

# Omadata - suostumusperusteinen henkilötietojen luovutus viranomaisen rekisteristä

Emilia Laitala  
Lapin yliopisto  
Oikeustieteiden tiedekunta  
Oikeusinformatiikka  
Maisteritutkielma  
2018

## Lapin yliopisto, oikeustieteiden tiedekunta

Työn nimi: Omadata – suostumusperusteinen henkilötietojen luovutus viranomaisen rekisteristä

Tekijä: Emilia Laitala

Opetuskokonaisuus ja oppiaine: Maisteritutkielma, Oikeusinformatiikka

Työn laji: Tutkielma  Laudaturtyö  Lisensiaatintyö  Kirjallinen työ

Sivumäärä: XVIII + 73

Vuosi: 2018

### Tiivistelmä:

Omadata-termillä viitataan henkilötietojen uudelleen käsittelyyn, jonka mukaan yksilö itse hallitsee omia tietojaan. Omadatassa yksilö asetetaan tiedonhallinnan keskiöön, jonka myötä hän voi itse suostumuksellaan antaa eri toimijoille luvan käsitellä omia henkilötietojaan. Tutkielmassa perehdytään tiedolliseen itsemääräämisoikeuteen, omadataan ja omadatan mukaisen mallin soveltamiseen julkisessa hallinnossa, erityisesti rekisterinpitäjän vastuun näkökulmasta. Painopisteenä tutkielmassa on selvittää, kuinka nykyinen yleislainsäädäntö mahdollistaa julkishallinnon toimijalle oikeuden siirtää henkilötietoja suoraan yksilön suostumuksella toiselle rekisterinpitäjälle. Tutkielman metodi on pääasiallisesti lainopillinen. Tutkielmassa käytetään esimerkkinä Yhteinen tiedon hallinta –hankkeessa rakenteilla olevaa suostumushallintarekisteriä.

Yleisessä tietosuoja-asetuksessa yksilön tiedollista itsemääräämisoikeutta on vahvistettu aiemmasta. Asetuksen johdosta rekisteröidyllä on uusia oikeuksia, joiden myötä omadatan mukaista henkilötiedon hallintaa voidaan lainsäädännön nojalla jo osittain toteuttaa. Henkilötietojen luovuttamista viranomaisen rekisteristä säätelee yleislakina laki viranomaisten toiminnan julkisuudesta (621/1999) ja lisäksi asiaa koskettaa lukuisat erityislainsäädännön säädökset. Viranomaisella on korostunut velvollisuus huolehtia siitä, kenelle ja mihin tarkoitukseen henkilötietoja luovutetaan. Tämä korostunut velvollisuus ei tue omadata-mallia, jossa yksilön antaman suostumuksen jälkeen henkilötiedot tulisi luovuttaa suoraan ilman luovuttavan rekisterinpitäjän osuutta luovutus päätökseen.

Johtopäätöksenä voidaan todeta julkisuuslainsäädännön luovutussäännösten olevan ristiriidassa suhteessa omadata-mallin mukaiseen henkilötiedon luovutukseen. Julkisuuslain 13 §:n 2 momentti ja 16 §:n 3 momentti säätelevät viranomaisen velvollisuudesta selvittää tietyissä tilanteissa henkilötiedon saajan käsittelyperuste sekä tietojen suojaus. Mikäli julkishallinnon yhteinen suostumushallintarekisteri toteutuisi, olisi lailla säädettävä erikseen myös sen osalta, mitä henkilötietoja viranomaisen voisi luovuttaa vain rekisteröidyn suostumuksen perusteella. Lisäksi tulisi erikseen säätää organisaatioiden välisten rajapintojen avaamisesta. Lainsäädännön muutosten tulisi sijoittua enemmänkin yleislainsäädäntöön erityislainsäädännön sijaan, jotta pirstaleisuus henkilötietojen käsittelyn sääntelyn suhteen ei kasvaisi enää nykyisestä.

Avainsanat: omadata, tiedollinen itsemääräämisoikeus, rekisterinpitäjän vastuu, suostumus, henkilötieto, tietosuoja-asetus

Suostun tutkielman luovuttamiseen Rovaniemen hovioikeuden käyttöön

Suostun tutkielman luovuttamiseen kirjastossa käytettäväksi

# SISÄLLYS

<b>LÄHTEET</b> .....	<b>V</b>
<b>LYHENTEET</b> .....	<b>XVIII</b>
<b>1 JOHDANTO</b> .....	<b>1</b>
1.1 Tutkielman tausta, tutkimuskysymykset ja tavoite .....	1
1.2 Tutkielman rajaus ja rakenne .....	3
1.3 Tutkielman metodi .....	4
<b>2 TIEDOLLINEN ITSEMÄÄRÄÄMISOIKEUS</b> .....	<b>6</b>
2.1 Määrittely .....	6
2.2 Nykytila .....	8
2.2.1 Sääntely .....	8
2.2.2 Tiedollista itsemääräämisoikeutta suojaavat oikeudet .....	9
2.3 Tiedollisen itsemääräämisoikeuden vahvistuminen .....	12
2.3.1 Aluksi .....	12
2.3.2 EU:n yleinen tietosuojasetus .....	12
2.3.3 Suostumus .....	14
2.3.4 Oikeus tulla unohdetuksi .....	16
2.3.5 Oikeus siirtää tiedot järjestelmästä toiseen .....	16
<b>3 OMADATA</b> .....	<b>20</b>
3.1 Määritelmä .....	20
3.2 Avoin data .....	23
3.3 Suostumushallintapalvelu .....	25
3.4 Luvitus .....	27
3.5 Omadata ja lainsäädäntö .....	29
3.5.1 Yleistä .....	29
3.5.2 Hallituksen esitys liikenteen turvallisuusvirastosta .....	31
3.5.3 Koski-rekisteri .....	32
3.6 Omadatan kansainvälinen kehitys .....	33
3.6.1 Yleisesti .....	33
3.6.2 Ranska .....	34
3.6.3 Yhdistynyt kuningaskunta .....	35
3.7 Omadatan haasteet .....	37
<b>4 SUOSTUMUS KÄSITTELYPERUSTEENA</b> .....	<b>39</b>
4.1 Viranomaisen tiedon hallinta ja sähköistynyt hallinto .....	39
4.2 Viranomaisen toimintaa ohjaavan lainsäädännön ja suostumuksen suhde .....	42
4.3 Suostumukseen liittyvä tarpeellisuusvaatimus .....	46

<b>5 REKISTERINPITÄJÄN VASTUU .....</b>	<b>50</b>
5.1 Yleisesti rekisterinpitäjän velvollisuudesta ja vastuusta .....	50
5.2 Henkilötietojen luovuttaminen viranomaisen rekisteristä.....	52
5.3 Rekisterinpitäjän vahingonkorvausvelvollisuus .....	57
5.4 Julkisuuslain soveltaminen suostumushallintarekisteriin.....	60
5.5 Vastuu henkilötiedosta siirrettäessä tieto suoraan rekisterinpitäjältä toiselle .....	63
<b>6 LOPUKSI .....</b>	<b>70</b>

# LÄHTEET

## 1 Kirjallisuus:

*Aarnio Aulis*: Laintulkinnan teoria. Yleisen oikeustieteen oppikirja. Werner Söderström Osakeyhtiö, Porvoo-Helsinki-Juva 1989. (Aarnio 1989)

*Alén-Savikko Anette & Pitkänen Olli*: Rights and entitlements in information – Proprietary perspectives and beyond. Teoksessa Data protection, privacy and european regulation in the digital age. Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisu, Helsinki 2016. (Alén-Savikko & Pitkänen 2016)

*Feiler Lukas, Forgó Nikolaus, Weigl Michaela*: The EU General Data Protection Regulation (GDPR): A Commentary. Globe Law and Business Ltd expect where otherwise indicated, 2018. (Feiler – Forgó – Weigl 2018)

*González Fuster Gloria*: The Emergence of Personal Data Protection as a Fundamental Right of the EU, Springer International Publishing Switzerland 2014. (González Fuster Gloria 2014)

*Heinonen Risto*: Digitaalinen minä, Edita Helsinki 2001. (Heinonen 2001)

*Hanninen Minna, Laine Elli, Rantala Kati, Rusi Mari, Varhela Markku*: Henkilötietojen käsittely – EU-tietosuoja-asetuksen vaatimukset, Helsingin Kamari Oy, 2017. (Hanninen ym. 2017)

*Hoikkala Minna, Kultalahti Jukka, Tuomela Jukka*: Tietoyhteiskuntakehityksen informaatio-oikeudelliset haasteet, Tampereen yliopisto, 2005. (Hoikkala ym. 2005)

*Jyränki Antero*: Valta ja vapaus: valtiosääntöoikeuden yleisiä kysymyksiä. Talentum, Lakimiesliiton kustannus, Helsinki 2003. (Jyränki 2003)

*Kallasvuo Karoliina*: Omadata ja oikeus siirtää tiedot järjestelmästä toiseen. Teoksessa Oikeus, tieto ja viesti – Viestintäoikeuden vuosikirja 2015 (Toim. Korpisaari Päivi).

Helsingin yliopiston oikeustieteellinen tiedekunta, Helsinki 2015. (Kallasvuo 2015)

*Kalliojärvi Tanja*: EU:n yleinen tietosuoja-asetus: tietoturvallisuudesta henkilötietojen käsittelyssä. Pro gradu -tutkielma, Lapin yliopisto 2016. (Kalliojärvi 2016)

*Kasvi Jyrki*: Koodi on lakia vahvempi. Teoksessa: Paratiisi vai panoptikon – Näkökulmia ubriikkiyhteiskuntaan (Toim. Päivikki Karhula). Eduskunnan kirjasto, Helsinki 2008. (Kasvi 2008)

*Kekkonen Jukka*: Oikeustieteen yhteiskunnallinen vaikuttavuus oikeushistorian valossa. Teoksessa Aarto Markus & Vartiainen Markku (toim.): Oikeus kansainvälisessä maailmassa: Ilkka Sadaviidan juhlakirja, s. 123-134. Edita Prima Oy, Helsinki 2008. (Kekkonen 2008)

*Kiuru Pertti; Mäkelä Jaana & Huvio Petteri*: Avoimen julkisen tiedon hyödyntämisen potentiaalista suomalaisissa yrityksissä. Aalto-yliopiston raportti, 30.4.2012. (Kiuru ym. 2012)

*Korhonen, Rauno*: Perusrekisterit ja tietosuoja, Edita Publishing Oy, Helsinki 2003. (Korhonen 2003)

*Kosta Eleni*: Consent in European Data Protection Law, Martinus Nijhoff publishers, Boston 2013. (Eleni 2013)

*Kulla Heikki*: Julkishallinnon verkostoitumisen haasteita. Teoksessa Turun yliopiston oikeustieteellinen tiedekunta 50 vuotta, toim. Tatu Hyttinen – Katja Weckström. Turun yliopisto, oikeustieteellinen tiedekunta 2011. (Kulla 2011)

*Kulla Heikki*: Hallintomenettelyn perusteet, Talentum Pro, Helsinki 2015. (Kulla 2015)

*Kultalahti Jukka*: Empiirinen metodi oikeudellisen tulkinnan apuvälineenä. Teoksessa Empiirisen oikeustutkimuksen kokemukset, haasteet ja tulevaisuus. Itä-Suomen yliopiston oikeustieteellisiä julkaisuja 26, toim. Anssi Keinänen, Mia Kilpeläinen ja Ulla Väättäinen, Itä-Suomen yliopisto, Joensuu 2010, s. 15-43. (Kultalahti 2010)

*Kuopus Jorma*: Sähköinen hallinto, tietoturvallisuus ja yksityisyyden suoja. Teoksessa: Viestintäoikeus, 2002 (Toim. Heikki Kulla). WSOY Lakitieto, Helsinki, s. 213-246.

(Kuopus 2002)

*Kuronen Timo*: Tietovarantojen hyödyntäminen ja demokratia, Sitra 174, Helsinki 1998.

(Kuronen 1998)

*Maynika James; Chui Michael; Farrell Diana; Van Kuiken Steve; Groves Peter and Almasi Doshi Elizabeth*: Open data: Unlocking innovation and performance with liquid information. McKinsey Global Institute Report. McKinsey & Company, 2013. (Manyika ym. 2013)

*Mayer – Schönberger Viktor, Cukier Kenneth*: Big Data. A Revolution That Will Transform How We Live, Work and Think. John Murray, Lontoo 2013. (Mayer – Schönberger & Cukier 2013)

*Mäenpää Olli*: Hallintosopimus – Hallintoviranomaisten sopimustoiminnan oikeudellisia ongelmia. Lakimiesliiton kustannus, Helsinki 1989. (Mäenpää 1989)

*Mäenpää Olli*: Julkisuusperiaate, WSOYpro, Helsinki 2008. (Mäenpää 2008)

*Määttä Tapio*: Ympäristöoikeudellisen tutkimuksen uudet suuntaukset ja menetelmät. Teoksessa Oikeustieteellinen opinnäytetyö, Joensuun yliopiston oikeustieteellisiä julkaisuja, toim. Tarmo Miettinen, Joensuun yliopisto, Joensuu 2004, s. 113-166. (Määttä 2004)

*Narayanan Arvind, Huey Joanna, W.Felte Edward*: A Precautionary Approach to Big Data Privacy. Teoksessa Data Protection on the Move – Current Developments in ICT and Privacy/Data Protection. Springer Science+Business Media Dordrecht 2016. (Narayanan – Huey – W.Felte 2016)

*Pahlman Irma*: Potilaan itsemääräämisoikeus. Edita Publishing Oy, Helsinki 2003.

(Pahlman 2003)

*Pahlman Irma*: Asiakirjajulkisuus ja tietosuoja sosiaali- ja terveydenhuollossa, 1. uudistettu painos 2007, Edita Publishing Oy. (Pahlman 2007)

*Pitkänen Olli; Tiilikka Päivi & Warma Eija*: Henkilötietojen suoja. Talentum. Helsinki 2013. (Pitkänen ym. 2013)

*Pitkänen Olli*: Sinun tietosi eivät ole sinun: rekisteröidyn oikeus hyödyntää omia henkilötietojaan. Teoksessa *Oikeus* 2014; 2, s. 202-214. (Pitkänen 2014)

*Poikola Antti; Kuikkaniemi Kai; Honko Harri*: MyData – A Nordic Model for human-centered personal data management and processing. Ministry of Transport and Communications, 2015. (Poikola ym. 2015)

*Pulkkinen Tuija*: Snellmanin perintö suomalaisessa sananvapaudessa. Teoksessa *Sananvapaus*, toim. Nordenstreng Kaarle. Porvoo, WSOY 1996, s. 194-209. (Pulkkinen 1996)

*Pöysti Tuomas*: Sähköinen identiteetti. Teoksessa: *Encyclopaedia Iuridica Fennica 7*, Oikeuden yleiset tieteet. Suomalainen Lakimiesyhdistys, Helsinki, p. 1112-1116. (Pöysti 1999a)

*Pöysti, Tuomas*: Tehokkuus, informaatio ja eurooppalainen oikeusalue. Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisut, Hakapaino Oy, 1999. (Pöysti 1999b)

*Saarenpää Ahti*: Tietosuoja. Teoksessa: *Encyclopaedia Iuridica Fennica 7*, Oikeuden yleiset tieteet. Suomalainen Lakimiesyhdistys, Helsinki 1999, p. 1163– 1173. (Saarenpää 1999)

*Saarenpää Ahti*: Oikeudellinen tieto verkkoyhteiskunnassa. Teoksessa: *Paratiisi vai panoptikon – Näkökulmia ubriikkiyhteiskuntaan* (Toim. Päivikki Karhula). Eduskunnan kirjasto, Helsinki 2008. (Saarenpää 2008)

*Saarenpää Ahti*: Henkilö- ja persoonallisuus oikeus. Teoksessa *Tammilehto, Timo* (toim.): *Oikeusjärjestys*. Osa 1, s. 218-409. 8 täydennetty painos. Lapin yliopiston oikeustieteellisiä julkaisuja. Rovaniemi 2012. (Saarenpää 2012)



*Salokannel Marjut*: Julkisesta datasta avoimeen dataan – Julkisen datan lisensiointi. Elinkeinoelämän tutkimuslaitos 16.8.2012, Keskusteluaiheita No 1277. (Salokannel 2012)

*Sorvari Hannu*: Tiedollinen itsemäärääminen ja markkinointi. Teoksessa: Viestintäoikeus, 2002 (Toim. Heikki Kulla). WSOY Lakitieto, Helsinki, s. 271–291. (Sorvari 2002)

*Van Dijk Jan*: The Network Society, 3rd Edition. London 2012. (Van Dijk 2012)

*Vilkkonen Eero*: Hallintotoimen mitättömyydestä, Suomalainen Lakimiesyhdistys, Vammala 1970. (Vilkkonen 1970)

*Voigt Paul – von dem Bussche Axel*: The EU General Data Protection Regulation (GDPR) – A Practical Guide. Springer International Publishing AG 2017. (Voigt – von dem Bussche 2017).

*Voutilainen, Tomi*: Tieteellisen tutkimuksen vapaus henkilötietojen käsittelyssä. Teoksessa: Oikeustieteellinen opinnäytetyö, 2004 (Toim. Miettinen). Joensuun yliopiston oikeustieteiden laitoksen julkaisuja nro 10, Joensuu. (Voutilainen 2004)

*Voutilainen, Tomi*: Hyvä sähköinen hallinto, Edita Publishing Oy, Helsinki 2005. (Voutilainen 2005)

*Voutilainen, Tomi*: ICT-oikeus sähköisessä hallinnossa, Edita Publishing Oy, Helsinki 2009. (Voutilainen 2009)

*Voutilainen Tomi*: Oikeus tietoon: informaatio-oikeuden perusteet, Edita 2012. (Voutilainen 2012)

*Voutilainen Tomi – Huttunen Kimmo*: Julkisen hallinnon tiedonhallinnan pirstoutuminen ja lainsäädäntö. Oikeus 2015 (44); I: s. 69–81. (Voutilainen – Huttunen 2015)

*Wallin Anna-Riitta, Nurmi Pekka*: Tietosuojalainsäädäntö: henkilörekisterilaki ja siihen liittyvät säädökset, Lakimiesliiton kustannus, 2. uudistettu painos, Helsinki 1991. (Wallin-Nurmi 1991)

*Wallin Anna-Riitta, Konstari Timo:* Julkisuus- ja salassapitolainsäädäntö – Laki viranomaisten toiminnan julkisuudesta ja siihen liittyvät lait. Gummerus Kirjapaino Oy, Jyväskylä 2000. (Wallin – Konstari 2000)

*Wallin, Anna-Riitta:* Tiedonsaanti asiakirjoista ja henkilötietojen suoja EU:n perusoikeuskirjassa tunnistettuina perusoikeuksina. Teoksessa Perusoikeudet EU:ssa (toim. Liisa Nieminen), Lakimiesliiton kustannus, Helsinki 2001. (Wallin 2001)

*Zanfir, Gabriela:* The right to Data portability in the context of the EU data protection reform. *International Data Privacy Law* (2012) 2 (3), s. 149–162. (Zanfir 2012)

## **2 Kotimaiset virallislähteet**

### **2.1 Hallituksen esitykset, valiokuntamietinnöt ja valiokuntalausunnot**

*HE 9/2018*, Hallituksen esitys eduskunnalle EU:n yleistä tietosuojaa-asetusta täydentäväksi lainsäädännöksi.

*HE 145/2017*, Hallituksen esitys laiksi liikenteen palveluista annetun lain muuttamiseksi ja eräiksi siihen liittyviksi laeiksi.

*HE 72/2017*, Hallituksen esitys eduskunnalle laiksi valtakunnallisista opinto- ja tutkintorekistereistä.

*HE 96/1998 vp*, Hallituksen esitys Eduskunnalle henkilötietolaiksi ja eräiksi siihen liittyviksi laeiksi.

HaVM (26/1998) vp, Hallintovaliokunnan mietintö hallituksen esityksestä eduskunnalle henkilötietolaiksi ja eräiksi siihen liittyviksi laeiksi.

U 21/2012 vp. Valtioneuvoston kirjelmä ehdotuksesta asetukseksi yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (Yleinen tietosuojasetus) sekä direktiiviksi yksilöiden suojelusta toimivaltaisten viranomaisten henkilötietojen

käsittelyssä rikosten torjumiseksi, tutkimiseksi, selvittämiseksi tai niistä syyttämiseksi tai rikosoikeudellisten seuraamusten täytäntöönpanemiseksi ja näiden tietojen vapaasta liikkuvuudesta (Tietosuojadirektiivi).

## **2.2 Oikeustapaukset, Eduskunnan apulaisoikeusasiamiehen ja apulaisoikeuskanslerin ratkaisut:**

Eduskunnan apulaisoikeusasiamiehen ratkaisuja: AOA 2901/2/04, antopäivä 21.9.2005.

