetuksen 36 artiklassa säädetystä kahdeksan viikon, monimukaisissa tapauksissa 14 viikon, määräajoista. Kansallisesti olisi tarvetta toimijalle, jolla olisi resurssit neuvoa ja tukea kuntia tietosuojasääntelyn soveltamisessa ja tuottaisi myös kansallisesti linjaavaa ohjeistusta erityisesti kansallisen tietosuojasääntelyn osalta. Tulkintaepäselvyydet ja tulkinnan jääminen kuntien vastuulle pahimmillaan merkittävästi hidastaa digitaalisten palveluiden kehittämistä riskien ollessa liian suuret investoinneille. Vastuuta laintulkintaan uudenlaisissa palvelukehitystilanteissa ei voi säilyttää

myöskään vapaamuotoisille verkostoille, jotka ovat usein vain muutaman aktiivisen toimijan varassa, vaan tulkintaa pitää tehdä kansallisesti viranomaisen taholta (erillinen elin). Verkostojen tulkinnasta ei voi tulla kansallista tulkintaa, johon kaikki toimijat voivat vedota palveluja kehitettäessä.

Yhdenmukaisia tulkintoja voisi vahvistaa kansalliselle valvontaviranomaiselle asetettavalla velvollisuudella antaa rekisterinpitäjälle ennakkoratkaisu rekisterinpitäjän suunnittelemastä henkilötietojen käsittelystä samaan tapaan, kuin nykyisin verohallinnolta voi saada sitovan ennakkoratkaisun. Tämä lisäisi oikeusvarmuutta rekisterinpitäjien voidessa luottaa tietosuojavaltuutetun ennakkoratkaisuun toimintaansa suunnitellessaan. Tämän hetkinen tietosuoja koskevan vaikutusten arvioinnin ennakkokuuleminen ei vastaa tähän tarpeeseen, sillä lain mukaan tietosuojavaltuutetun tulee ottaa kantaa ainoastaan vaikutusten arvioinnissa suunniteltuihin henkilötietojen käsittelyn suojatoimenpiteiden riittävyteen ja ennakkokuuleminen on rajattu ainoastaan korkean riskin henkilötietojen käsittelyyn.

Kunnat käyttävät samankaltaisia tietojärjestelmiä samantapaisten henkilörekisterien henkilötiedoille. Koska tietosuojavelvoitteet ovat samat, olisi hyödyllistä voida hankkia valmiiksi tietosuojan kannalta asianmukaisiksi arvioituja digipalveluita. Tällaisia tietosuojan kannalta riittäviksi sertifioituja digipalveluita hankkiessaan kunta voisi luottaa noudattavansa tietosuojasäädöksiä ja sen oma tietosuoja-arviointi olisi suoraviivaista tehdä. Tietosuojalainsäädäntö mahdollistaa kansallisen viranomaisen hyväksymät käytännesäännöt, jotka voisivat olla yksi keino rakentaa yhteisiä malleja.

Helsingin kaupunki katsoo yhteistyötä ja yhdenmukaisuutta koskevien määräysten käytännössä johtaneen siihen, että ohjauksen ja neuvonnan saaminen tietosuojavaltuutetun toimistosta vaikeissa tulkintatilanteissa on vaikeutunut. Valvontaviranomainen on usein pidättäytynyt antamasta ohjeita tilanteissa, joissa se katsoo tarvittavan unionin tasoisia yhtenäisiä linjauksia. Helsingin kaupunki katsoo tämän olevan ongelmallista, sillä valvontaviranomaisen neuvontaa kaivattaisiin nimenomaan niissä tilanteissa, joissa EU-tason kannanottojen saaminen on hyvin hidasta. Rekisterinpitäjät joutuvat kaupungin mukaan tekemään tulkintoja ilman riittävää ohjausta, mikä johtaa tietosuojan toteutumisen kannalta huonoon lopputulokseen.

Euroopan tietosuojaneuvoston ohjeet ovat yleisesti ottaen hyödyllisiä, mutta monessa ohjeessa on vältetty ottamasta kantaa juuri niihin tulkintakysymyksiin, joiden kanssa rekisterinpitäjät painivat. Ohjeistuksissa tulisi pyrkiä vahvemmin selkeyttämään, miten saa/ei saa, tai miten tulee/ei-tule toimia tulkinnanvaraisuuksien vähentämiseksi. Erityisesti pienempien kuntien resurssit seurata tarkkaan EU-tietosuojaneuvoston ohjeistuksia ovat keskimäärin vähäiset, ja suomalaiskunnilla on lisäksi kansallisia omaispiirteitä palveluiden järjestämisen ja kehittämisen sekä sitä myöden järjestelmien tarpeiden osalta.

Digitaalisten palveluiden kehittäminen sekä datan ja uusien teknologioiden hyödyt julkisten palveluiden tarjoamiselle on yksi keskeinen tekijä hallitusohjelmakirjausten taustalla. Nykytilassa

lainsäädäntö tekee tästä kehittämisestä haastavaa ja hankkeen aikana olisi erityisen tärkeää löytää ratkaisuja kehittää paitsi lainsäädäntöä, myös tukea sen soveltajille.

Palmgren Soile
Helsingin kaupunki