Apulaisoikeuskansleri: AOK 187/1/2009, antopäivä 8.2.2011.

Apulaisoikeuskansleri: AOK 947/1/02, antopäivä 16.4.2004.

Korkeimman hallinto-oikeuden ratkaisu 2012:55.

KHO 4.10.2010 T 2558

## **2.3 Muu kotimainen virallisaineisto**

Elinkeinoelämän tutkimuslaitos: Koski Heli, Kiuru Pertti, Mäkelä Jaana, Salokannel Marjut; Julkinen tieto käyttöön. Keskusteluaiheita No 1276, 19.6.2012.

Liikenne- ja viestintäministeriö: Julkinen data – johdatus tietovarantojen avaamiseen, Editia Prima Oy, Helsinki 2010.

LVM 2/2014: My Data - johdatus ihmiskeskeiseen henkilötiedon hyödyntämiseen. Liikenne- ja viestintäministeriön julkaisuja 2014 / 2014.

Oikeusministeriö: ”EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmän mietintö”, TATTI Työryhmä. Oikeusministeriön julkaisu 35/2017.

Oikeusministeriön blogi 6.4.2016: Anu Talus: Tietosuoja-asetus – uutta ja vanhan vahvistamista. [http://oikeusministerio.fi/blogi/-/asset\\_publisher/nprlwbUtjMQ0/blog/anu-talus-tietosuoja-asetus-uutta-ja-vanhan-vahvistamista](http://oikeusministerio.fi/blogi/-/asset_publisher/nprlwbUtjMQ0/blog/anu-talus-tietosuoja-asetus-uutta-ja-vanhan-vahvistamista). Luettu 12.5.2018.

Tietosuojavaikuttetun toimisto: Henkilötietojen luovuttaminen viranomaisten henkilörekisteristä, päivitetty 27.07.2010.

Tietosuojavaltuutetun toimisto: Lokitiedot henkilötietojen suojaamisen välineenä, 12.11.2012, päivitetty 10.06.2014.

Valtioneuvosto: Ehdotus valtioneuvoston periaatepäätökseksi julkisen sektorin digitaalisten tietoaineistojen saatavuuden parantamisesta ja uudelleenkäytön edistämisestä, 3.3.2011.

Valtioneuvoston kanslia: Knuutila Aleks, Kokkonen Vesa, Sundquist Heikki, Kuittinen Ossi & Thure Salla: MyData muutosvoimana: Julkishallinnon henkilötiedon ihmiskeskeisen hyödyntämisen mallit ja vaikutukset. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 61/2017.

Valtioneuvoston kanslia: Ratkaisujen Suomi; Pääministeri Juha Sipilän hallituksen strateginen ohjelma 29.5.2015, Hallituksen julkaisusarja 10/2015.

Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 61/2017: Aleks Knuutila, Vesa Kokkonen, Heikki Sundquist, Ossi Kuittinen, Salla Thure – MyData muutosvoimana: Julkishallinnon henkilötietojen ihmiskeskeisen hyödyntämisen mallit ja vaikutukset.

Valtiovarainministeriön julkaisuja 2/2012; Julkishallinnon tietovarantojen saatavuuden ja käytön edistäminen -työryhmän loppuraportti - Julkishallinnon tietoluovutusten periaatteet ja käytännöt.

Valtiovarainministeriö: Avoimen tiedon ohjelman 2013-2015 käynnistäminen, taustamuistio 22.3.2013.

Valtiovarainministeriön raportti – 31/2015: Avoimesta datasta innovatiiviseen tiedon hyödyntämiseen – Avoimen tiedon ohjelman 2013-2015 loppuraportti.

Valtiovarainministeriö: Tiedonhallinnan lainsäädännön kehittämislinjaukset, Työryhmän raportti, Valtiovarainministeriön julkaisuja 37/2017.

Valtiovarainministeriö: Sähköinen asiointi: Selvitys sääntelyn nykytilasta sekä kehittämistarpeista ja -vaihtoehdoista, Valtiovarainministeriön julkaisu - 22/2018.

### **3 Ulkomaiset virallislähteet ja virallisaineistot**

#### **3.1 Ulkomaiset virallislähteet**

Articles of Association of MIDATA Cooperative, Seated in Zürich, Switzerland  
(Unofficial English Translation)

BIS 13.4.2011: Department for Business, Innovation & Skills, Behavioural Insights Team and Cabinet Office: Better choices: better deals. Consumers powering growth.  
13.4.2011.2011.

BIS 28.6.2012: Department for Business, Innovation & Skills: midata. Review and consultation. 28.6.2012.

BIS 27.7.2012: Department for Business, Innovation & Skills: midata: Government response to the 2012 consultation. 27.7.2012.

#### **3.2 Euroopan Unioni**

Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus). EUVL L 119, 4.5.2016.

Euroopan parlamentin ja neuvoston asetus yksityiselämän kunnioittamisesta ja henkilötietojen suojasta sähköisessä viestinnässä ja direktiivin 2002/58/EY kumoamisesta (sähköisen viestinnän tietosuoja-asetus). 10.1.2017. COM (2017) 10 final.

Euroopan parlamentin ja neuvoston direktiivi 95/46/EY annettu 24 päivänä lokakuuta 1995, yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta.

Euroopan Unionin Perusoikeuskirja 2000/C 364/01.

Euroopan parlamentin ja neuvoston direktiivi 2003/98/EY, annettu 17 päivänä marraskuuta 2003, julkisen sektorin hallussa olevien tietojen uudelleenkäytöstä.

Komission tiedonanto neuvostolle, Euroopan parlamentille, Euroopan talouskomitealle sekä alueiden komitealle: sähköisen hallinnon merkitys huomisen Euroopassa, KOM (2003) 567.

Komission ehdotus. Euroopan parlamentin ja neuvoston asetus yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (yleinen tietosuojasetus). KOM (2012) 11 lopullinen. (Komission ehdotus 2012)

### **3.3 Euroopan unionin tietosuojatyöryhmä**

WP242 rev.01: Article 29 Data Protection Working Party: Guidelines on the right to data portability. 16/EN WP242 rev.01, 5.4.2017.

WP 173: Article 29 Data Protection Working Party: Opinion 2/2010 on the principle of accountability. 00062/10/EN, WP 173, 13.7.2010.

Article 29 Data Protection Working Party: Opinion 15/2011 on the definition of consent. 13.6.2011.

WP 29 3/2013: On purpose limitation. WP 203, annettu 2.4.2013.

## **4 Internet-lähteet**

*Albarede Marine, Molins Manon*: ”If I can use your data, you can too... however you please”. The MesInfos project on SelfData. Saatavilla osoitteesta <http://mydata2016.org/2016/07/27/if-i-can-use-your-data-you-can-too-however-you-please/>. 23.4.2018. (Albarede – Molins 2016)

*Avoim rajapinta*: Avoimen rajapinnan määritelmä. Saatavilla osoitteesta <http://avoinrajapinta.fi>. 1.5.2018. (Avoim rajapinta www-sivut)

*CSC:* Bid data just beginning to explode -infograikka. Saatavilla osoitteesta <https://visual.ly/community/infographic/technology/big-data-just-beginning-explode>.

25.2.2018. (CSC: Big data just beginning to explode -infografiikka)

*European Commission:* Building a European data economy. Saatavilla osoitteesta <https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy>.

22.4.2018. (European Commission 2017)

*Finanssivalvonta:* Finanssivalvonnan www-sivut. Saatavilla osoitteesta [http://www.finanssivalvonta.fi/fi/Finanssiasiakas/Finanssialan\\_palveluita/Vakuutuspalvelut/Korvaukset/Vakuutuksen\\_myontaminen/Pages/Default.aspx](http://www.finanssivalvonta.fi/fi/Finanssiasiakas/Finanssialan_palveluita/Vakuutuspalvelut/Korvaukset/Vakuutuksen_myontaminen/Pages/Default.aspx).

23.3.2018.

(Finanssivalvonnan www-sivut)

*Helsinki region info share:* Mitä on avoin data? Saatavilla osoitteesta <https://hri.fi/fi/ohjeet/mita-on-avoin-data/>.

17.5.2018. (Helsinki region info share 2017)

*JulkICT:* Yhteinen tiedon hallinta -hankkeen sivusto. Saatavilla osoitteesta <https://wiki.julkict.fi/julkict/yti>.

14.1.2018. (JulkICT:n www-sivut)

*Jaatinen Tanja:* Julkisen sektorin avoin data ja henkilötietojen suoja. Pro gradu -tutkielma, Helsingin yliopisto 2014. Saatavilla osoitteesta

<https://helda.helsinki.fi/handle/10138/156800?show=full>. 5.5.2018. (Jaatinen 2014)

*Kauhanen-Simanainen Anne:* Avoin tieto – mahdollisuus avoimelle tulevaisuudelle, diasarja Lounais-Suomen aluetietopäivillä 22.10.2014. <https://seco.cs.aalto.fi/events/2014/2014-01-24-ldf/ip2/kauhanen-simanainen.pdf>.

3.5.2018. (Kauhanen-Simanainen Anne 2014)

*Kauppalehti:* Pirkko Tammilehdon blogikirjoitus. Saatavilla osoitteesta <https://www.kauppalehti.fi/uutiset/henkilotiedoista-tulee-kauppatavaraa---ihmiset-eivat-valttamatta-ymmarra-datan-oikeaa-arvoa/tNi5KDnJ>.

11.6.2018. (Kauppalehti 2018)

*Kontkanen Henri:* Avoin data. Saatavilla osoitteesta [https://www.hel.fi/hel2/tietokeskus/data/dokumentit/koulutusmateriaali/Hyodyntamiskoulu\\_tus\\_Henri\\_Kotkanen.pdf](https://www.hel.fi/hel2/tietokeskus/data/dokumentit/koulutusmateriaali/Hyodyntamiskoulu_tus_Henri_Kotkanen.pdf).

1.5.2018. (Kontkanen 2016)

*MesInfos:* MesInfos-projektin kotisivut. Saatavilla osoitteesta <http://mesinfos.fing.org/english/>. 27.4.2018. (MesInfos 2012)

*MesInfos:* MesInfos-projektin kotisivut. Saatavilla osoitteesta <http://mesinfos.fing.org/the-mesinfos-pilot-project-one-year-later/>. 28.4.2018. (MesInfos 2017)

*MIDATA:* Articles of Association of MIDATA Cooperative. Saatavilla osoitteesta [https://midata.coop/docs/MIDATA\\_Statuten\\_20170403\\_English.pdf](https://midata.coop/docs/MIDATA_Statuten_20170403_English.pdf). 27.4.2018. (MIDATA 2017)

*Opetushallitus:* Koski-hankkeen info. Saatavilla osoitteesta <http://www.oph.fi/kehittamishankkeet/koski> 25.2.2018. (Opetushallituksen www-sivut)

*Sitra:* Ihmislähtöinen datatalous. Saatavilla osoitteesta <https://www.sitra.fi/aiheet/ihmislahtoinen-datatalous/>. Vierailtu 25.4.2018. (Sitra 2018)

*Sitra:* Kohti reilua datataloutta periksi antamatta. Saatavilla osoitteesta <https://www.sitra.fi/blogit/kohti-reilua-datataloutta-periksi-antamatta/>. 25.4.2018. (Sitra blogi)

*Salminen Juho:* Suomessa miljoona henkilörekisteriä: ”Isoilta ruumiilta välttytty”. Suomen Kuvalehti 9.11.2011. Saatavilla osoitteesta <https://suomenkuvalehti.fi/jutut/kotimaa/suomessa-miljoona-henkilorekisteria-isoilta-ruumiilta-valtytty/>. 20.4.2018. (Salminen 2011)

*The Green Button:* Green Button Data. Saatavilla osoitteesta <http://www.greenbuttondata.org>. 17.4.2018. (The Green Button www-sivut)

*Valtioneuvoston viikko:* Liite Virallisen lehden numeroon 104/11.9.2017. Saatavilla osoitteesta [https://www.edilex.fi/valtioneuvoston\\_viikko/2017\\_36.pdf](https://www.edilex.fi/valtioneuvoston_viikko/2017_36.pdf). 4.4.2018. (Valtioneuvoston viikko 2017)

*Valtiovarainministeriö:* Kansallisen palveluarkkitehtuurin perustiedot. Saatavilla osoitteesta <http://vm.fi/palveluarkkitehtuuri/perustiedot>. 24.3.2018. (Valtiovarainministeriön www-sivut)



*Valtiovarainministeriö:* Valtiovarainministeriön tietopolitiikka ja ohjaus –sivut liittyen avoimeen tietoon. Saatavilla osoitteesta <https://vm.fi/avoin-tieto>. 27.4.2018. (Valtiovarainministeriön tietopolitiikka ja ohjaus)

*Valtiovarainministeriö:* Yhteinen tiedon hallinta -hankkeen asettamispäätös. Saatavilla osoitteesta [https://api.hankeikkuna.fi/asiakirjat/2ba10498-6ec4-4240-a776-d8dcb207d0cf/34e8024d-49ee-4deb-a59b-dfe36f316d1c/ASETTAMISPAATOS\\_20161013140556.PDF](https://api.hankeikkuna.fi/asiakirjat/2ba10498-6ec4-4240-a776-d8dcb207d0cf/34e8024d-49ee-4deb-a59b-dfe36f316d1c/ASETTAMISPAATOS_20161013140556.PDF).31.3.2018. (Valtiovarainministeriö 2016)

*Väestörekisterikeskus:* Väestörekisterikeskuksen tietojen luovutuksen kieltämistä koskeva info. Saatavilla osoitteesta <http://vrk.fi/vaestotietojarjestelma/tietojen-luovutuksen-kieltaminen>. 3.2.2018. (Väestörekisterikeskuksen www-sivut)

*Väestörekisterikeskus:* Suostumusperusteinen henkilötietojen hallinta, työpajaversio. Saatavilla <https://docs.google.com/document/d/14JJP7K6sWfEArU18Czq44JZEn1jlc27Qf743t3aMR-LM/edit#>. 9.2.2018. (Väestörekisterikeskus 2017)

*Yleisradio Oy:* Yle Uutisten artikkeli ”Digisyrjäytyminen voi vaarantaa perusoikeudet”. Saatavilla osoitteesta <https://yle.fi/aihe/artikkeli/2018/08/13/marianne-heikkila-digisyrjaytyminen-voi-vaarantaa-perusoikeudet>. 14.8.2018. (Yle Uutiset 2018)

**LYHENTEET**

AOA	Eduskunnan apulaisoikeusasiamies
AOK	Apulaisoikeuskansleri
HE	Hallituksen esitys
HetiL	Henkilötietolaki
HO	Hovioikeus
JulkL	Julkisuuslaki
KHO	Korkein hallinto-oikeus
TsA	Tietosuoja-asetus
WP29	Euroopan unionin tietosuojatyöryhmä

# 1 JOHDANTO

## 1.1 Tutkielman tausta, tutkimuskysymykset ja tavoite

Henkilötieto on dataa, jota kerätään yhä kiihtyvämpään tahtiin. Kerättyä henkilötietoa käytetään muun muassa mainonnan kohdistamisessa yksilöille tai yrityksille. Henkilötiedon avulla saadaan myös kerättyä dataa ihmisten käyttäytymisestä sekä mahdollisista kiinnostuksen kohteista, mutta siitä huolimatta data ja informaatio yleisesti eivät ole lailla suojattuja.<sup>1</sup> Yksittäisen kansalaisen on käytännössä mahdotonta tietää sitä, mitä tietoa hänestä on tallennettu ja keiden rekisterinpitäjien toimesta. Henkilötietojen käsittelyyn liittyy useita erityiskysymyksiä muuttuvan ja yhä kiihtyvämpään tahtiin kehittyvän teknologian rinnalla. Selvää on se, että aikaisempi henkilötiedon käsittelymalli ei sellaisenaan sovellu uudistuvaan teknologiseen ympäristöön, vaan on kehitettävä uusia malleja hallita henkilötietoja. Olemassa olleet henkilötietojen suojaa turvaavat oikeudet ovat tulleet haavoittuvaisiksi<sup>2</sup> ja Euroopan unionin yleinen tietosuojasetus (2016/679) pyrkii vastaamaan tähän haasteeseen.

Henkilötietoa on sekä yksityisten yritysten että viranomaisten rekistereissä. Viranomaisten rekisterit ovat pääsääntöisesti hyvin luotettavia, mutta myöskään viranomaisilla ei ole keskitettyä tietoa siitä, mihin kaikkialle yksilöstä on tallennettu tietoa. Julkisen hallinnon toimijoiden tiedon hallinta on jakautunut eri tahoille, eikä näiden välillä ole selvää yhteyttä. Tämä on aiheuttanut sen, että yksilön halutessa itsestään tietoja julkishallinnon rekistereistä, joutuu hän tiedustelemaan asiaa jokaiselta viranomaiselta erikseen. Henkilötiedon hallinta näyttäytyykin tällä hetkellä yksilön näkökulmasta hallitsemattomalta. Tätä ongelmaa omadatan mukainen omien tietojen hallinta pyrkii ratkaisemaan.

Mydata, eli suomennettuna omadata, tarkoittaa yksilön omien henkilötietojen hallintaa. Omadata on kansainvälisestikin kehitteillä oleva malli, jossa yksilön henkilötiedot avataan yksilölle itselleen hallittavaksi. Omadatassa yksilö asetetaan tiedonhallinnan keskiöön, jonka myötä hän voi itse suostumuksellaan antaa eri toimijoille luvan käsitellä omia henkilötietojaan. Julkisen sektorin hallussa olevat tiedot ovat avoimen datan myötä avattu

---

<sup>1</sup> Alén-Savikko & Pitkänen, s. 12.

<sup>2</sup> González Fuster 2014, s. 271.

yhä laajemmin myös muiden kuin valtion hyödynnettäväksi.<sup>3</sup> Avoimen datan rinnalle on tullut keskustelu julkisen sektorin hallussa olevan henkilötietomassan hyödyntämisestä ja kansalaisten oikeudesta omiin tietoihin. Tutkielman tavoitteena onkin selventää omadatan mukaisen henkilötiedon hallinnan soveltuvuutta julkiseen sektoriin. Painopisteenä tutkielmassa on tarkastella, kuinka nykyinen lainsäädäntö mahdollistaa julkishallinnon toimijalle oikeuden siirtää henkilötietoja suoraan yksilön suostumuksella toiselle rekisterinpitäjälle.

Tutkielmassa omadata-mallia tarkastellaan julkishallinnolla tulevaisuudessa mahdollisesti käytössä olevan suostumushallintarekisterin kautta. Esimerkkitapauksena tutkielmassa käytetään yhtä hallituksen kärkihanketta, Yhteinen tiedon hallinta -hanketta, jäljempänä YTI-hanke, jonka yhteydessä rakennetaan julkishallinnolle ensimmäistä suostumushallintarekisteriä. Kyseisen suostumushallintarekisterin toteutuksen myötä yksilöillä olisi mahdollisuus säädellä omien opintotietojensa luovutusta, sillä rekisteri on tarkoitus perustaa niin sanotun KOSKI-rekisterin yhteyteen.<sup>4</sup> Tutkielmassa kuitenkin tutkitaan yleisemmin henkilötietojen hallintaa tilanteessa, jossa luovutettavat henkilötiedot ovat peräisin viranomaisen perusrekistereistä ja tietoja luovutetaan yksilön antaman suostumuksen perusteella. Henkilötietojen hallintaan suostumuksen perusteella liittyy vielä paljon epäselvyyksiä muun muassa tiedonhallinnan sekä yleistä tietosuojaa-asetusta tukevan lainsäädännön ollessa vielä eduskunnan käsittelyssä.<sup>5</sup> Eräs keskeisimmistä kysymyksistä onkin yksilön tiedollisen itsemääräämisoikeuden kokonaisuuden merkitys suostumusten hallinnassa ja siinä, kuinka laajasti kehitteillä olevaa omadata-mallia voidaan todellisuudessa julkishallinnossa hyödyntää. Toinen näkökulma on rekisterinpitäjän ja rekisteröidyn suhde vastuun näkökulmasta; voidaanko suostumus antaa viranomaisen rekisteriä koskien, mikä on suostumuksen perusteella tiedon luovuttavan rekisterinpitäjän vastuu sekä mikä on tiedon vastaanottavan tahon vastuu.

Tutkielmassa esimerkkinä käytetty rakenteilla oleva suostumushallintarekisteri on tarkoitus toteuttaa Valtiovarainministeriön 1.10.2016 asettaman Yhteisen tiedon hallinta –hankkeen yhteydessä. Hankkeen toimikausi päättyy 31.12.2018. Hankkeen asettamispäätöksessä hankkeen tavoitteita kuvataan seuraavasti: ”Yhtenä kärkihankkeen toimenpiteenä

---

<sup>3</sup> Ks. LVM:n johdatus tietovarantojen avaamiseen, tiivistelmä sivu 6.

<sup>4</sup> Ks. lisää KOSKI-rekisteristä kappaleesta 3.5.3.

<sup>5</sup> Hallitus on antanut keväällä 2018 lakiluonnoksen uudeksi tietosuojalain (HE 9/2018). Tietosuojalain oli tarkoitus tulla voimaan 25.5.2018, mutta voimaantulo on viivästynyt. Tätä tutkielmaa kirjoitettaessa syksyllä 2018 lakiesitys on eduskunnan hallintovaliokunnassa valmisteilla. Asian käsittely jatkuu syyskuussa 2018.

vahvistetaan periaatetta, että tietoa kysytään vain kerran ja hyödynnetään monipuolisesti. Samalla vahvistetaan kansalaisen oikeutta omiin tietoihin ja viranomaisen mahdollisuuksia käyttää tietoa”. Edelleen päätöksessä kuvataan yhden luukun palvelumallia, jolla tarkoitetaan hankkeen puitteissa sitä, että ”kansalainen tai yritys asioi julkisessa hallinnossa tai kun on olemassa tiettyyn tilanteeseen liittyvä palvelutarve, julkisen hallinnon palveluita tuottavat organisaatiot voivat tietoon ja tiedon sujuvaan siirtymiseen perustuen antaa palvelun välttämättä moninkertaista asiointia ja tietojen ilmoittamista. Yhden luukun palvelumalli tarkoittaa palvelurajapinnan taustalla tapahtuvaa automaattista tai muutoin asiakkaalle näkymätöntä tehokkaaseen tiedon hallintaan ja digitaaliseen toimintatapaan perustuvaa prosessia”. Hankkeen tavoitteita ovat järjestelmällisesti ja tavoitteellisesti johdettu tiedon määrittely ja hallinta, tietoon perustuvan päätöksenteon tuki, kansalaisten omien tietojen hyödyntäminen sekä tiedon jakelun parantaminen.<sup>6</sup> Tiivistettynä YTI-hanke tavoittelee julkishallinnon yhteisiä tietovarantoja sekä sitä, että julkishallinnolla olevat tiedot yksilöstä ovat lain edellyttämien viranomaisten saatavilla. Tästä tulee yhden luukun palvelun –periaate, jonka mukaan henkilötiedot kysytään henkilöltä itseltään vain kerran, jonka jälkeen ne ovat julkishallinnon tietovarannoissa sekä tarpeen mukaan siirrettävissä rajapinnan avulla viranomaiselta toiselle.

## 1.2 Tutkielman rajaus ja rakenne

Tutkielman tavoitteena on selvittää omadata-mallin soveltuminen julkiseen hallintoon tilanteessa, jossa sovelletaan sääntelyä luovutettaessa tietoa viranomaisen henkilörekisteristä. Tutkielmassa myös selvitetään sitä, miten oman tiedon hallinta soveltuu julkiseen sektoriin, kun tiedot tulevat usein kolmansilta tai syntyvät prosessissa. Tutkielma on rajattu koskemaan vain julkishallinnon tietojen luovutusta omadata-mallin mukaisesti. Tutkimuksen ulkopuolelle on rajattu tietojen luovutus yksityisen sektorin rekisteristä. Tutkielmassa ei myöskään perehdytä tarkemmin viranomaista koskevaan erityislainsäädäntöön sääntelyn runsauden takia. Viidennessä kappaleessa käsitellään rekisterinpitäjän vastuita ja velvoitteita myös henkilötietoja vastaanottavan rekisterinpitäjän näkökulmasta. Siltä osin vastuukysymykset ulottuvat myös muille kuin viranomaistahoille, mutta pääosin tutkielmassa keskitytään nimenomaisesti viranomaisen henkilötiedon hallintaan ja sen soveltumista omadatan mukaiseen henkilötietojen käsittelymalliin.

---

<sup>6</sup> Valtiovarainministeriö 2016. Ks. Lisää YTI-hankkeesta Valtiovarainministeriön sivuilta <http://vm.fi/yhteinen-tiedon-hallinta/perustiedot>.

Tutkielman aluksi selvitetään tiedollisen itsemääräämisoikeuden määritelmää, sen lainsäädännöllistä pohjaa sekä yleisen tietosuoja-asetuksen johdosta tulleita muutoksia. Tiedollinen itsemääräämisoikeus on tulevaisuudessa entistä keskeisemmässä asemassa henkilötietojen käsittelyn lisääntyessä, joten termin määrittely tutkielman kannalta on hyvin olennaista. Tiedollinen itsemääräämisoikeus ja omadata liittyvät toisiinsa hyvin olennaisesti, sillä ne sisältävät samoja oikeuksia, mutta omadataan liittyy lisäksi olennaisena yksilön suostumus. Kolmannessa luvussa käydään läpi tutkimuksen toista merkittävää osa-aluetta; omadataa. Omadatan määritelmä, tausta sekä nykytilanne kartoitetaan. Lisäksi kuvataan tutkielman esimerkkitapauksena olevan YTI-hankkeen suostumushallintarekisterin suunniteltu toteutusmuoto ja sen erilaiset variaatiot.

Neljäs ja viides luku käsittelevät suostumukseen perustuvaa ja viranomaisen toimesta tapahtuvaa henkilötietojen käsittelyä sekä rekisterinpitäjän vastuuta. Koska viranomaiset käsittelevät henkilötietoja lähtökohtaisesti lain nojalla, tavoitteena on selvittää suostumuksen suhde viranomaisen käsittelemään ja luovuttamaan henkilötietoon. Viidennessä luvussa käsitellään yleisesti viranomaisen vastuuta henkilötiedon käsittelystä ja tiedon luovuttamista viranomaisen rekisteristä. Tuloksia sovelletaan omadata-malliin, jossa yksilön rooli korostuu suostumuksen antamisen myötä. Tavoitteena on selvittää sitä, miten viranomaisen rekisterissä oleva henkilötieto voidaan luovuttaa suostumuksen perusteella edelleen sovellettaessa voimassa olevaa lainsäädäntöä.

### 1.3 Tutkielman metodi

Tutkielman metodi on ensisijaisesti lainopillinen eli oikeusdogmaattinen. Lainopillisen metodin tarkoitus on voimassa olevan oikeuden systematisointi, tulkitseminen sekä analysointi. Voimassa olevaa oikeutta voidaan tulkita myös kriittisesti.<sup>7</sup> Tarkoituksena on selventää, miten voimassaolevan oikeuden mukaan omadata-malli soveltuu julkishallintoon ja siellä sovellettavaan henkilötietojen luovutukseen. Selventäminen pitää sisällään sekä säännösten tulkintaa että lainsäädännön muutosehdotuksia.<sup>8</sup> Lainoppi voidaan jakaa käytännölliseen ja teoreettiseen lainoppiin. Käytännöllinen lainoppi on pääosin tulkintajuridiikkaa ja teoreettinen lainoppi keskittyy oikeudenalan yleisten oppien tutkimiseen.<sup>9</sup> Tutkielma painottuu enemmän käytännölliseen lainoppiin, mutta sisältää

---

<sup>7</sup> Jyränki 2003, s. 15.

<sup>8</sup> Aarnio 1989, s. 57.

<sup>9</sup> Määttä 2004, s. 119.

myös teoreettisen lainopin piirteitä. Tutkielman päälähteitä ovat voimassa oleva lainsäädäntö sekä lakien esityöt ja niistä tehdyt selvitykset, muun muassa Euroopan unionin tietosuojatyöryhmän linjaukset.

Lainoppia tukevana tutkimusmenetelmänä on käytetty päätösempiriaa sen osalta, kun tarkoitus on ollut täsmällisen kokemuseräisen tiedon hankkimista ja sen hyödyntämistä.<sup>10</sup> Päätösempiria ei kuitenkaan ole tutkielmassa vahvassa roolissa johtuen omadatan tuoreesta kehitymisestä. Täten oikeuskäytäntöä ei ole vielä muodostunut omadatan ympärille tukemaan lain tulkintaa. Päätösempiirinen analyysi kohdistuukin osittain muuhun tulkintaan, kuin suoraan omadataan.

Tutkielmaan sisältyy myös *de lege ferenda* -suosituksia lainsäädännön kehittämistä koskien siltä osin kuin ongelmia nykylainsäädännön ja omadatan soveltamisen osalta julkishallinnossa on tunnistettu. *De lege ferenda* -näkökulma antaa lukijalle ymmärrystä siitä, millaisen sääntelykehikon avulla omadatan kokonaisvaltainen hyödyntäminen olisi mahdollista myös julkishallinnossa. Julkishallinnon tiedonhallinta onkin tutkielmaa kirjoitettaessa murroksessa, mutta omadataa ei suomalaisessa lainsäädännössä vielä kovin paljoa tunneta muutamia lakeja lukuun ottamatta.

Tutkielmalle haasteen on asettanut se, että sitä tehtäessä ei ole ollut voimassa olevaa lainsäädäntöä tai lainsäädännöllisiä kannanottoja liittyen suoraan omadataan tai sen sääntelyyn. Tästä johtuen tutkimuksessa ei ole voitu tukeutua esimerkiksi hallituksen esityksiin. Vaikka tutkimuksen metodi on lainopillinen, jossa tulkitaan voimassa olevaa oikeutta, ei laintulkintaa ole voitu tehdä omadatan sääntelyyn liittyen sen puuttumisen vuoksi. Nykylainsäädäntöä on tulkittu asettaen omadatan mukainen tiedon hallinta sen sääntelyn piiriin ja tulkiten sen soveltuvuutta esimerkiksi julkisuuslakiin. Tutkimuksen tavoite onkin arvioida objektiivisesti mahdollisia riskejä ja vastuukysymyksiä liittyen uudenlaiseen henkilötietojen hallintaan. Oikeustieteellinen tutkimus ei tulisi aina nojautua voimassa oleviin normeihin, vaan sen tulisi kyetä analysoimaan olemassa olevia rakenteita analyttisesti ja tarjoamaan myös vaihtoehtoisia ratkaisumalleja. Tieteen ei tulisi olla päätöksentekijöiden ohjailtavissa, vaan tutkimuksen piirissä voidaan etsiä totuutta myös tieteen lähtökohtien kautta.<sup>11</sup>

---

<sup>10</sup> Kultalahti 2010, s. 16.

<sup>11</sup> Kekkonen 2008, s. 134.

## 2 TIEDOLLINEN ITSEMÄÄRÄÄMISOIKEUS

### 2.1 Määrittely

Tiedollisen itsemääräämisoikeuden voidaan katsoa liittyvän valtion ja kansalaisten väliseen suhteeseen sen osalta, miten yksilöllä määritellään olevan määräämisoikeutta suhteessa valtion oikeuksiin. Suomen lainsäädäntö on aatehistoriallisesti roomalais-saksalaista alkuperää. Hegelin oikeusfilosofia, J.V. Snellmanin tavoin luettuna, on määrittänyt valtion ja kansalaisten välisten suhteiden ymmärtämistä.<sup>12</sup> Perinteisesti valtion asema on ollut vahva, mutta se on myös muuttunut ja kansalaisyhteiskunta joutuu määrittelemään paikkansa valtion ja markkinoiden välissä. Vanhempi Hegeliläinen traditio on alkanut muuttua länsimaisen liberalismiin traditioiden suuntaan. Tuija Pulkkinen tiivistää näiden kahden tradition olennaisen eron:

*Demokratian kriteeriksi muodostuu liberaalissa traditiossa se, kuinka hyvin yksilöiden vapaus on suojattu poliittisen koneiston toiminnalta, kun taas hegeliläisessä traditiossa demokratian kriteeri on, kuinka moni yksilö on mukana yhteiskunnan tietoisessa itsensä ohjaamisessa.<sup>13</sup>*

Tiedollinen itsemääräämisoikeus on yksi informaatio-oikeuden kantavista periaatteista.<sup>14</sup> Ihmisen itsemääräämisoikeus nähdään yhtenä keskeisistä osista länsimaista ihmiskäsitystämme. Itsemääräämisoikeus koostuu neljästä eri osa-alueesta:

- \* oikeudesta sisäiseen vapauteen
- \* oikeudesta ulkoiseen vapauteen
- \* oikeudesta kompetenssiin
- \* oikeudesta valtaan<sup>15</sup>

---

<sup>12</sup> Hegeliläinen traditio määrittelee yksilön ja valtion välisen suhteen siten, että yksilön velvollisuutena on uhrautua kokonaisuuden hyväksi. Ajattelutavan mukaan ihmisyksilö ja hänen mielipiteensä ovat olemassa vain kulttuurisen yhteisön seurauksena. Liberaali ajattelutapa taas olettaa loogisena lähtökohtana yksilön käsitteen. Sen mukaan yhteiskunta koostuu yksilöistä, jotka vaihtavat mielipiteitä. Katso lisää hegeliläisen ja liberaalin tradition eroista sekä sananvapauden liitynnästä, Pulkkinen 1996, alkaen sivulta 198.

<sup>13</sup> Pulkkinen 1996, s. 200.

<sup>14</sup> Pöysti 1999, s.471.

<sup>15</sup> Korhonen 2003, s. 84.



Itsemääräämisoikeuden puitteissa kansalaisella on oikeus säilyttää määräysvalta<sup>16</sup> itseään koskevaan tietoon eli salata tieto tai julkistaa se yhteiskunnassa.<sup>17</sup> Itsemääräämisoikeuden voidaan katsoa myös koostuvan julkisesta ja yksityisestä itsemääräämisoikeudesta. Yksityinen itsemääräämisoikeus määrittelee yksilön suhdetta toisiin yksilöihin ja julkinen itsemääräämisoikeus taas kattaa yksilön oikeutta osallistua yhteiskunnan toimintaan.<sup>18</sup>

Julkinen itsemääräämisoikeus on tällä hetkellä murroksessa johtuen yhä kehittyvästä tiedonhallinnasta, jossa manuaalinen henkilötietojen käsittelyn siirtyy sähköiseen muotoon. Nykyisen hallituksen tavoite onkin digitalisoida julkiset palvelut erilaisten hankkeiden myötä. Esimerkkinä vuoden 2017 loppuun päättynyt Kansallinen palveluarkkitehtuuriohjelma, joka on toteuttanut julkisen hallinnon yhteistä kokonaisarkkitehtuuria rakentamalla sähköisen asioinnin tukipalveluita Suomi.fi-palveluiden muodossa.<sup>19</sup> Samalla myös julkisen hallinnon henkilötietojen käsittely elää murrosvaihetta organisaatioiden ottaessa käyttöön uusia toimintatapoja sekä uusia sähköisen asioinnin tukipalveluita. Henkilötietojen käsittelyn muuttuessa sähköiseksi, on tiedollisen itsemääräämisoikeuden merkitys korostunut. Henkilön oikeutta omiin tietoihin ei voida unohtaa digitalisoituneessa maailmassa, vaan päinvastoin, oikeus omiin tietoihin yhtenä perusoikeutena vahvistuu; jokaisella on oikeus tiedolliseen itsemääräämisoikeuteen myös jatkossa. Ihminen ei ole vain hallintoalamainen, jonka henkilötiedot ovat vapaasti hyödynnettävissä tehokkuuden ja tuottavuuden nimissä, vaan sen sijaan henkilötiedot ovat yhä kiinteämpi osa henkilön itsemääräämisoikeutta siinä missä esimerkiksi fyysinen tai alueellinen itsemääräämisoikeus on jokaisen henkilökohtainen asia.<sup>20</sup>

Tiedollinen itsemääräämisoikeus on yksi perusoikeuksista, jonka määrittely on eri lähteestä riippuen erilaista. Perusidea on kuitenkin sama; tiedollisella itsemääräämisoikeudella tarkoitetaan yksilön oikeutta tietää itseään koskevien tietojen käytöstä sekä vaikuttaa näiden tietojen käyttöön.<sup>21</sup> Tiivistettynä tiedollinen itsemääräämisoikeus tarkoittaa ”yksilön oikeutta tietää ja määrätä itseään koskevien tietojen käytöstä eli oikeutta kontrolloida, jaskaako itseään koskevia tietoja, milloin ja kenen kanssa, vai pitääkö itseään koskevat tiedot

---

<sup>16</sup> Tiedollista itsemääräämisoikeutta ei kuitenkaan tule mieltää omistusoikeudeksi kyseisiin tietoihin. Tieto on hyvin erilainen kuin aineellinen esine, joten tietoon kohdistuvat oikeudet ovat yleensä kiello-oikeuksia. Katso lisää omistusoikeuden määritelmästä suhteessa tietoon Pitkänen ym. 2013, s. 10-13.

<sup>17</sup> Saarenpää 2008, s.156.

<sup>18</sup> Korhonen 2003, s. 84.

<sup>19</sup> Ks. lisää KaPA-ohjelmasta Valtiovarainministeriön www-sivuilta.

<sup>20</sup> Saarenpää 1999, s.1165.

<sup>21</sup> Voutilainen 2004, s. 66.

salassa. Tiedolliseen itsemääräämisoikeuteen kuuluu myös oikeus valvoa itseään koskevien tietojen käsittelyä sekä oikeus itseään koskevien tietojen oikeellisuuteen”.<sup>22</sup> Tiedolliseen itsemääräämisoikeuteen voidaan myös liittää keskeiset yksityisyyden suojaan vaikuttavat elementit, joita ovat oikeus yksityiselämään ilman perusteetonta ulkopuolista puuttumista, oikeus tietää itseään koskevien tietojen käytöstä, oikeus vaikuttaa itseään koskevien tietojen käyttöön sekä oikeus tulla arvioiduksi oikeiden ja relevanttien tietojen perusteella.<sup>23</sup> Voutilaisen mukaan ”tiedollinen itsemääräämisoikeus koostuu oikeudesta pitää salassa itseään koskeva tieto, oikeudesta saada itseään koskeva tieto, oikeudesta tarkastaa itseään koskevat tiedot, oikeudesta korjauttaa itseään kohdistuvissa tiedoissa olevat virheet, oikeudesta vaikuttaa itseään koskevien tietojen keräämiseen ja luovuttamiseen sekä oikeudesta julkistaa tai antaa itseään koskevia tietoja”.<sup>24</sup>

## 2.2 Nykytila

### 2.2.1 Sääntely

Tiedollisen itsemääräämisoikeuden perusta tulee perustuslaista. Perustuslain 7.1 §:n mukaan jokaisella on oikeus elämään sekä henkilökohtaiseen vapauteen, koskemattomuuteen ja turvallisuuteen. Kyseinen perustuslain säännös pitää sisällään oikeuden itsemääräämiseen, jonka eräänä elementtinä on tiedollinen itsemääräämisoikeus.<sup>25</sup> Perustuslain 7.1 §:n säännös sisältää myös jokaiselle oikeuden turvallisuuteen. Tästä oikeudesta on johdettavissa vaatimus sähköisen hallinnon tietoturvallisuudesta huolehtimiseen, joka osaltaan mahdollistaa tiedollisen itsemääräämisoikeuden toteuttamista.<sup>26</sup> Verrattuna yksityisyyden suojaamiseen liittyvään käsitteeseen, tiedollisessa itsemääräämisoikeudessa korostuu yksilön olemisen subjekti henkilötietojensa käsittelyssä.<sup>27</sup> Vaikka tiedollista itsemääräämisoikeutta ei nimenomaisesti ole lakiin kirjattu, on lain kirjauksista johdettavissa tiedollisen itsemääräämisoikeuden pääsäännöt.

Tietosuojalainsäädännön yleislaki henkilötietolaki (523/1999), jonka tarkoituksena on toteuttaa yksityiselämän suoja ja muita yksityisyyden suoja turvaavia perusoikeuksia

---

<sup>22</sup> Hoikkala ym. 2005, s. 284.

<sup>23</sup> Wallin - Nurmi 1991, s. 21.

<sup>24</sup> Voutilainen 2012, s. 243.

<sup>25</sup> Sorvari 2002, s. 272.

<sup>26</sup> Voutilainen 2005, s.48.

<sup>27</sup> Sorvari 2002, s.272.

henkilötietoja käsiteltäessä sekä edistää hyvän henkilötietojen käsittelytavan kehittämistä ja noudattamista (HetiL 1 §). Henkilötietoa koskeva sääntelykenttä on muuttumassa ja EU:n yleisen tietosuoja-asetuksen myötä henkilötietolaki kumotaan ja säädetään uusi tietosuojalaki.<sup>28</sup> Ennen yleistä tietosuoja-asetusta rekisterinpito on pitkälti pohjautunut henkilötietolakiin ja EU:n tasoiseen sääntelyyn, eivätkä henkilötiedon yleiset periaatteet tietosuoja-asetuksen myötä ole muuttumassa.<sup>29</sup> Yleisiä periaatteita voidaan edelleen tarkastella siirtymässä olevan henkilötietolain sääntelyn pohjalta. Henkilötietolain 2 luvussa on säädetty yleisistä periaatteista, joiden nojalla henkilötietoja voidaan käsitellä. Rekisterinpitäjän on muun muassa perusteltava asiallisesti henkilötietojen käsittelyn tarkoitus rekisterinpitäjän kannalta. Lisäksi käsittelyn käyttötarkoitussidonnaisuus sekä käsittelyn yleiset edellytykset tulee täyttyä. Rekisterinpito on henkilötietolain nojalla toteutettava suunnitelmallisesti sekä asiakaslähtöisesti. Henkilötietolain hallituksen esityksessä mainitaan yksilöllä olevan lähtökohtaisesti päätösvalta siihen, miten häntä koskevia tietoja saa käyttää, jollei lainsäädännössä toisin ole osoitettu.<sup>30</sup>

### 2.2.2 Tiedollista itsemääräämisoikeutta suojaavat oikeudet

Tietosuojallista peruseriaatetta ilmentää Ahti Saarenpään mukaan ”vaatimus rekisteröidyn tiedonsaanti-, oikaisu-, vastustus- ja kielto-oikeuksien sääntelystä laissa”. Edelleen Saarenpää korostaa sitä, että henkilö itse on henkilötietojen käsittelyn subjekti, ei vain objekti. Tästä johtuen rekisteröidyn tulee voida tietää missä ja miten häntä koskevia henkilötietoja käsitellään.<sup>31</sup> Rekisteröidyllä olevat oikeudet ovat keino vaikuttaa siihen, miten yksilön tietoja käsitellään ja minne niitä luovutetaan. Oikeudet ovat kuitenkin nykyllä lainsäädännön valossa olleet rajattuja sen suhteen, kuinka laajasti henkilötietojen käsittelyyn yksilö voi vaikuttaa.

Käsitteet tiedonsaantioikeus sekä oikeus tietoon tai informaatioon liittyvät läheisesti toisiinsa, mutta niitä voidaan myös pitää toistensa synonyymeina.<sup>32</sup> Käsitteitä eriteltäessä on löydettävissä useita eri tiedonsaantioikeuksia liittyen muun muassa asianosaisen oikeuteen saada tietoa, käsitellä tietoa, oikeutta ilmaista tietoa sekä oikeutta aktiivisesti hankkia tietoa. tiedonsaantioikeuden yksi määritelmä on oikeus tiedolliseen yksityisyyteen ja tiedolliseen

<sup>28</sup> Ks. uudesta tietosuojalaista HE 9/2018.

<sup>29</sup> Ks. tietosuoja-asetuksesta laajemmin luvusta 2.3.2.

<sup>30</sup> HE 96/1998 vp, s.4.

<sup>31</sup> Saarenpää 1999, s.1171.

<sup>32</sup> Ks. Korhonen 2003, s.16, jossa Korhonen käyttää käsitteitä pääasiallisesti toistensa synonyymeina.

itsemääräämisoikeuteen.<sup>33</sup> Tiedonsaantioikeus osaltaan mahdollistaa tiedollisen itsemääräämisoikeuden yksilön pyrkiessä hallinnoimaan tietojensa käyttöä. Tiedollisen itsemääräämisoikeuden edellytyksenä on vapaus muodostaa käsitys niistä yhteyksistä, joihin henkilötietoa luovutetaan sekä siitä tiedosta, joka on luovutuksen kohteena. Tiedolliseen itsemääräämiseen kuuluu rekisteröidyn mahdollisuudet valvoa oikeuksiaan sekä mahdollisuus halutessaan tarkastaa henkilötietojensa käsittely rekisterinpitäjältä.<sup>34</sup> Eri asia kuitenkin on se, missä määrin yksilöllä on mahdollisuus saada tietoa siitä, missä kaikkialla rekistereissä hänen tietojaan käsitellään. Tietosuoja-asetuksen 15 artiklan mukaan rekisteröidyllä on oikeus saada rekisterinpitäjältä vahvistus siitä, että häntä koskevia henkilötietoja käsitellään sekä oikeus saada pääsy henkilötietoihinsa.

Tiedonsaantioikeuden yleissääntely liittyen viranomaisessa asiointiin tulee laista viranomaisen toiminnan julkisuudesta (621/1999). Lain 11 §:ssä säädetään asianosaisen oikeudesta ”saada asiaa käsittelevältä tai käsitelleeltä viranomaiselta tieto muunkin kuin julkisen asiakirjan sisällöstä, joka voi tai on voinut vaikuttaa hänen asiansa käsittelyyn”. Edelleen lain 12 §:ssä säädetään oikeudesta saada tieto itseään koskevasta asiakirjasta. Pykälän mukaisesti ”jokaisella on oikeus saada tieto hänestä itsestään viranomaisen asiakirjaan sisältyvistä tiedoista 11 §:n 2 ja 3 momentissa säädetyin rajoituksin, jollei laissa toisin säädetä”. Tiedonsaanti on siten perusoikeus, jota voidaan vain laissa säädetyn edellytyksen täytyttyä perustellusti rajoittaa. 12 §:n sananmuoto ei edellytä asianosaisen asemaa. Oikeuskirjallisuudessa on kuitenkin tulkittu 12 §:n muodostavan kapea-alaisemman tiedonsaantioikeuden kuin julkisuuslain 11.1 §:ssä säädetty asianosaisjulkisuus. 12 §:n perusteella on yksilön oikeus saada tieto vain asiakirjasta, jotka koskevat häntä itseään, ei välttämättä samoja tietoja kuin asianosainen 11.1 §:n perusteella saisi.<sup>35</sup>

Oikaisuoikeus on jo ennen tietosuoja-asetuksen voimaan astumista ollut yksi rekisteröidyn oikeuksista. Rekisteröidyllä on henkilötietolain 29 §:n nojalla ollut oikeus tiedon korjaamiseen. Rekisterinpitäjän on ilman aiheetonta viivytystä oikaistava tai täydennettävä rekisterissä oleva virheellinen henkilötieto. Tietosuoja-asetuksessa sama oikeus toteutuu 16 artiklan nojalla, jonka mukaan rekisteröity on oikeutettu tietojensa oikaisemiseen. Oikaisuoikeus voidaan katsoa olevan hyvin keskeinen osa tiedollista itsemääräämisoikeutta siinä suhteessa, että rekisteröidyllä on oikeus saada virheelliset tiedot korjattua ja sitä myötä

---

<sup>33</sup> Korhonen 2003, s. 16-17.

<sup>34</sup> Sorvari 2002, s. 273.

<sup>35</sup> Pahlman 2007, s. 59. Ks. erityisesti potilaan tiedonsaantioikeudesta, Pahlman 2007, s.58-59.

vaikuttaa myös omaan tietosuojansa. Henkilötietojen korjaamisen tarve voi ilmetä muulloinkin, kuin pelkästään tietojen tarkastamisen yhteydessä. Rekisteröity voi esimerkiksi havaita tiedoissaan virheellisiä henkilötietoja saadessaan asiakirjoja, joissa on häntä itseään koskevia tietoja.<sup>36</sup>

Kielto-oikeudesta on säädetty henkilötietolain 30 §:ssä, jossa rekisteröidylle on kirjattu oikeus kieltää rekisterinpitäjää käsittelemästä häntä itseään koskevia tietoja eräissä tilanteissa. Pykälän mukaan kielto-oikeutta on rekisteröity voinut käyttää silloin, kun asia koskee suoramainontaa, etämyyntiä, markkina- ja mielipidetutkimusta sekä henkilömatrikkeliä ja sukututkimusta. Kielto-oikeus on ollut passiivinen siten, että rekisterinpitäjä on voinut käsitellä rekisteröidyn henkilötietoja, ellei rekisteröity ole erikseen käyttänyt kielto-oikeutta. Kielto-oikeus on koskenut myös rekisterinpitäjän käsittelemiä tietoja suostumuksen perusteella. Rekisteröity on voinut peruuttaa suostumuksensa henkilötietojen käsittelyyn milloin tahansa, jolloin kielto-oikeus on ulottunut myös suostumusperusteiseen henkilötietojen käsittelyyn. Kielto-oikeus ei ole ehdoton oikeus, jolla rekisteröity voi kieltää kaikki henkilötietojensa käsittely käyttötarkoituksesta riippumatta. Esimerkiksi lain nojalla tapahtuva henkilötiedon käsittely on lähtökohtaisesti oikeus, jota rekisteröity ei voi kieltää. Rekisteröidyllä ei myöskään ole oikeutta kieltää henkilötietojensa käsittely tieteellistä tai historiallista tutkimusta tai tilastokäyttöä varten. Tätä kielto-oikeuden rajoitusta ei myöskään uudessa kansallisessa tietosuojalaissa olla muuttamassa. Uuden tietosuojalain edotuksen 31 §:n mukaan käsiteltäessä henkilötietoja tieteellistä tai historiallista tutkimustoimintaa varten, voidaan tietosuoja-asetuksen rekisteröidyn oikeuksista poiketa pykälän sisältämien poikkeuksien täytyessä.<sup>37</sup> Tietosuoja-asetuksessa säädetään oikeudesta käsittelyn rajoittamiseen. 18 artiklan nojalla rekisteröidyllä on oikeus siihen, että rekisterinpitäjä rajoittaa käsittelyä artiklan a-d alakohtien nojalla. Tässäkään suhteessa rajoitusoikeus ei ole ehdoton, vaan tiettyjen edellytysten täytyessä rekisteröidyllä on mahdollisuus vedota rajoitusoikeuteensa.

---

<sup>36</sup> Voutilainen 2012, s. 270.

<sup>37</sup> HE 9/2018 vp, s. 114.

## 2.3 Tiedollisen itsemääräämisoikeuden vahvistuminen

### 2.3.1 Aluksi

Tiedollinen itsemääräämisoikeus on korostunut yhteiskunnan digitalisaation myötä. Yksilöt eivät enää ole vain tiedon keruun kohteita, vaan päinvastoin on arvioitu, että kaikesta digitaalisesta tiedosta jopa yli 70 prosenttia on yksilöiden itsensä tuottamaa. Kuitenkin näistä tiedoista 80 prosenttia on yritysten hallussa.<sup>38</sup> Tiedollisen itsemääräämisoikeuden korostaminen osana henkilön perusoikeuksia on nyt ja tulevaisuudessa yhä kiinteämpi osa yhteiskuntaa. Yksilön tiedollinen itsemääräämisoikeus ei tietosuojasääntelyn myötä ole toteutunut siten, että yksilön vaikutusmahdollisuus omien tietojensa käsittelyyn toteutuisi nyky-yhteiskunnassa.<sup>39</sup> Uuden tietosuoja koskevan sääntelyn myötä tiedollista itsemääräämisoikeutta on vahvistettu ja rekisterinpitäjän tulee tehdä muutoksia henkilötietojen käsittelyyn, jotta lain säätämät velvoitteet täytyisivät myös jatkossa. Vaikuttavin vahvistus on EU:n yleinen tietosuoja-asetus, josta käytetään useasti lyhennystä GDPR, joka tulee sen englanninkielisestä käännöksestä ”General Data Protection Regulation”. Vielä täytäntöönpanoa odottava kansallinen tietosuojalainsäädäntö osaltaan tulee täydentämään asetuksen vaatimuksia. Uuden tietosuojalainsäädännön myötä henkilötietolaki kumotaan kokonaan,<sup>40</sup> joten tutkielmassa keskitytään enemmän henkilötietojen käsittelyn sääntelyyn tietosuoja-asetuksen näkökulmasta.

### 2.3.2 EU:n yleinen tietosuoja-asetus

Euroopan unionin tietosuoja koskeva henkilötietodirektiivi (95/46/EY) oli vuodesta 1995 henkilötietojen käsittelyä suojaava ja ohjaava direktiivi. Direktiivin tarkoituksena oli yhdenmukaistaa luonnollisten henkilöiden henkilötietojen käsittelyä koskevien perusoikeuksien ja -vapauksien suojelua sekä varmistaa henkilötietojen vapaa liikkuvuus jäsenvaltioiden välillä. Direktiivi ei kuitenkaan enää vastannut nykypäivän vaatimuksia henkilötietojen käsittelystä. Direktiivin ratkaisut eivät riittäneet suojaamaan henkilötietojen

---

<sup>38</sup> CSC: Big data just beginning to explode -infografiikka.

<sup>39</sup> Esimerkinä voidaan mainita henkilötietolain 28 §:n mukainen tarkastusoikeuden toteuttaminen, jonka mukaan rekisteröity, joka haluaa tarkastaa itseään koskevat tiedot rekisterinpitäjältä, voi saada tutustua tietoihinsa rekisterinpitäjän luona tai vaihtoehtoisesti voi saada tiedot itselleen kirjallisesti. Toteutus ei vastaa digitalisoituneen yhteiskunnan tietojen käsittelyä, jossa tieto kulkee sähköisesti paikasta toiseen.

<sup>40</sup> Hallituksen esitys Eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi (HE 9/2018) ilmestyi maaliskuussa 2018. Esityksessä ehdotetaan, että samalla kumottaisiin henkilötietolaki sekä laki tietosuojalautakunnasta ja tietosuojavaltuutetusta.

käsittelyä, eikä sen johdosta sääntely ole ollut yhdenmukaista kaikissa jäsenvaltioissa. Jäsenvaltioiden väliset eroavuudet henkilötietojen suojaan voivat estää henkilötietojen vapaan liikkuvuuden unionin alueella. Erityisesti verkkoympäristössä toimimiseen liittyy henkilötietojen käsittelyn kannalta huomattavia riskejä. Tällaisten suojelun tasojen eroavaisuudet jäsenvaltioiden välillä sekä lisääntynyt henkilötietojen käsittelyn sääntelytarve johtivat uuden asetuksen sääntelyyn.<sup>41</sup>

EU:n tietosuojalainsäädännön alku liittyy Eurooppa-neuvoston hyväksymään Tukholman ohjelmaan. Tukholman ohjelman mukaan tietojen suojaamiseksi tulee olla kattava Euroopan unionin tasoinen strategia niin EU:n sisällä kuin suhteessa muihinkin maihin.<sup>42</sup> Suomi piti tärkeänä Euroopan unionin henkilötietoja koskevan lainsäädännön yhdenmukaistamista ja yksinkertaistamista siten, että samalla säilytettäisiin tietosuojan korkea taso. Ennen asetusta eurooppalainen tietosuojasääntely on muodostunut 28 jäsenvaltion epäyhtenäisestä sääntelystä, jonka vuoksi rajat ylittävän toiminnan sujutus sisämarkkinoilla on ollut sääntelyn tarpeessa.<sup>43</sup> Euroopan oikeus- ja sisäministerit muodostivat 15. kesäkuuta 2015 yleisnäkemyksen EU:n uudesta tietosuoja-asetuksesta.<sup>44</sup>

Tietosuoja-asetus annettiin 27 päivänä huhtikuuta 2016. Se korvasi 20 vuotta vanhan tietosuojadirektiivin. Asetus on kaikilta osiltaan velvoittava ja sitä on sovellettu sellaisenaan kaikissa jäsenvaltioissa 25 päivästä toukokuuta 2018. Asetuksen tavoitteena on ollut yhdenmukaistaa eurooppalainen tietosuojalainsäädäntö ja vahvistaa eri jäsenvaltioiden viranomaisten välistä yhteistyötä. Asetuksen keskeisimmät uudistukset liittyvät yksilöiden mahdollisuuksiin kontrolloida henkilötietojaan sekä helpottaa yksilöiden valvontaa suhteessa rekisterinpitäjän käsittelemään henkilötietoon. Asetuksessa onkin kautta linjan korostunut tiedollinen itsemääräämisoikeus.<sup>45</sup> Esimerkiksi suostumukseen liittyviä edellytyksiä on tarkennettu, rekisterinpitäjältä vaaditaan entistä enemmän läpinäkyvyyttä artikkelissa 5 määritellyn osoitusvelvollisuuden muodossa, lisätty rekisteröidylle oikeus tietojen siirtoon sekä oikeus tulla unohdetuksi. Tietosuojan merkitystä korostaa asetuksen säännösten rikkomisen johdosta mahdollistetut hallinnolliset sakot, joita

---

<sup>41</sup> Komission tiedoksianto 2012, s. 3, tietosuoja-asetuksen johtolause 3, 9 ja 10.

<sup>42</sup> U 21/2012 vp, s. 2.

<sup>43</sup> Kalliojärvi 2016, s. 45.

<sup>44</sup> Kalliojärvi 2016, s. 46.

<sup>45</sup> Oikeusministeriö 2016.

valvontaviranomainen voi jatkossa määrätä.<sup>46</sup> Tietosuoja-asetusta sovelletaan mihin tahansa prosessiin, jossa käsitellään henkilötietoa.<sup>47</sup>

### 2.3.3 Suostumus

Suostumus itsessään ei ole uusi henkilötietojen käsittelyperuste, mutta suostumus on noussut yhdeksi tärkeimmistä kysymyksistä liittyen yksityisyyden suojaan ja henkilötiedon käsittelyyn.<sup>48</sup> Nykyisessä henkilötietolaissa säädetään henkilötietojen käsittelystä suostumuksen perusteella.<sup>49</sup> Suostumus on ensisijainen peruste henkilötietojen käsittelyn laillisuudelle (general ground for lawfulness)<sup>50</sup> Mikäli henkilö on antanut yksiselitteisen suostumuksen henkilötietojensa käsittelyyn, hänen yksityisyyden suojan ja itsemääräämisoikeuden voidaan arvioida olevan maksimissaan.<sup>51</sup> Yksi keino tietosuojan toteuttamiseen onkin se, että yksilöt hallinnoivat heidän omia henkilötietojaan niin paljon, kuin se vain olisi mahdollista.<sup>52</sup>

Tietosuoja-asetuksen johtolauseessa 32 mainitaan siitä, miten yksilön suostumus hänen henkilötietojensa käsittelyyn tulisi antaa:

“Suostumus olisi annettava selkeästi suostumusta ilmaisevalla toimella, kuten kirjallisella, mukaan lukien sähköisellä, tai suullisella lausumalla, josta käy ilmi rekisteröidyn vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen tahdonilmaisu, jolla hän hyväksyy henkilötietojensa käsittelyn.”<sup>53</sup>

Edelleen johtolauseen mukaan suostumus voitaisiin katsoa toteutuvan esimerkiksi silloin, kun *rekisteröity rastittaa ruudun vieraillessaan internetsivustolla, valitsee tietoyhteiskunnan palveluiden teknisiä asetuksia tai esittää minkä tahansa muun lausuman tai toimii tavalla, joka selkeästi osoittaa tässä yhteydessä, että hän hyväksyy henkilötietojensa käsittelyä*

<sup>46</sup> Ks. asetuksen rikkomisesta johtuvista seurauksista tietosuoja-asetuksen johtolauseet 148-152.

<sup>47</sup> Feiler – Forgó – Weigl 2018, s. 14.

<sup>48</sup> Kosta 2013, s. 4.

<sup>49</sup> Henkilötietolain (1999/523) 8 §:n 1-kohta säätelee henkilötietojen käsittelyn yhden yleisen edellytyksen olevan rekisteröidyn antama yksiselitteinen suostumus. Myös 12 §:n mukaisesti arkaluonteisia tietoja voidaan käsitellä rekisteröidyn antaman suostumuksen perusteella sekä 4-luvussa määriteltyjä henkilötietojen käsittelyä erityisiä tarkoituksia varten tarvitaan rekisteröidyn suostumus.

<sup>50</sup> WP29 Data Protection Working Party: Opinion 15/2011 on the definition of consent, adopted on 13 July 2011 (“tietosuojatyöryhmän suostumusta koskeva lausunto”), s.6.

<sup>51</sup> Wallin 2001, s. 380.

<sup>52</sup> Van Dijk 2012, s. 129.

<sup>53</sup> Tietosuoja-asetus 2016/679, 32 johtolause.



*koskevan ehdotuksen.*<sup>54</sup> Määritelmän mukaan suostumusta ei sen vuoksi pitäisi voida antaa vaikenemalla, valmiiksi rastitetuilla ruuduilla tai jättämällä jokin toimi toteuttamatta, vaan tosiasiallisesti suostumuksen ilmaisevalla toimella.<sup>55</sup> Valmiiksi rastitettu ruutu, tai sivuston käytön jatkaminen ei vielä toteuta suostumuksen antamisen edellytyksiä. Suostumusta ei siten asetuksen valossa näyttäisi voitavan enää antaa konkludenttisesti, kuten hallituksen esityksessä on henkilötietojen käsittelyyn aikaisemmin tulkittu, jossa on mainittu konkludenttisen suostumuksen voivan joissain tapauksissa täyttää suostumuksen vaatimukset.<sup>56</sup>

Tietosuoja-asetuksen johtolause 42 osaltaan määrittelee sitä, miten rekisteröidyn henkilötietojen käsittelyn perustuessa suostumukseen osoitetaan, että suostumus olisi tosiasiallisesti annettu.

”Kun tietojen käsittely perustuu rekisteröidyn suostumukseen, rekisterinpitäjän olisi voitava osoittaa, että rekisteröity on antanut suostumuksensa käsittelytoimiin. Etenkin jos suostumus annetaan muuta seikkaa koskevan kirjallisen ilmoituksen yhteydessä, olisi varmistettava suojatoimin, että rekisteröity on tietoinen antamastaan suostumuksesta ja siitä, kuinka pitkälle menevästä suostumuksesta on kyse.”<sup>57</sup>

Johtolauseessa myös käsitellään sitä, milloin suostumusta ei voida pitää vapaaehtoisesti annettuna: ”*Jos rekisteröidyllä ei ole todellista vapaan valinnan mahdollisuutta ja jos hän ei voi myöhemmin kieltäytyä suostumuksen antamisesta tai peruuttaa sitä ilman, että siitä aiheutuu hänelle haittaa*”.<sup>58</sup> Tietosuoja-asetuksessa korostetaan aikaisempaa enemmän rekisteröidyn todellista tietoisuutta siitä, mihin hän on suostumustaan antamassa.<sup>59</sup> Mikäli rekisterinpitäjä ei täytä asetuksen vaatimuksia suostumuksen pyytämisen osalta, voidaan katsoa rekisterinpitäjän käsittelevän henkilötietoja lain vastaisesti.

---

<sup>54</sup> Tietosuoja-asetus, 23 johtolause.

<sup>55</sup> Tietosuoja-asetus, 23 johtolause.

<sup>56</sup> HE 96/1998 vp, s. 36.

<sup>57</sup> Tietosuoja-asetus, 42 johtolause.

<sup>58</sup> Tietosuoja-asetus, 42 johtolause.

<sup>59</sup> Myös tulevassa sähköisen viestinnän tietosuoja-asetuksessa (2017/0003) korostetaan rekisteröidyn suostumuksen antamista metadatan käsittelyyn saadakseen erityisiä palveluja, kuten suojelupalveluja. Asetuksen 18 johtolauseen mukaan suostumus internetin tai puheviestinnän käytöstä saatavien tietojen käsittelyyn ei ole pätevä, jos rekisteröidyllä ei ole todellista vapaan valinnan mahdollisuutta. Asetus tulee voimaan vuonna 2019 ja sen on tarkoitus korvata sähköisen viestinnän tietosuojadirektiivi (2002/58 EY).

### 2.3.4 Oikeus tulla unohdetuksi

Tietosuoja-asetuksen 17 artikla säätelee oikeudesta tietojen poistamiseen eli oikeudesta tulla unohdetuksi. Artiklan mukaan rekisteröidyllä on oikeus saada rekisterinpitäjä poistamaan rekisteröityä koskevat henkilötiedot ilman aiheetonta viivytystä, edellyttäen että jokin artiklassa mainituista perusteista täyttyy. Perusteet henkilötiedon poistamiseen ovat artiklan a-f kohtien mukaan tilanteet jossa henkilötiedot ovat tarpeettomia, rekisteröity on peruuttanut suostumuksensa, rekisteröity vastustaa käsittelyä, henkilötietojen käsittely on lainvastaista, henkilötiedot ovat poistettava lakiin perustuvan velvoitteen noudattamiseksi tai henkilötiedot ovat kerätty 8 artiklan 1 kohdassa tarkoitetun tietoyhteiskunnan palvelujen tarjoamisen yhteydessä. Artiklan 3 kohdassa säädetään edelleen tilanteista, jolloin 1 ja 2 kohtaa ei sovelleta. Rekisteröidyn oikeus tulla unohdetuksi sovelletaan esimerkiksi tilanteessa, jolloin kyseessä on suostumukseen perustuva asiakas ja palveluntarjoaja – suhde, eikä palveluntarjoajalla ole mitään muuta lakiin säädettyä oikeutta käsitellä henkilötietoja. Tällöin henkilötiedot tulee poistaa rekisterinpitäjän rekisteristä, vaikka rekisterinpitäjällä olisi ollut vielä tiedoille käyttötarkoitus.

Oikeus tulla unohdetuksi liittyy myös suostumushallintapalveluun siten, että oikeus voi tulla sovellettavaksi myös kyseisessä rekisterissä annetun suostumuksen myötä. Mikäli rekisteröity haluaa peruuttaa suostumuksensa, tulee rekisterinpitäjällä olla prosessit valmiina sen suhteen, miten tiedot tullaan tehokkaasti poistamaan. Suostumushallintarekisteriin liittyy myös teknisiä kysymyksiä liittyen oikeuteen tulla unohdetuksi, mutta ne kysymykset ovat rajattu pois tämän tutkielman piiristä.

### 2.3.5 Oikeus siirtää tiedot järjestelmästä toiseen

Digitalisoitunut maailma on luonut yksilöille omaa digitaalista persoonallisuutta. Internetin kehitys mahdollistaa käyttäytymisen verkossa siten, että se jättää yksilöstä digitaalisen jalanjäljen. Yksilön sähköisellä identiteetillä tarkoitetaan *”luonnollisen henkilön tiettyjen ominaisuuksien tai tietojen tallentamista sähköiseen muotoon sekä näiden ominaisuuksien tai tietojen käyttämistä erilaisiin tarkoituksiin sähköisessä toimintaympäristössä”*.<sup>60</sup>

---

<sup>60</sup> Voutilainen 2009, s. 240. Yksilön sähköinen identiteetti voidaan myös määritellä laajemmin. Ks. esimerkiksi Pöysti (1999a), s. 1112-1116, jossa sähköisen identiteetin määritelmä on *”luonnolliseen tai oikeushenkilöön tai viranomaiseen teknisesti ja oikeudellisesti luotettavalla tavalla liittyvää informaatiota, jonka perusteella henkilö on tunnistettavissa sähköisessä toimintaympäristössä”*.

Digitaalisen ympäristön luoma data, varsinkin yhdistettynä, voivat ilmentää digitaalista persoonaa. Tästä näkökulmasta katsottuna, yksilön oikeus siirtää henkilötietojaan järjestelmästä toiseen voidaan nähdä edellytyksenä digitaalisen persoonan kehittymiselle ja jopa osana ihmisoikeuksia.<sup>61</sup> Omadatan olennainen osa onkin vaatimus henkilötiedon siirrettävyydestä ja yhdisteltävyydestä eri rekistereiden välillä.<sup>62</sup>

Yleinen tietosuoja-asetus säättää uutena oikeutena rekisteröidyn oikeudesta siirtää henkilötietojaan järjestelmästä toiseen. Yleisen tietosuoja-asetuksen 20 artiklan 1. kohta säätelee seuraavasti:

”Rekisteröidyllä on oikeus saada häntä koskevat henkilötiedot, jotka hän on toimittanut rekisterinpitäjälle, jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa, ja oikeus siirtää kyseiset tiedot toiselle rekisterinpitäjälle sen rekisterinpitäjän estämättä, jolle henkilötiedot on toimitettu”.

1-kohdan mukaisen oikeuden edellytys täyttyy, mikäli käsittely perustuu suostumukseen 6 tai 9 artiklan nojalla tai sopimukseen 6 artiklan nojalla, ja käsittely suoritetaan automaattisesti. 2-kohdassa säädetään rekisteröidyn oikeudesta saada tiedot siirrettyä suoraan rekisterinpitäjältä toiselle, mikäli se vain teknisesti on mahdollista. Siirto-oikeuden piirissä ovat lisäksi vain sellaiset tiedot, jotka rekisteröity on itse toimittanut rekisterinpitäjälle. Tältä osin artiklan tulkinta ei ole täysin selvää sen osalta, mitä tarkoitetaan ”rekisteröidyn toimittamilla henkilötiedoilla”. Esimerkiksi sopimuksen perusteella käsiteltäviä henkilötietoja käsitellään usein edelleen, kun niitä muutetaan tai luokitellaan tiettyjen kriteerien mukaisesti. Tällaiset alkuperäiset rekisteröidyn sopimuksen perusteella toimittamat tiedot kuuluvat artiklan 20 piiriin, mutta rekisterinpitäjän myöhemmin käsittelemien tietojen osalta tulkinta voi olla hyvinkin eri.<sup>63</sup>

Siirto-oikeutta ei sovelleta silloin, kun käsittely perustuu muuhun lailliseen perusteeseen kuin suostumukseen tai sopimukseen. Lakisääteisen tehtävän hoitaminen, yleisen edun suorittaminen tai julkisen vallan käyttö ovat käsittelyperusteina sellaisia, joihin kyseistä artiklaa ei tarvitse soveltaa.<sup>64</sup> Tietosuoja-asetuksen johtolauseessa kuitenkin erikseen todetaan, ettei oikeus siirtää henkilötietoja saisi luoda rekisterinpitäjille velvoitetta ylläpitää

---

<sup>61</sup> Zanfir 2012, s.151.

<sup>62</sup> LVM 2/2014, s. 9-10.

<sup>63</sup> Voigt – von dem Bussche 2017, s. 170

<sup>64</sup> Tietosuoja-asetus, 68 johtolause.

teknisesti yhteensopivia tietojärjestelmiä.<sup>65</sup> Siirto-oikeus suoraan rekisterinpitäjältä toiselle on olemassa silloin, kun se on teknisesti mahdollista. Asetuksessa ei kuitenkaan oteta kantaa siihen, milloin katsotaan olevan teknisesti mahdollista siirtää tiedot järjestelmästä toiseen, vaan se jättää soveltamismahdollisuuden siltä osin. Tiedonhallinnan lainsäädännön työryhmän raportissa onkin korostettu sitä, että asetus ei luo rekisteröidylle subjektiivista oikeutta siirtää henkilötietojaa järjestelmästä toiseen. Oikeus on olemassa silloin, mikäli tiedot on saatettu siirtokelpoiseen muotoon. Asetus ei siis estä viranomaisia kehittämään tiedonsiirtotapojaan yhteentoimiviksi siten, että ne mahdollistavat rekisteröidyn 20 artiklan mukaisen oikeuden asetuksessa tarkoitettulla tavalla, mutta se ei myöskään velvoita viranomaisia rakentamaan yhteentoimivia tietojärjestelmiä.<sup>66</sup>

Yleisen tietosuoja-asetuksen mukaan siirto-oikeus ei ole rajoittamaton myöskään silloin, kun henkilötietojen käsittely perustuu suostumukseen tai sopimukseen. Asetuksen 20 artiklan 4-kohta säätelee siten, että oikeus ei saa vaikuttaa haitallisesti muiden oikeuksiin ja vapauksiin. Johtolauseessa todetaan 4-kohdasta: *”jos tietyssä henkilötietoja sisältävässä tietojoukossa tiedot koskevat useampia kuin yhtä rekisteröityä, oikeus vastaanottaa henkilötietoja ei saisi rajoittaa toisten rekisteröityjen tämän asetuksen mukaisia oikeuksia ja vapauksia.”*<sup>67</sup> Mikäli siirrettävät tiedot sisältävät kolmansien osapuolten henkilötietoja, käsittelyn oikeudellinen perusta on tunnistettava. Tiedot vastaanottanut rekisterinpitäjä ei voi käyttää tietoja muuhun tarkoitukseen, kuin määriteltyyn käyttöön.<sup>68</sup> Henkilötietojen käsittely tulee olla tästäkin syystä läpinäkyvää, jotta voidaan varmistua siitä, että uutta 20 artiklan mukaista siirto-oikeutta ei käytetä keinona saada henkilötietoja rekisterinpitäjän omiin käyttötarkoituksiin. Siirto-oikeuden tulee tosiasiallisesti vahvistaa rekisteröidyn tiedollista itsemääräämisoikeutta voidessaan siirrellä tietojaan eri toimijoille ilman, että tästä aiheutuu vastaanottavan rekisterinpitäjän toimesta uutta keinoa kolmansien osapuolten henkilötietojen kalasteluun.

Ennen tietosuoja-asetuksen voimaantuloa, 20 artiklaa lähinnä oleva oikeus on ollut henkilötietolain 26-28 §:n mukainen rekisteröidyn tarkastusoikeus.<sup>69</sup> Tarkastusoikeus on mahdollistanut rekisteröidyn oikeuden saada tietää, mitä häntä koskevia tietoja henkilörekisteriin on tallennettu, tai ettei henkilörekisterissä ole häntä koskevia tietoja.

---

<sup>65</sup> Tietosuoja-asetus, 68 johtolause.

<sup>66</sup> Valtiovarainministeriön julkaisu – 37/2017, s.24.

<sup>67</sup> Tietosuoja-asetus, 68 johtolause.

<sup>68</sup> WP 242 rev.01, s. 11.

<sup>69</sup> WP 242 rev.01, s. 3.

Tarkastusoikeuden käyttäjän on lain vaatimusten mukaan tullut esittää tarkastuspyyntö rekisterinpitäjälle allekirjoitetulla asiakirjalla tai henkilökohtaisesti rekisterinpitäjän luona. Rekisterinpitäjän on ollut varattava rekisteröidylle tilaisuus tutustua tarkastuspyynnön kohteena oleviin tietoihin sekä annettava tiedot pyydettäessä kirjallisesti. Henkilötietolain tarkastusoikeus on antanut rekisteröidylle oikeuden saada tietoa häntä koskevista henkilötiedoista, kun taas tietosuoja-asetuksen 20 artiklan mukainen oikeus siirtää tiedot järjestelmästä toiseen antaa rekisteröidylle tosiasiallisen oikeuden saada häntä koskevat tiedot itselleen ja siten mahdollistaa henkilötietojen käsittelyn rekisteröidyn haluamalla tavalla.<sup>70</sup>

---

<sup>70</sup> Kallasvuo 2015, s. 156.

## 3 OMADATA

### 3.1 Määritelmä

Omadata tarkoittaa *kansalaisen tai yhteisön oikeutta ja mahdollisuutta hallita hänestä itsestään kerättyä tietoa ja jakaa sitä valitsemilleen tahoille. Kyse voi olla yritysten tai julkisen hallinnon keräämästä tiedosta. Tämä voi vahvistaa ihmisten tiedollista itsemääräämisoikeutta ja olla tulevaisuudessa osa asiakaskeskeistä palvelua.*<sup>71</sup> Omadatasta käytetään useasti termiä MyData, josta omadata on suomennos. Tässä tutkielmassa käytetään suomennettua termiä kielellisen selkeyden vuoksi. Omadatalla pyritään ratkaisemaan yksityisyyden suojan ja henkilötietojen käsittelyn pirstaleisuuden haasteisiin asettamalla ihminen tiedon hallinnan keskiöön. Omadataperiaatteen mukaisesti organisaatio tarjoaa keräämänsä yksilöä koskevat tiedot takaisin ihmiselle itselleen hyödynnettäväksi.<sup>72</sup> Yksilöiden hallinnoima henkilötieto parantaisi myös tietosuojaa.<sup>73</sup> Antamalla yksilölle itselleen pääsyn omiin henkilötietoihinsa, mahdollistaisi se oman tiedon käsittelyn valvomista sekä puuttumista mahdollisiin virheisiin. Tämä edesauttaisii henkilötiedon laadun paranemista, kun tiedot olisivat yksilön itsensä tarkastamia.<sup>74</sup> Tällainen korostunut itsemääräämisoikeus mahdollistaisi yksilön itsensä määrittelyn sen osalta, mihin haluaa tietojaan käytettävän. Yksilö voisi esimerkiksi luovuttaa tietojaan hyödynnettäväksi paremman palvelun tai muun lisäarvon saamiseksi.<sup>75</sup> Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarjassa on esitetty MyData-periaatteet, joita ovat:

- ihmiskeskeinen tiedonhallinta ja yksityisyys,
- käytettävä data sekä
- liiketoimintaympäristön avoimuus.<sup>76</sup>

Ihmiskeskeisen tiedon hyödynnettävyydellä tarkoitetaan sitä, että yksilöt tulisi nähdä aktiivisina toimijoina, ei vain pelkästään toiminnan kohteina. Ihmisillä tulisi olla oikeuksia omiin tietoihinsa sekä myös todellisia keinoja tiedon hallintaan ja niiden hyödyntämiseen. Yksilöä koskeva tieto eri lähteistä tulisi myös olla saatavissa kootusti ja helposti. Käytettävä

---

<sup>71</sup> Valtiovarainministeriön julkaisu - 37/2017, s.24.

<sup>72</sup> LVM 2/2014, s. 5.

<sup>73</sup> Van Dijk 2012, s. 129.

<sup>74</sup> Manyika ym. 2013, s. 4.

<sup>75</sup> Pitkänen ym. 2013, s. 16.

<sup>76</sup> Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 61/2017, s. 5-6.

data -periaate tarkoittaa selvityksen mukaan sitä, että *rekistereihin ihmisistä kerätty tieto tulisi nähdä uudelleen käytettävänä resurssina*. Kolmannella periaatteella, eli liiketoimintaympäristön avoimuudella taas tarkoitetaan liiketoimintamalleja, joissa asiakkuuden vaihto on helppoa ja tieto seuraa ihmisten mukana. Vaikka julkishallinto ei toimi liiketoiminnallisin perustein, julkinen sektori voi pyrkiä luomaan avointa toimintaympäristöä.<sup>77</sup>

Omadatalle ei Suomen lainsäädännössä ole tällä hetkellä määritelmää. Omadata käsitetään henkilötiedoksi, jota yksilö itse voi hallita. Esimerkiksi rikosrekisteri on sellaista henkilötietoa, jota yksilö ei voi hallita ja määritellä sen käyttöä. Omadata on siis henkilötietoa, mutta kaikki henkilötieto ei ole omadataa. Valtiovarainministeriön selvityksen mukaan, *mikäli yksilöllä ei ole mahdollisuutta hyödyntää itse ja hallinnoida jonkun muun hänestä keräämää henkilötietoa, niin sitä ei voida vielä kutsua My Dataksi*.<sup>78</sup> Valtioneuvoston selvityksessä on esitetty neljä erilaista luokkaa sen mukaan, millaisia rekisteröidyn oikeudet ovat käsitellyn tiedon suhteen. Nämä neljä luokkaa ovat: salaiset henkilötiedot, joihin yksilöllä ei ole pääsyä; tieto, johon liittyy arvioitavia riskejä; laissa määriteltyjen viranomaisten tehtävien tai palvelussuhteen pohjalta käsitelty tieto; sekä suostumuksen pohjalta käsitelty tieto.<sup>79</sup> Luokittelu kuvaa hyvin sitä, miten omadata-mallia ei voida soveltaa kaikkeen olemassa olevaan henkilötietoon. Sovellettavan henkilötiedon osalta on tehtävä arvio siitä, voiko yksilö todellisuudessa hallinnoida henkilötietoaan, vai onko se lain mukaan määritelty viranomaisen tehtäviin, ja sitä kautta yksilön hallinnoinnin ulottumattomiin.

Henkilötiedon hallinta voi olla oikeudesta riippuen joko passiivista tai aktiivista. Liikenne- ja viestintäministeriön selvityksessä henkilötiedon hallinta on jaoteltu passiivisiin sekä aktiivisiin oikeuksiin. Passiivisia oikeuksia ovat:

- Oikeus tietää – yksilöllä on oikeus tietää, mitä kaikkea henkilötietoa hänestä on olemassa.
- Oikeus nähdä – yksilö pääsee näkemään itseään koskevan henkilötiedon.
- Oikeus oikaista – yksilö voi oikaista häntä koskevan väärän henkilötiedon.

<sup>77</sup> Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 61/2017 s. 5-6.

<sup>78</sup> Valtiovarainministeriön julkaisuja 37/2017, s.12.

<sup>79</sup> Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 61/2017, s. 14-15.

- Oikeus valvoa – yksilö voi tarkistaa, kuka hänen henkilötietoaan käsittelee ja miksi.<sup>80</sup>

Yksilön aktiivisia omadata-oikeuksia taas ovat:

- Oikeus saada – yksilö saa halutessaan tiedon itselleen uudelleenkäytettävässä muodossa ja saa hyödyntää sitä itse haluamallaan tavalla.
- Oikeus jakaa – yksilö voi julkaista tiedon eteenpäin kolmansille osapuolille, jos tähän on tekniset edellytykset.
- Oikeus poistaa – yksilö voi poistaa henkilötietonsa sieltä missä ne ovat.<sup>81</sup>

Passiiviset oikeudet ovat jo nykyisessä lainsäädännössä turvattuja oikeuksia. Henkilörekistereihin liitetty tarkastusoikeuden vaatimus mahdollistaa yksilön itseään koskevan tiedon saamisen, tiedon korjaamisen sekä tietyissä tilanteissa myös tiedon poistamisen.<sup>82</sup> Aktiivisien oikeuksien osalta taas yksilöllä on rajoitettu oikeus. Henkilötiedot tulee poistaa rekisteröidyn pyynnöstä, mikäli kyseessä ei ole tietosuoja-asetuksen 17 artiklan 3 kohtaan perustuva henkilötietojen käsittelyoikeus.<sup>83</sup> Aktiivinen omadataan perustuva oikeus mahdollistaa yksilölle henkilökohtaisempaa, yksilön tarpeisiin räätälöityjä palveluita, mahdollisuuden omien käyttäytymisten ja tottumusten seurantaan sekä vahvistaa yksilön asemaa yritysten ja julkisen hallinnon tiedonhallinnan keskellä.<sup>84</sup>

Perusidea ehdotetuksi omadata-infraksi on niin kutsuttu omadata-tili. Yksittäiselle henkilölle omadata-tili olisi henkilötietojen hallintakeskus. Tilillä yksilö voisi antaa palveluille oikeuden saada hänen henkilötietojaan. Tili tallentaisi tiedot siitä, miten hänen henkilökohtaiset tiedot ovat yhteydessä eri palveluihin, sekä suostumukset yksilön antaman tiedon käyttämiseen. Omadata-tiliä tarjoaisivat organisaatiot, jotka toimisivat

---

<sup>80</sup> LVM 2/2014, s. 19. Liikenne- ja viestintäministeriö julkaisi uuden version heinäkuussa 2018 LVM 2/2014 selvityksestä (MyData – johdatus ihmiskeskeiseen henkilötiedon hyödyntämiseen), jossa on päivitetty tilanne sen osalta, miten MyData on kehittynyt vuodesta 2014 tähän päivään asti. Päivitetystä julkaisusta esitellään myös uusia teknologisia ratkaisuja sekä pilottihankkeita MyDatana osalta. Selvityksen mukaan siinä ”valoitetaan, mitä hyötyjä MyDatasta on, ketkä sen parissa toimivat ja millainen on näkyvässä oleva polku käytännön toteutuksiin ja kohti yhteentoimivaa ja ihmiskeskeistä henkilötiedon jakamisen ekosysteemiä”, LVM 3/2018, s. 12.

<sup>81</sup> LVM 2/2014, s. 19.

<sup>82</sup> Henkilötietolain 6-luku käsittelee rekisteröidyn oikeuksia sekä niihin liittyviä rajoituksia. Henkilötietolain nykyinen sääntely rekisteröidyn oikeuksien suhteen on suppeampi kuin yleisen tietosuoja-asetuksen asettamat oikeudet.

<sup>83</sup> Tietosuoja-asetuksen myötä käytetään termiä ”oikeus tulla unohdetuksi”, joka tarkoittaa rekisteröidyn oikeutta saada rekisterinpitäjä poistamaan rekisteröityä koskevat henkilötiedot.

<sup>84</sup> Poikola ym. 2015, s. 4.



omadataoperaattoreina. Omadata-tilin ensisijainen tehtävä olisi suostumuksen hallinta, eli tietoja ei välttämättä lähetetä varsinaiselle omadata-tilille, vaan sen avulla vain hallinnoidaan henkilötietoa. Sovellusohjelmointirajapinnat<sup>85</sup> mahdollistaisivat tiedonlähteiden ja datan käyttäjien välisen yhteyden, joten tieto liikkuisi suoraan rekisteristä toiseen perustuen yksilön antamaan suostumukseen.<sup>86</sup>

### 3.2 Avoin data

Julkisia tietovarantoja on ryhdytty avaamaan laajasti niin Suomessa kuin muuallakin maailmassa kansalaisten ja yritysten käyttöön. Avoin data tarkoittaa organisaation tuottamaa tai hallinnoimaa tietoa, joka on koneluettavassa muodossa maksutta kenen tahansa hyödynnettävissä, muokattavissa sekä jaettavissa yksityisiin että kaupallisiin tarkoituksiin.<sup>87</sup> Avoin data on laillisesti uudelleenkäytettävissä siten, että dataa ei ole lisensoitu tarkoituksena rajoittaa käyttäjäkuntaa tai käyttötarkoitusta.<sup>88</sup> Avoin data ei kuitenkaan tarkoita samaa asiaa kuin julkinen tieto. Julkiseen tietoon on kaikilla pääsy, mutta niiden hyödyntämiseen liittyy erilaisia rajoitteita.<sup>89</sup> Julkista tietoa ei voida automaattisesti saada maksutta hyödynnettäväksi esimerkiksi kaupallisiin tarkoituksiin, sillä tiedon hyödyntämistä säädellään lainsäädännön tasolla.

Avoimen tiedon lähtökohtana on 17.11.2003 annettu Euroopan parlamentin ja neuvoston direktiivi julkisen sektorin hallussa olevien tietojen uudelleenkäytöstä eli niin sanottu PSI-direktiivi. PSI-direktiivin tarkoituksena on parantaa julkisen sektorin tiedon saatavuutta jäsenvaltioissa yhdenmukaistamalla sääntelyä sekä poistamalla tiedon uudelleenkäytön esteitä. Direktiivin johdanto-osan 5 mukaan julkisen sektorin tieto on merkittävä raaka-aine digitaalisissa palveluissa ja siitä tulee yhä merkittävämpi sisällönlähde. Laajentamalla mahdollisuuksia käyttää julkisen sektorin mahdollistetaan samalla myös eurooppalaisten yhtiöiden hyödyntää avattuja tietoja ja myötävaikuttaa taloudelliseen kasvuun. 1 artiklan mukaisesti ”direktiivillä vahvistetaan vähimmäissäännöt jäsenvaltioiden julkisen sektorin elinten hallussa olevien asiakirjojen uudelleenkäytölle sekä käytännön keinot niiden

---

<sup>85</sup> Rajapinnoista käytetään yleisimmin nimitystä Application Programming Interface eli API, joiden kautta henkilötieto liikkuu palvelusta toiseen. Ohjelmointirajapinta määrittelee, miten tietoja tai palveluita tarjotaan sovelluksille tai tietojärjestelmille, ks. lisää rajapinnoista esimerkiksi avoin rajapinta [www-sivut tai Kontkanen 2016](http://www.sivut.tai).

<sup>86</sup> Poikola ym. 2015, s. 5-6.

<sup>87</sup> Valtiovarainministeriön tietopolitiikka ja ohjaus.

<sup>88</sup> Kauhanen – Simanainen 2014, s. 4.

<sup>89</sup> Helsinki region info share 2017.

uudelleenkäytön helpottamiseksi”. Johdanto-osan 21 mukaan direktiiviä on sovellettava noudattaen tietosuojan sääntelyä.

Julkisen tiedon avaamista on edistetty hallitustasoisesti. Tiedon avaamisen periaatteet on hyväksytty valtioneuvoston periaatepäätöksessä 3.3.2011. Periaatepäätöksen kohteena on edistää julkisen sektorin ”digitaalisten tietoaisteiden uudelleenkäyttöä, joiden käsittelyyn ei kohdistu lakisääteisiä rajoituksia”<sup>90</sup> Periaatepäätöksen pohjalta asetettiin Avoimen tiedon ohjelma 2013-2015, jonka tavoitteena oli saavuttaa kansainvälisiä, yhteiskunnallisia sekä hallinnollisia hyötyjä. Avoimen tiedon katsottiin olevan perustana avoimuudelle ja tehokkuudelle sekä saavuttavan uusia liiketoiminnallisia mahdollisuuksia. Avoimen tiedon ohjelman päämääränä oli saada kaikki merkittävät julkiset tietovarannot verkossa saataville koneluettavassa muodossa vuoteen 2020 mennessä.<sup>91</sup> Ohjelman päättyttyä julkisia tietovarantoja on Suomessa runsaasti saatavilla liittyen etenkin ympäristöön ja infrastruktuuriin. Tavoitteena on yhä edelleen kiinnittää huomiota siihen, miten tietojen hyödyntämistä voidaan edistää julkisen hallinnon tasolla, ja mitkä ovat julkisen ja yksityisen sektorin roolit.<sup>92</sup>

Avoimella datalla ja omadatalle on tiettyjä liittymäkohtia ja niitä onkin verrattu toisiinsa tulevaisuuden tiedon hallinnan osalta. Molemmat edustavat uudenlaista tiedon hallintaa ja ajattelutavan muutosta, jossa julkisen sektorin hallussa oleva data luovutetaan myös muiden toimijoiden saataville. Molemmissa tarvitaan myös periaatteita, sääntelyä, koneluettavia rajapintoja, standardeja sekä palveluita tiedon hallittuun siirtämiseen.<sup>93</sup> Kuten omadataan, myös julkisen dataan ja sen avaamiseen liittyy erilaisia lakeja, direktiivejä sekä suosituksia, jotka voivat rajoittaa tiedon hyödyntämistä. Avoimen datan osalta on otettava huomioon muun muassa julkisuuslaki, tietosuojalainsäädäntö, maksuperustelaki, tekijänoikeuslaki, kansainväliset suositukset, kilpailulainsäädäntö sekä EU-direktiivit.<sup>94</sup> Avoimen datan nojalla ei kuitenkaan voida loukata yksilön oikeuksia ja avata esimerkiksi henkilötietoja kaikkien saataville. Tässä suhteessa omadata edustaa jatkoa julkisen sektorin tietovarantojen avaamiselle, jossa arvioitavaksi tulee henkilötietojen avaaminen yksilölle

<sup>90</sup> Ehdotus valtioneuvoston periaatepäätökseksi julkisen sektorin digitaalisten tietoaisteiden saatavuuden parantamisesta ja uudelleenkäytön edistämisestä, s. 1.

<sup>91</sup> Avoimen tiedon ohjelman 2013-2015 käynnistäminen, taustamuistio, s. 1-2.

<sup>92</sup> Ks. Avoimen tiedon ohjelman 2013-2015 loppuraportti, jossa kerrotaan ohjelman aikana tehdyistä toimista datan avaamisen edistämiseksi sekä jatkotoimista liittyen tulevaisuuteen (Valtiovarainministeriön raportti – 31/2015).

<sup>93</sup> LVM 2/2014, s. 17.

<sup>94</sup> LVM – Julkinen data – johdatus tietovarantojen avaamiseen, 2010, s. 7.

itselleen. Omadataan ja Avoimeen dataan liittyy osaltaan myös Big Data, jota ei kuitenkaan tässä tutkielmassa käsitellä syvällisemmin.<sup>95</sup>

### 3.3 Suostumushallintapalvelu

Suostumustenhallinnassa tavoitellaan tilannetta, jossa omadata-palveluihin liittyvät käyttäjien suostumukset hallinnoidaan infrastruktuuripalveluna, jota voidaan käyttää sen luottamusverkostoon kuuluvissa palveluissa. Tällöin yksilöivät suostumukset tallennettaisiin koneluettavassa muodossa suostumushallintarekisteriin, jota kautta voitaisiin varmistua siitä, että yksilö todella on antanut suostumuksensa henkilötietojen käsittelyyn.<sup>96</sup> Suostumusten hallinta on julkishallinnossa vasta kehitteillä, joten tarvetta on kartoittaa eri toteutuksia sitä koskien. YTI-hankkeessa on suunniteltu suostumushallintapalvelun erilaisia mahdollisia toteutustapoja, ja sitä, missä suostumuksia hallinnoiva rekisteri voisi tulevaisuudessa sijaita. Väestörekisterikeskuksen vastuulla on tuottaa Suomi.fi-palveluita, jotka sisältävät sellaisia teknisiä ominaisuuksia, joita voidaan hyödyntää suostumushallintarekisterissä.<sup>97</sup>

Yksi vaihtoehto on toteuttaa keskitetty suostumushallinta muiden Suomi.fi-palvelujen yhteyteen. Keskitetty rekisteri tarjoaisi yksilölle mahdollisuuden hallinnoida omia, viranomaisen rekistereissä olevia tietojaan yhdestä paikasta. Suomi.fi-portaali olisi keskitetty kanava, jonne suostumukset koottaisiin. Toinen vaihtoehto olisi hajautettu suostumustenhallinta, jossa jokaisella toimijalla olisi oma suostumushallintapalvelunsa. YTI-hankkeen omadata-työpaketin myötä on myös tarkoitus selvittää ja ratkoa sellaisia kysymyksiä omien tietojen hallintaan liittyen, jotka koskettavat koko julkisen hallinnon sektoria. Tulevaisuuden tavoitteena on nähdä julkinen hallinto enemmän yhtenäisenä kokonaisuutena sen sijaan, että jokainen virasto toimii omalla alueellaan ilman yhteyttä

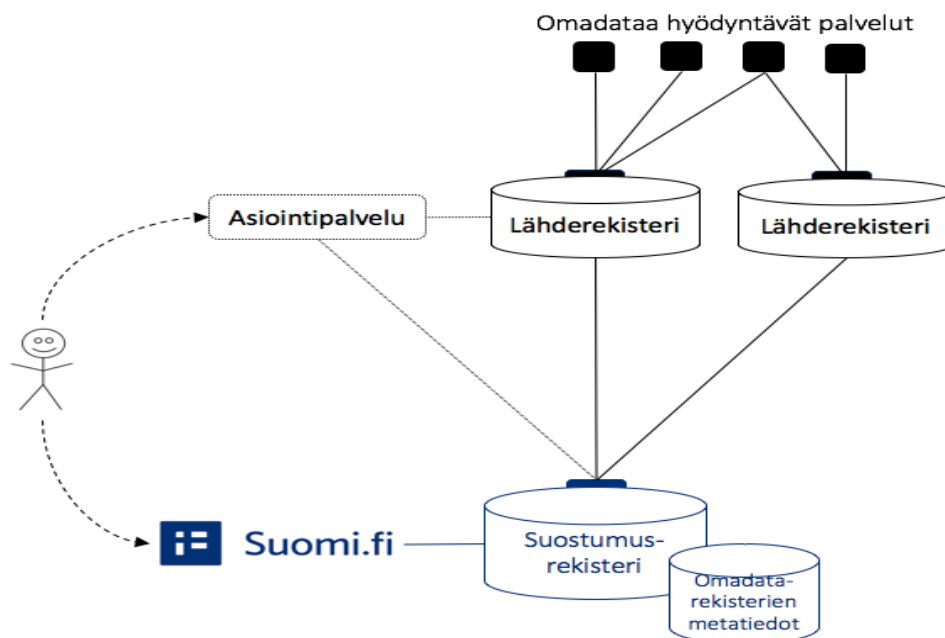
---

<sup>95</sup> Big Data tarkoittaa suurten ja järjestelemättömien tietomassojen keräämistä ja hyödyntämistä. Big Dataan liittyy haaste sen osalta, että kun data kerran julkaistaan, sitä ei saada enää pois. Ajan kuluessa analyttiset tekniikat yhdistellyn tiedon osalta paranevat, jotka taas voivat paljastaa tietoa alkuperäisistä tiedoista. Tästä seuraa se, että paljastuneet tiedot tulevat yhä haavoittuviksi uudelleenidentifiointiin, ellei tietojenkäsittelyssä käytetä menetelmiä, joilla suojataan uudelleenkäyttöä. Ks. lisää Big Datasta Narayanan – Huey – W. Felten 2016, s. 357.

<sup>96</sup> YTI-hankkeen Omadata-työpakettiin liittyen järjestettiin työpaja, jossa työstettiin julkishallinnon omadatan mahdollisuuksia sekä toteutustapoja. Työpajan tuloksena syntyi työpajaversioinen dokumentti ”suostumusperusteinen henkilötietojen hallinta”, jossa on esitelty mahdollisia suostumushallintapalvelun toteutustapoja. Korostettakoon kuitenkin edelleen se, että kaikki tässä esitetyt vaihtoehdot ovat skenaarioita, eikä niiden toteuttamisesta ole lopullisia päätöksiä tehty. Väestörekisterikeskus 2017.

<sup>97</sup> Lisätietoja Suomi.fi-palveluista ja niiden sisällöistä löytyy Väestörekisterikeskuksen ylläpitämästä suomi.fi-sivustolta osoitteesta <https://suomi.fi>.

muihin viranomaisiin. Tällä edistetään myös tulevaisuuden tiedon hallintaa siten, että julkinen hallinto toimii tehokkaana kokonaisuuten ja myös kansalainen voi nähdä viranomaisen yhtenä suurena toimijana. Alla on esitetty kaksi potentiaalista vaihtoehtoa siitä, miten suostumustenhallintapalvelu voitaisiin tulevaisuudessa toteuttaa.

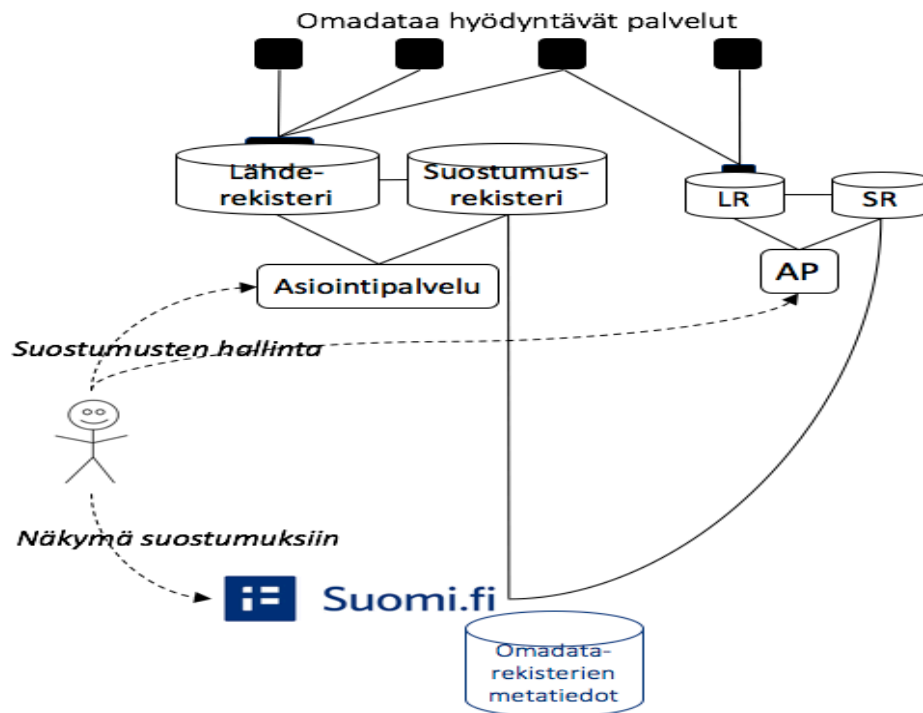


Keskitetty Suomi.fi-suostumustenhallinta -vaihtoehto<sup>98</sup>

Keskitettyssä suostumushallintapalvelussa kaikki julkishallinnon omadataan pohjautuvat suostumukset säilytettäisiin ja hallinnoitaisiin keskitetyn ratkaisun avulla, joka olisi osa Suomi.fi-palveluita. Käyttäjä voisi hallinnoida omia suostumuksiaan Suomi.fi-palvelussa ollessaan sinne kirjautuneena. Suostumusrekisteriin varsinaisia henkilötietoja ei tallennettaisi, vaan ainoastaan tieto suostumuksen olemassaolosta. Tällöin suostumusrekisteristä muodostuisi henkilörekisteri, jossa säilytettäisiin tieto siitä, mihin rekistereihin ja minkä henkilötiedon osalta yksilö on antanut suostumuksensa. Varsinainen henkilötiedon luovutus tapahtuisi sektori- tai virastokohtaisista rekistereistä. Kun henkilötiedon luovutus tulisi ajankohtaiseksi, eli omadataa hyödyntävä palvelu pyytää lähderekisteristä henkilötietoja, lähderekisteri tarkastaisi luovutuspyynnön saatuaan keskitetystä suostumusrekisteristä tiedon siitä, onko kyseisellä palvelulla oikeus pyydettyihin tietoihin. Mikäli suostumus olisi olemassa, eli henkilötiedon käsittelyperuste täyttyy, lähderekisteri luovuttaisi tiedot.<sup>99</sup>

<sup>98</sup> Väestörekisterikeskus 2017, s. 41.

<sup>99</sup> Väestörekisterikeskus 2017, s. 38.



Virastokohtainen, hajautettu suostumushallinta<sup>100</sup>

Hajautettu suostumushallinta taas kuvan mukaisesti olisi ratkaisu, jossa julkishallinnon suostumukset säilytettäisiin sektori- tai virastokohtaisissa ratkaisuissa ja Suomi.fi-palveluiden kautta olisi keskitetty näkymä kaikkiin henkilön suostumuksiin. Julkishallinnon organisaatioilla, jotka tuottaisivat omadataa, olisi omat suostumushallintarekisterit joiden kautta henkilö antaisi suostumuksia. Yksittäisiin suostumusrekistereihin toteutettaisiin rajapinta Suomi.fi-palveluun, johon koottaisiin keskitetysti näkymä yksilön antamista suostumuksista.<sup>101</sup> Koska Suomi.fi-palvelussa sijaitsevat omadata-rekisterien metatiedot tuotaisiin vain näytettäväksi rekisteröidylle hänen ollessaan kirjautuneena palveluun, ei Suomi.fi-palveluun syntyisi omaa suostumushallintaa.

### 3.4 Luvitus

Omadata-ajatteluun liittyy keskeisenä ajatuksena yksilön henkilötietojen luvittaminen. Luvituksella tarkoitetaan suostumuksia, joiden myötä yksilö antaa rekisterinpitäjälle oikeuden käsitellä hänen henkilötietojaan. Suostumukset ovat tietoisia ja vapaaehtoisia omien tietojen käytön hyväksymisiä, ja suostumuksen antajan tulee tietää mihin tarkoitukseen henkilötietoja käsitellään.<sup>102</sup> Suostumushallinnan kautta yksilö hallinnoi

<sup>100</sup> Väestörekisterikeskus 2017, s. 42.

<sup>101</sup> Ibid. s. 41.

<sup>102</sup> Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 61/2017, s.7.

omien henkilötietojensa käytöstä jopa yksittäisen henkilötiedon osalta. Kansalainen harvoin tietää millä tavoin häntä koskevaa tietoa käytetään, eikä hän voi tehdä valintoja itseään koskevien tietojen käsittelystä.<sup>103</sup> Henkilötietojen luvittamisen kautta yksilö voi antaa suostumuksia liittyen henkilötietojen käyttöön sellaisille toimijoille, jotka palvelevat hänen tarkoituksiaan ja kiinnostuksenkohteitaan. Toisaalta taas kansalainen voi kieltää henkilötietojen käsittelyn sellaisen rekisterinpitäjän toimesta, jonka ei katso olevan oikeutettu tai tarpeellinen tietojensa käsittelyyn.

Kuten edellä 3.1 kappaleessa on lueteltu, rekisteröidyn oikeuksien luokista ilmenee henkilötietojen jako eri luokkiin sen mukaan, mikä on rekisteröidyn oikeuksien suhde tietoihin. Rekisterinpitäjä voi käsitellä henkilötietoja eri käsittelyperustein lainkohdasta riippuen. Omatantuvittamisen voidaan ulottaa koskemaan ainoastaan suostumuksen perusteella käsiteltäviä henkilötietoja. Rekisteröity ei siis voi jatkossakaan säädellä sitä, voiko rekisterinpitäjä käsitellä lakiin perustuen hänen henkilötietojensa vai ei. Mikäli laissa on asetettu rekisterinpitäjälle tehtävä, johon kuuluu määriteltyjen henkilötietojen käsittely, ei rekisteröity voi kieltää tällaisten tietojen käsittelyä.

Nykyisessä lainsäädännössä viranomaisen säätelee sitä, mitä tietoja voidaan luovuttaa rekisteristä kolmannelle osapuolelle. Pääsääntöisesti henkilötietojen luovutus viranomaisten rekistereistä pohjautuu lakiin viranomaisten toiminnan julkisuudesta, henkilötietolakiin sekä lukuisiin erityislainsäädöksiin. Julkisuuslaki sisältää periaatteet sekä salassapitomääräykset. Julkisuuslain mukaan tietoa voidaan luovuttaa henkilörekisteristä, jos tiedot vastaanottavalla taholla on oikeus käsitellä tietoa henkilötietolain sekä erityislakien rajaamalla tavalla.<sup>104</sup>

Erityislainsäädännöstä esimerkkinä voidaan ottaa Väestörekisterikeskuksen ylläpitämä väestörekisteri, joka sisältää henkilötiedot jokaisesta Suomen kansalaisesta. Väestörekisterikeskuksen tietojen luovutusta säätelee laki väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista (661/2009). Väestörekisterikeskus luovuttaa henkilötietoja sekä julkishallinnon että yksityisen sektorin toimijoille lainsäädännön mukaisesti. Lain neljäs luku säätelee tarkemmin tietojen julkisuudesta ja niiden luovuttamisesta. Lain 28 §:n mukaisesti *väestötietojärjestelmän tietoja voidaan luovuttaa vain, jos tässä laissa säädetty edellytykset tietojen luovuttamiselle ovat olemassa eikä henkilön oikeudesta kieltää tietojensa luovuttaminen muuta johdu*. Nykyisen lainsäädännön

<sup>103</sup> Valtioneuvoston viikko, liite Virallisen lehden numeroon 104/11.9.2017, s. 13.

<sup>104</sup> Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 61/2017, s.78.

mukaan yksilöllä on oikeus kieltää tietojensa luovuttaminen. Väestörekisterikeskuksen tietojen luovutuskiellon informaation mukaisesti ”henkilöllä on oikeus kieltää tietojensa luovuttaminen väestötietojärjestelmästä henkilötietolain (523/1999) 30 §:n nojalla suoramarkkinointia, markkina- ja mielipidetutkimusta, henkilömatrikkelia ja sukututkimusta varten sekä väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista annetun lain 35 §:n nojalla yhteystietojensa luovuttaminen yhteys-, osoite- tai muuna vastaavana tietopalveluna sekä tietojensa luovutus asiakasrekisterin tai muun vastaavan rekisterin päivitystä varten”.<sup>105</sup> Yksilön luvittaessa omia henkilötietoja tietojen luovutuksesta päättävä taho olisi rekisteröity itse. Valtioneuvoston selvityksessä on selvitetty sitä, miten Väestörekisterikeskuksen luovutuskäytäntö muuttuisi omadata-mallin kehityksen myötä. Selvityksen ehdotuksen mukaan omadata muuttaisi nykyiset tietoluvat yksilöiden hallitsemiksi käyttöluviksi. Tällöin sopimuksen tietojen käytöstä tekisi se henkilö, jonka tiedoista on kysymys.<sup>106</sup> Tällöin viranomaisen rooli kolmansille suostumuksenvaraisten tietojen luovuttamiseen pienenesi huomattavasti nykyisestä tietoluvan mukaisesta mallista yksilökeskeiseen tietojen luovutukseen. Luvussa 5 on tarkasteltu tarkemmin tätä muutosta.

### 3.5 Omadata ja lainsäädäntö

#### 3.5.1 Yleistä

Omadatasta käydään paljon keskustelua ja se liittyy vahvasti tulevaisuuden skenaarioihin siitä, miten henkilötietoja tulevaisuuden digitalisoituneessa maailmassa tulisi hallita. Omadata on maailmanlaajuisesti kehitysvaiheessa oleva ilmiö, jonka ympärille on kertymässä kasvavaa vauhtia teknologiaa ja liiketoimintaa ja yritykset yhä enenemässä määrin ovat kiinnostuneista henkilötietojen uudenlaisen hyödyntämisen mahdollisuuksista.<sup>107</sup> Juha Sipilän hallitusohjelmassa on hallituskauden kärkihankkeiden osalta yhdeksi tavoitteeksi asetettu digitalisoida julkiset palvelut, johon osaltaan kuuluu se, että *vahvistetaan kansalaisten oikeutta valvoa ja päättää itseään koskevien tietojen käytöstä, samalla varmistaen tietojen sujuva siirtyminen viranomaisten välillä.*<sup>108</sup> Jotta omadata-mallia voidaan tehokkaasti toteuttaa, on lainsäädännössä tunnistettava omadatan mahdolliset

<sup>105</sup> Väestörekisterikeskuksen www-sivut.

<sup>106</sup> Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 61/2017, s. 48.

<sup>107</sup> LVM 2/2014, s.9.

<sup>108</sup> Hallituksen julkaisusarja 10/2015, s. 26.

vaikutukset. Tällä hetkellä julkista hallintoa koskeva lainsäädäntö ei lähde yksilön oikeuksista omiin tietoihinsa, vaan enemmänkin viranomaisen on henkilötietojen käsittelyn määrittelevä taho. Nykypäivänä suunta on kuitenkin kohti yksilön itsemääräämisoikeuden korostamista, eikä julkisen sektorin katsota enää voivan vapaasti määrätä keräämistään henkilötiedoista.<sup>109</sup> Kuten edellä on mainittu, henkilötietojen käsittely nykytilassa pohjautuu pitkälti henkilötietolakiin, julkisuuslakiin sekä erityislainsäädäntöihin. Eri raporteissa lainsäädännön osalta on kuitenkin tunnistettu se, että lainsäädäntöä tulee muuttaa kansallisesti, jotta ensinnäkin EU:n tietosuojasetus tehokkaasti toteutuu ja toisaalta myös kansallinen digitalisaatio etenee mahdollisimman tehokkaasti.

Tällä hetkellä tiedon hallintaan kansallisella tasolla laajalti tulee vaikuttamaan valmisteilla oleva laki tiedonhallinnan lainsäädännöstä, jonka on tarkoitus tulla voimaan vuoden 2019 alusta lähtien. Tiedonhallintalaista on julkaistu vuonna 2017 työryhmän raportti lain kehittämissuunnitelmista ja sen pohjalta on tarkoitus julkaista hallituksen esitys syksyllä 2018. Jo työryhmän raportin tiivistelmässä tulee ilmi se, että tällä hetkellä tiedonhallintaa koskeva lainsäädäntö on hajanaista, runsasta ja epätarkkaa, eikä se vastaa digitalisoituneen yhteiskunnan vaatimiin muutoksiin.<sup>110</sup> Nykymuotoinen tiedonhallinta ja tietoaisteiden muodostuminen perustuu viranomaisten erillisyyseriaatteeseen, jossa kukin viranomaisen muodostaa oman tiedonhallinnan yksikkönsä ja siten myös vastaa tietojen hallinnasta. Tämä taas on johtanut siihen, että viranomaiset keräävät tietoja *vain omien tehtäviensä ja käyttötarpeensa mukaisesti, eli tietoaisteiden muodostamisesta puuttuu kokonaisprosessiajattelu.*<sup>111</sup> Raportista ilmenee lain tavoitetila henkilötietojen käsittelyn suhteen; tavoitteena on tietojen sujuvampi liikkuminen viranomaisten välillä siten, että tietoja kysytään yksilöltä vain kerran ja tämän jälkeen tieto olisi käytettävissä viranomaisella lakisääteisen tehtävän hoitamiseen ilman erityislainsäädäntöön pohjautuvaa sääntelyä.<sup>112</sup> Tiedonhallinnan laki pyrkii vähentämään hallinnollista prosessia viranomaisten välillä tiedon liikkuvuuden suhteen. Koska henkilötietoja kerätään myös viranomaisten tarpeisiin yhä kiihtyvään tahtiin, tulisi kokonaisuuden hallitseminen olla itsestäänselvyys. Henkilötietojen käsittelyn läpinäkyvyyden kannalta lainsäädännön selkeyttäminen on ensiarvoisen tärkeää. Erityislainsäädäntöä tarvitaan, mutta suuret linjat tulisi säätää yleislainsäädännöllä.

---

<sup>109</sup> Saarenpää 2012, s. 509.

<sup>110</sup> Valtiovarainministeriön julkaisu – 37/2017, s. 3.

<sup>111</sup> Valtiovarainministeriön julkaisu – 37/2017, s. 92.

<sup>112</sup> Valtiovarainministeriön julkaisu – 37/2017, s. 23.



### 3.5.2 Hallituksen esitys liikenteen turvallisuusvirastosta

Tutkielmaa kirjoitettaessa on elokuuhun 2018 mennessä ilmestynyt muutamia hallituksen esityksiä, joissa on nimenomaisesti mainittu omadata. Hallituksen esitys laiksi liikenteen palveluista annetun lain muuttamiseksi ja eräksi siihen liittyviksi laeiksi nostaa omadata-käsitteen useassa kohdassa esille ja edistää omadata-mallin käyttöönottoa. Esityksen mukaan omadatassa keskeisintä on *henkilön mahdollisuus siirtää tietojaan uudelleen käytettävässä muodossa itselleen, määräämäänsä paikkaan tai valtuuttamaansa palveluun hyödynnettäväksi* eli tietosuoja-asetuksen 20 artiklan mukainen oikeus siirtää tiedot järjestelmästä toiseen.<sup>113</sup> Lakiesitys velvoittaa Liikenteen turvallisuusvirastoa luovuttamaan julkiset tiedot avoimen rajapinnan kautta. Lain 3 luku tietojen luovuttamisesta, sen 8 § tulisi säätelämään henkilön omien tietojen hallintaa.

”Liikenteen turvallisuusviraston on mahdollistettava rekisteröidyn omien tietojen hakeminen ja kopioiminen toiseen tietojärjestelmään avoimen rajapinnan välityksellä koneluettavassa muodossa. Tämä ei koske sellaisia salassa pidettäviä tietoja, jotka Liikenteen turvallisuusvirasto on saanut rikos- tai sakkorekisteristä eikä valvonta- ja seuraamustietoja.”

Säännös on askel uuteen malliin henkilötietojen käsittelyssä, jossa omadata-malli otetaan huomioon jo lainsäädäntövaiheessa. Kyseinen laki säätelisi siten, että Liikenteen turvallisuusviraston olisi tosiasiallisesti toteutettava uusia rajapintoja tietojen siirrettävyyden mahdollistamiseksi ja mahdollistamaan omadataan perustuvien palvelujen syntymistä. Kuten tiedonhallinnan lainsäädännön kehittämislinjausten työryhmän raportissa on yleisen tietosuoja-asetuksen 20 artiklasta mainittu, tiedonsiirtoon liittyvä säännös ei muodosta viranomaiselle velvollisuutta tuottaa lakisäätteisten tehtävien yhteydessä tietoaineistoja siirtoa edellyttävään muotoon.<sup>114</sup> Hallituksen esityksessä on tämä huomioitu säätämällä tosiasiallisesti avointen rajapintojen rakentamisesta, jolloin tiedon siirto on mahdollista sähköisessä muodossa suoraan rekisterinpitäjältä toiselle. Huomionarvoista on se, että henkilön siirtäessä tietoja järjestelmästä toiseen, säilyvät siirrettävät tiedot tiedon luovuttajan rekisterissä, eikä sen osalta esimerkiksi siirrettävää henkilötietoa poisteta. Tieto vain siirretään järjestelmästä toiseen, mutta se säilyy myös alkuperäisessä järjestelmässä.

---

<sup>113</sup> HE 145/2017, Nykytila, luku 2.

<sup>114</sup> Valtiovarainministeriö, 2017, s. 25.

### 3.5.3 Koski-rekisteri

Omadata-mallia tukeva, vuoden 2018 alusta voimaan tullut lainsäädäntö on laki valtakunnallisista opinto- ja tutkintorekistereistä (884/2017) eli niin sanottu Koski-laki. Koski-rekisteriin on koottu kunkin kansalaisen tiedot koulutuksesta yksittäisestä opintosuorituksesta suoritettuihin tutkintoihin asti. Koski-rekisteri sisältää tiedot myös henkilöiden opinto-oikeuksista sekä suoritettujen tutkintojen sisällöstä ja vaatimuksista. Rekisteristä kansalaisten lisäksi myös viranomaiset saavat tarvittavat koulutustiedot keskitetysti yhdestä paikasta.<sup>115</sup> Laki paitsi mahdollistaa opintosuoritusten tietoturvallisen luovuttamisen edelleen, turvaa opintosuoritusten- ja tutkintotietojen yhdenmukaisuuden sekä edistää koulutukseen hakemista ja elinikäistä oppimista.

Lain 10 §:ssä säädetään tietojen luovuttamisesta tietovarannosta. Pykälän mukaan tietovarannosta tietoja voidaan luovuttaa viranomaiselle laissa säädetyn tehtävän hoitamiseksi, koulutusrahastolle lain säännöksen perusteella sekä sille, jolla yksilöidyn suostumuksen perusteella on oikeus saada rekisterin tietoja. Yksilöidystä suostumuksesta säädetään edelleen lain 29 §:ssä: ”Henkilö, josta on tallennettu tietoja tässä laissa tarkoitettuun rekisteriin tai tietovarantoon, voi palvelussa antaa yksilöidyn suostumuksensa rekisterissä tai tietovarannossa olevan tiedon luovuttamiseen viranomaiselle tai muulle taholle sekä peruuttaa antamansa suostumuksen”. Tiedot luovutetaan sähköisessä muodossa eikä luovutettavia tietoja tallenneta Opetushallituksen palveluun. Koski-palvelu avattiin 2018 alusta ja sen on tarkoitus olla käytössä lain vaatimusten mukaisesti vuonna 2019. Lain 29 §:n mukainen suostumustenhallinta ei ole vielä palveluun toteutettu, mutta se on tarkoitus toteuttaa osana YTI-hankkeen omadata-työpaketin pilottia. Työpaketissa toteutetaan suostumushallintapalvelu Koski-rekisteriin yhteistyössä Opetushallituksen sekä Väestörekisterikeskuksen kanssa.

Koski-rekisteri on ensimmäinen askel uuteen omadata-malliin, jossa lainsäädäntö mahdollistaa tietojen luovutuksen paitsi viranomaiselle lakisäätöisen tehtävän hoitamiseksi, myös yksilön oman suostumuksen kautta. Lain hallituksen esityksessä todetaan, että henkilön suostumukseen perustuvia luovutuksia ei rajattaisi siten, että se koskisi vaan viranomaisia, vaan tietoja voidaan luovuttaa myös yksityisille toimijoille.<sup>116</sup> Sääntely mahdollistaa aiempaa tehokkaammin yksilön oikeuksia omiin opintotietoihin. Kansalainen

---

<sup>115</sup> Opetushallituksen www-sivut.

<sup>116</sup> HE 72/2017, yksityiskohtaiset perustelut.

voi päättää ilman lain rajoituksia siitä, kenelle lakisääteisten käsittelijöiden lisäksi hän haluaa opiskelu- ja tutkintotietojaan luovuttaa. Esimerkiksi työnhaussa yksilö voisi mahdollisesti luovuttaa potentiaaliselle työnantajalle omia opintosuoritustietojaan. Kyseinen mahdollisuus herättää myös kysymyksiä yksilön sekä rekisterinpitäjän vastuukysymyksistä. Hallituksen esityksessä todetaan, että Opetushallituksella ei olisi tosiasiallista harkintavaltaa sen suhteen, luovutetaanko pyydetty tiedot vai ei, sillä luovutus perustuu lakiin tai yksilön antamaan suostumukseen.<sup>117</sup>

### 3.6 Omadatan kansainvälinen kehitys

#### 3.6.1 Yleisesti

Omadata on käsitteenä uusi myös muuallakin kuin Suomessa. Käsitteenä omadatan tai Mydatan alkuperä tulee Iso-Britanniasta, sen vuoden 2011 kuluttajastrategiasta.<sup>118</sup> Useissa maissa on erilaisia omadataan liittyviä hankkeita tai erilaisia siihen perustuvia toteutuksia. Esimerkiksi Yhdysvalloissa on kehitetty omadatan yksinkertainen muoto, jonka avulla kuluttajat saavat energiankulutus- ja terveysdatansa itselleen. Nämä niin kutsutut ”green button” ja ”blue button” ovat alun perin kehitetty sotaveteraanien tarpeisiin, jotta he pystyisivät käyttämään erikoislääkäripalveluja vammojen hoidossa. Vaikka toteutus on hyvin yksinkertainen, on tämä ollut askel suuntaan, jossa henkilötietoja ei tarvitse toimittaa paperitulosteena. Minimitoteutusta tätä taas voidaan pitää siitä syystä, että henkilötiedot tulee manuaalisesti ladata sen sijaan että tiedot voisi siirtää automaattisesti rajapintojen kautta.<sup>119</sup> Sveitsissä taas on terveystietoihin perustuva MIDATA-alusta, jonne yksilö voi kerätä terveystietonsa sekä jakaa tietoja haluamallaan tavoilla. MIDATA: aa varten on perustettu erillinen osuuskunta, joka tukee, hallinnoi ja päättää dataan liittyvistä asioista.<sup>120</sup>

Kansainvälisesti on siis useissa eri maissa ollut kokeiluhankkeita omadataan liittyen. Usein ne liittyvät yksilön ja yrityksen väliseen tietojen vaihtoon. Tällöin valtion hallinnoima, perusrekistereissä oleva henkilötieto ei ole mukana kokeilussa, vaan toteutus liittyy asiakkaan tekemiin toimiin ja niiden johdosta kerättyyn henkilötietoon. Tietävästi ei ole toteutettu KOSKI-rekisterin tyylistä, suostumukseen perustuvaa henkilötietojen hallintaa,

<sup>117</sup> HE 72/2017, yksityiskohtaiset perustelut.

<sup>118</sup> LVM 2/2014, s. 12.

<sup>119</sup> LVM 2/2014, s. 29. ks. lisää The Green Button [www-sivuilla](http://www.sivuilla).

<sup>120</sup> MIDATA 2017 s. 2. Ks. lisää Sveitsin MIDATA:sta sen kotisivuilta osoitteesta <https://midata.coop/#about>.

jossa luovutettava tieto on peräisin viranomaisen rekisteristä. Perusrekisterissä olevaan henkilötiedon luovutukseen liittyy erilaista sääntelyä verrattuna siihen, että luovutettavana oleva henkilötieto on yksilön itsensä tuottamaa dataa.

### 3.6.2 Ranska

*” If I (an organization) can use your data, you can too... however you please.”*

Ranskassa aloitettiin vuonna 2012 omadataan pohjautuva projekti nimeltään MesInfos. MesInfos-projekti perustuu yllä olevaan ideaan henkilötiedon jakamisesta. Henkilötietoja keräävät organisaatiot jakavat kyseiset tietokannat tietoja koskevien henkilöiden kanssa. Tästä lähtökohdasta MesInfos on pyrkinyt tutkimaan, mikä voisi olla todellinen paradigman muutos digitaalisessa taloudessa. Projektissa henkilötiedosta käytetään termiä ”Self Data”, joka tarkoittaa henkilötietojen keräämistä, käyttöä ja jakamista yksilöille heidän omalla hallinnallaan yksilöiden omien tarpeiden ja pyrkimyksien toteuttamiseksi.<sup>121</sup>

Vuosien 2013-2014 välillä projektissa toteutettiin ensimmäinen omadataan pohjautuva kokeilu. 300 testajaa saivat heidän henkilötietonsa kuudelta suurelta ranskalaiselta yritykseltä. Jokainen heistä pystyi tallentamaan nämä tiedot heidän henkilökohtaiselle tietopalustalle, joka oli ranskalaisen yrityksen tarjoama Cozy Cloud. Testihenkilö pystyi myös jakamaan omadataa edelleen viidelle eri toimijalle. Esimerkiksi yhden palvelun avulla henkilöt pystyivät saamaan heidän viikoittaiset hiilidioksidipäästönsä ruoan kulutuksensa perusteella. Yksi tärkeimmistä havainnoista kokeilun tuloksena oli se, että henkilökohtaisten tietojen antaminen oli osa organisaation ja asiakkaan luottamuksen rakentamista.<sup>122</sup> Vuosien 2016-2017 aikana pilottia laajennettiin koskemaan 3000 testajaa, jotka saivat käyttöönsä Cozy Cloud: in. Lisäksi pilottiin osallistui aikaisempaa laajempi joukko organisaatioita, jotka keräävä henkilötietoa käyttöönsä.

MesInfos-projektin haasteiksi on huomattu käytötapausten luominen. Projektiin on ollut haastavaa houkutella yrittäjiä kehittyviin markkinoihin, erityisesti kun kyseessä on ollut uudenlainen alusta (Cozy Cloud). Ranskassa tarkoituksena on rakentaa Self Data ekosysteemi, joka piloteista huolimatta on vielä alkuvaiheessa. Ekosysteemiin kuuluisivat yritykset, jotka tarjoavat omadataa yksilöille. Ekosysteemin avulla omadatan käyttö laajenisi

---

<sup>121</sup> MesInfos 2012.

<sup>122</sup> Albarede-Molins, 2016.

yhä suuremmalle joukolle yrityksiä ja yksilöitä. Tarkoituksena Ranskassa on siirtyä piloteista tietojen haltijoiden pitkäaikaiseen sitoutumiseen.<sup>123</sup>

MesInfos-projekti osoittaa sen, että omadataan pohjautuva henkilötietojen käsittely voi toimia käytännössä ja siitä voivat sekä organisaatiot että yksilöt hyötyä. Henkilötiedon yhdistely eri rekistereistä saattaa luoda uusia käyttötarkoituksia henkilötiedolle sekä mahdollisesti myös synnyttää uusia liikeideoita. Ranskan projektissa ei kuitenkaan ole kyse valtion hankkeesta, joten siinä ei pilotoitu julkisen hallinnon organisaatioiden henkilötietoa. On siis huomattava, että yksityisten toimijoiden lähtökohdat henkilötietojen hyödyntämiseen voivat poiketa huomattavasti julkisen sektorin vastaavista, joten käyttötapauksia ei voida suoraan soveltaa julkiselle sektorille. Lisäksi oikeudelliset vastuukysymykset liittyen rekisterinpitäjän henkilötietojen luovuttamiseen voivat olla erilaiset maiden omasta lainsäädännöstä riippuen.

### 3.6.3 Yhdistynyt kuningaskunta

Yhdistyneessä kuningaskunnassa on omadatan käsitteestä käytetty termejä midata, My Data sekä mydata. Mydata on saanut lähtökohtansa taloudellisista intresseistä, jonka tarkoituksena on saada yritykset tehostamaan palveluitaan.<sup>124</sup> Mydatan alkuperä on Yhdistyneen kuningaskunnan vuoden 2011 hallituksen kuluttajastrategiassa, jonka tarkoituksena oli tukea hallituksen kasvustrategiaa. Strategian tavoitteena Mydatan osalta oli auttaa yritysten asiakkaita saamaan pääsy omiin tietoihinsa sekä kontrolloida niitä. Kuluttajilla olisi mahdollisuus saada tietoa omista kulutustottumuksistaan sekä mahdollisesti muuttaa niitä tehokkaampaan suuntaan. Hallitus perusti ohjelman, jota kutsuttiin ”mydata” -nimityksellä. Tällöin yli 20 johtavaa yritystä eri sektorioilta osallistuivat hallituksen ohjelmaan mydatan edistämiseksi.<sup>125</sup> Hallituksen strategian mukaan yksilöiden tuottama data sisältää huomattavan määrän taloudellista arvoa, jota hallinnoi pankit, puhelinyhtiöt, internetyhtiöt sekä muut yrityssektorin toimijat. Edelleen strategiassa korostettiin, että yksilöllä olisi laillinen oikeus saada tieto yrityksen hallussa olevasta henkilötiedosta, mutta tätä oikeutta ei hyödynnetä kovin laajalti. Mydata-ohjelmassa valtion osuus oli tarkoitus olla vähäinen: valtio ei osallistuisi datan käsittelyyn, vaan se tarjoaisi visiota, auttaisi luomaan

---

<sup>123</sup> MesInfos 2017.

<sup>124</sup> Kallasvuo 2015, s. 14-15.

<sup>125</sup> BIS 13.4.2011, s. 6.

tietoisuutta ohjelmasta kansalaisille sekä auttaisi markkinoita toimimaan tehokkaasti ja tietoturvallisesti.<sup>126</sup>

Mydata-ohjelmaa arvioitiin vuonna 2012 avoimen lausuntokierroksen avulla, joka suunnattiin organisaatioille sekä yksityishenkilöille. Lausuntokierroksen tuloksena nousi esiin sääntelyn tarpeellisuus koskien mydataa. Esille nousi muun muassa kysymys siitä, kuinka yritys, joka vastaa kolmannen osapuolen henkilötietopyyntöön liittyen asiakkaan tietoihin voi varmistua siitä, että kolmas osapuoli käyttää tietoja tavalla, jolla asiakas haluaa kolmannen osapuolen käyttävän sitä. Lausunnoissa pohdittiin sitä, voidaanko voimassa olevaa sääntelyä soveltaa mydataan, vai tulisiko säätää kokonaan uutta lainsäädäntöä.<sup>127</sup> Hallitus kokosi lausuntokierroksen pohjalta vastuksen, jonka mukaan kuluttajilla tulisi olla yhtä suuri oikeus saada omat tietonsa siirrettyä koneluettavassa muodossa edelleen kuin yrityksillä on oikeus kerätä tietoja kuluttajista. Hallitus korosti, että mydatan hyödyt edesauttaisivat myös talouden kasvua. Hallitus päätyi ehdottamaan projektin jatkamisen ohella säätämään lailla mydatasta. Lakiehdotuksen mukaan organisaatiot velvoitettiin antamaan kuluttajan pyynnöstä hänen tietonsa kulutuksestaan elektronisessa, koneluettavassa muodossa. Annettava data rajattiin myös koskemaan sellaista kuluttajan tietoa, joka olisi yhdistettävissä kuluttajaan.<sup>128</sup>

Ehdotuksen johdosta päädyttiin säätämään lailla mydatasta, jonka säännökset sisällytettiin Yhdistyneen kuningaskunnan sääntelyyn ”Enterprise and Regulatory Reform Act 2013”. Mydataa koskevat lainsäädännölliset piirteet sisältyvät lain 89-91 kohtiin (Supply of Customer Data), jossa säädetään muun muassa asiakkaan oikeudesta saada henkilötietonsa koneluettavassa muodossa. Lain 89 2 kohdan mukaan velvoite kuluttajadatan tarjoamisesta koskee pääsääntöisesti vain energia-, tele- ja finanssisektoria. Julkisen sektorin säännösten soveltamisala rajattiin ulkopuolelle.

Yhdistyneen kuningaskunnan Mydata-ohjelman myötä päädyttiin siten säätämään lain tasoisesti henkilötietojen luovutuksesta koneluettavassa muodossa. Sääntely kuitenkin koskee vain tiettyjä yritysmuotoisia toimijoita, eikä se sisällä julkishallinnon sektoria. Hallituksen vastauksessa liittyen lausuntokierrokseen rajattiin julkisen sektorin toimijat lainsäädännön piiristä pois perustelemalla valtion avoimen datan strategioilla, joissa valtio

---

<sup>126</sup> BIS 13.4.2011, s. 18-19.

<sup>127</sup> BIS 28.6.2012, s. 9-10.

<sup>128</sup> BIS 27.7.2012, s. 3-4 ja 11-14.

on sitoutunut antamaan kansalaisille pääsyn omiin julkisissa rekistereissä oleviin tietoihinsa. Lisäksi lausuntokierroksella julkisen sektorin soveltuvuus säädettävänä olevaan lainsäädäntöön herätti myös huolta julkisen sektorin toimijoissa.<sup>129</sup> Sääntelyä ei suoraan voida verrata kehitteillä olevaan suostumushallintapalveluun, joka on nimenomaisesti julkishallinto lähtöinen. Yhdistyneen kuningaskunnan malli vastaa hyvin pitkälti Ranskan yllä esitettyä mallia kuluttajille tarjottavasta tiedosta.

### 3.7 Omadatan haasteet

Omadatan periaate lähtee yksilön omien tietojen hallinnan –periaatteesta. Erillisen suostumusrekisterin rakentaminen on suuri haaste nykyisen lainsäädännön valossa, sillä tietosuojasta säätäminen on sirpaloitunut satojen erilaisin tavoittein säädettyjen säännösten epäyhtenäiseksi kokonaisuudeksi.<sup>130</sup> Henkilötietojen sääntely lakisääteisyysjohdosta tapahtuvasta käsittelystä on hajaantunut useaan eri yleis –ja erityislainsäädäntöön. Parhaimmillaan yhden viraston sisällä voi olla useita eri lakiperusteita henkilötietojen käsittelyyn, jotka liittyvät eri käsittelytarpeisiin.

Lainsäädännön pirstaleisuus sekä ei-semanttisesti säädetty lainsäädäntö aiheuttaa haasteita myös ontologian osalta. Lainsäädännössä samalle sisällölle tai tarkoitusperälle voi olla useita eri käsitteitä, jotka kuitenkin lopulta tarkoittavat samaa asiaa. Esimerkkinä tästä mainittakoon sana sijaintitieto. Sijaintitiedosta käytetään kolmessa eri laissa kolmea eri nimeä: paikkatieto (sähköisen viestinnän tietosuojalaki [516/2004]), paikantamistieto (meripelastuslaki [1145/2001]) ja sijaintitieto (rajavartiolaki [578/2005]).<sup>131</sup> Mikäli tulevaisuudessa halutaan yhteentoimiva alusta, jonka puitteissa julkishallinto pystyy tehokkaasti toimimaan, tulisi lainsäädäntö harmonisoida myös sanastotyön osalta. Tämä on kuitenkin pidemmän ajan prosessi, eikä nyt omadata-malli voi odottaa harmonisointityön tuloksia, vaan on toimittava sen puitteissa mitä tällä hetkellä laki mahdollistaa.

Oman haasteensa suostumushallintarekisterin toteuttamiseen ja sen kehittämiseen asettaa myös lainsäädännön puute. Nykyinen tiedonhallinnan kotimaan laajuinen ydinlainsäädäntö on peräisin 1990-luvulta, eikä lakimuutoksia tiedonhallintaa koskien ole sittemmin

---

<sup>129</sup> BIS 27.7.2012, s. 15-16.

<sup>130</sup> Saarenpää 2008, s.120.

<sup>131</sup> Kasvi 2008, s.92.

säädetty.<sup>132</sup> Kasvin mukaan ”Perinteinen lainsäädäntöprosessi on tietoyhteiskuntakehityksen tahdille aivan liian hidaskas. Teknologian kehitys ei pysähdy odottamaan, kun työryhmä laatii mietinnön, asianosaiset antavat lausunnot, ministeriö valmistelee esityksen ja eduskunta säätää lain. Uutta teknologiaa koskevat lait ovatkin usein jo syntyessään vuosia ajastaan jäljessä”.<sup>133</sup> Tätä tutkielmaa kirjoitettaessa uusi tiedonhallinnan lainsäädäntö on valmisteilla ja edennee hallituksen esityksestä eduskunnan käsittelyyn syksyllä 2018. Laki on suunniteltu hyväksyttäväksi siten, että se tulee voimaan alkuvuonna 2019. Tähän uuteen tiedonhallinnan lainsäädäntöön tuskin ehtii kattavasti lainsäädäntö koskien suostumusrekisteriä ja sen hallinnointia. Digitalisaatio Suomessa menee eteenpäin todella nopeaa, eikä lainsäädäntö ole aikaansa edellä, vaan hankkeissa on otettava huomioon sekä vanha tai jopa vanhentunut lainsäädäntö sekä mahdollisesti tuleva lainsäädäntö. Kuitenkin on huomattava, että digitalisaation johdosta toteutettavat uudet palvelut eivät välttämättä ole lain vaatimusten mukaisia edes jatkossakaan. Usein uudet toimintatavat vaativat lainsäädännöllistä selvitystä, eikä esimerkiksi perustuslain ylitse voida tuottaa uusia palveluja vain vetoamalla kehittyvään teknologiaan. Kaikki uudistukset vaativat perusteellista selvitystä etenkin silloin, kun kyseessä on henkilötietojen suoja koskevat asiat.

---

<sup>132</sup> Voutilainen – Huttunen 2015, s. 69. Tähän ydinlainsäädäntöön kuuluvat laki viranomaisten toiminnan julkisuudesta (621/1999), laki verotietojen julkisuudesta ja salassapidosta (1346/1999), arkistolaki (831/1994), laki potilaan asemasta ja oikeuksista (785/1992), laki sosiaalihuollon asiakkaan asemasta ja oikeuksista (812/2000). Tähän samaan ytimeen kuuluu myös henkilötietolaki siihen asti, kunnes se korvataan uudella tietosuojalalla.

<sup>133</sup> Kasvi 2008, s.86.



## 4 SUOSTUMUS KÄSITTELYPERUSTEENA

### 4.1. Viranomaisen tiedon hallinta ja sähköistynyt hallinto

Tarkasteltaessa suostumukseen perustuvaa käsittelyperustetta viranomaisten toimesta, on aluksi syytä selkeyttää viranomaisen tiedon hallinnan sekä henkilötietojen käsittelyn sääntelyn oikeusperusta. Suhteessa yksityiseen toimijaan, rekisterinpitäjänä viranomaisella on laista johdettuja velvoitteita sekä oikeuksia. Suostumusta, jonka yksilö on antanut rekisterinpitäjälle liittyen hänen henkilötietojen käsittelyyn, ei aina voida soveltaa yhdenmukaisesti viranomaisen ollessa rekisterinpitäjänä. Viranomaisen tietohallinnon järjestämistä ohjaa useat yleisnormit. Näitä ovat muun muassa viranomaisten toiminnan julkisuudesta annettu laki (621/1999), arkistolaki (831/1994), sähköisestä asioinnista viranomaistoiminnassa annettu laki (13/2003) sekä laki julkisen hallinnon tietohallinnon ohjauksesta (634/2011).<sup>134</sup>

Julkisen sektorin tietojen käyttöä taas ohjaavat perustuslaki (732/1999), erityislainsäädännöt sekä kansainväliset velvoitteet, kuten direktiivit ja kansainväliset sopimukset. Lukuisiin kansainvälisiin sopimuksiin sisältyy salassapitovelvoitteita tai sopimuksen nojalla luovutettavien tietojen käyttötarkoitussidonnaisuuden määrittelyä ennalta määriteltyihin tarkoituksiin. Esimerkkinä tällaisista sopimuksista voidaan mainita turvallisuusluokiteltuja tietoja sisältävät tietojen vaihdot eri maiden välillä.<sup>135</sup> Sekä perustuslaki että Suomea sitovat kansainväliset sopimukset ja säädökset rajoittavat lainsäätäjän mahdollisuutta säätää tietojen luovuttamisesta kaupallisiin tarkoituksiin viranomaisen rekisteristä.

Tietojen julkisuutta ja niiden luovuttamista viranomaisrekisteristä säätelee yleislakina laki viranomaisten toiminnan julkisuudesta (621/1999).<sup>136</sup> Julkisuuslain soveltamiseen liittyy julkisuusperiaate, jonka mukaan viranomaisten asiakirjat ovat julkisia, jollei laissa erikseen säädetä. Asiakirjajulkisuutta ei tulisi tulkita liian suppeasti, sillä julkisuusperiaate kohdistuu viranomaisella olevaan tietoon riippumatta sen tallennustavasta. Asiakirjajulkisuus on osa

---

<sup>134</sup> Voutilainen 2009, s. 11. Laki julkisen tiedonhallinnan ohjauksesta tullaan kumoamaan valmisteilla olevalla uudella tiedonhallinnan lainsäädännöllä.

<sup>135</sup> Valtiovarainministeriön julkaisu 2/2012, s. 29.

<sup>136</sup> Henkilötietojen käsittelyä säätelee tietosuojasetus sekä sitä tukeva lainsäädännöt. Julkisuuslaki sen sijaan säätelee tiedon luovuttamista viranomaisten rekisteristä. Julkisuuslakia ollaan myös osaltaan valmisteilla olevan tiedonhallinnan lainsäädännön yhteydessä muuttamassa, mutta tutkielman kirjoittamisen vaiheessa ei muutoksista ole vielä tietoa.

laajempaa, koko viranomaistoimintaa ohjaavaa periaatetta. Periaatteen mukaan jokaisella on oikeus saada tieto viranomaisten toiminnasta ja julkisesta vallankäytöstä sekä osallistua ja vaikuttaa viranomaisten käsiteltävänä oleviin asioihin.

Suomessa julkisuusperiaatteen juuret ulottuvat aina vuoteen 1766, jolloin Ruotsin valtiopäivillä hyväksyttiin painovapausasetus, joka edellytti yleistä tiedon saatavuutta asiakirjoista.<sup>137</sup> Vuonna 1951 säädettiin laki yleisten asiakirjain julkisuudesta (83/1951) ja vuonna 1995 säädettiin perusoikeusuudistuksen myötä asiakirjajulkisuus osaksi perustuslain perusoikeuksia. Vuonna 1999 tuli voimaan nykyinen julkisuuslaki, jota säädetään viranomaisten julkisuuskäytäntöihin.<sup>138</sup> Koska viranomaisilla on yleinen velvollisuus edistää perusoikeuksien toteuttamista, viranomaisilla on myös velvollisuus julkisuuden toteuttamiseen. Myös Salokannel näkee julkisen tiedon saatavuuden osana perusoikeutta. Hänen mukaansa ”perusoikeudellisesta näkökulmasta voidaan katsoa, että kansalaisten sananvapauden täysimääräinen toteuttaminen edellyttää, että heillä on mahdollisuus myös saada käyttöönsä julkisin varoin tuotettu tieto, jotta yhteiskunnan panos julkiseen tietoon tulisi myös kokonaistaloudelliselta kannalta yhteiskunnan hyödyksi”.<sup>139</sup>

Julkisella sektorilla on merkittävä rooli tiedon tuottajana ja ylläpitäjänä. Viranomaisten rekistereissä on valtavasti yhteiskunnallisesti merkittäviä tietovarantoja ja näillä tiedoilla on myös todellista taloudellista arvoa. Suurin osa näistä tietovarannoista on vain niiden käytössä, joilla on pääsy aineistoihin.<sup>140</sup> Julkinen sektori hallinnoi tuottamia henkilötietoja ja myös luovuttaa niitä edelleen lain määrittelemissä rajoissa, joten julkisen sektorin tietoja hyödynnetään laajasti myös yksityisellä sektorilla. Yksityisellä sektorilla julkisen sektorin tietoja käytetään yritysten asiakastietojen ylläpidossa, markkinoinnissa, profiloinnissa, suunnittelussa sekä muissa vastaavissa yritykselle lisäarvoa tuovissa toimissa.<sup>141</sup> Monet tietopalveluyritykset taas myyvät julkisen sektorin tietoja edelleen omien palvelujen osana tai jatkojalostettuna.<sup>142</sup> Alla olevassa taulukossa on yhteenveto julkisen sektorin

---

<sup>137</sup> Mäenpää 2008, s. 1-5.

<sup>138</sup> Jaatinen 2014, s. 23.

<sup>139</sup> Salokannel 2012, s. 2.

<sup>140</sup> Poikola – Kela – Hintikka 2010, s.11.

<sup>141</sup> Julkishallinnon tietojen luovutusten periaatteet ja käytännöt 2/2012, s. 29.

<sup>142</sup> Esimerkkinä julkisen sektorin tietojen uudelleen käytölle yksityisen sektorin toimesta on Datscha Oy, joka on yrityksille tarkoitettu tietopalvelu- ja analysointityökalu, jota käytetään kiinteistömarkkinoilla. Datscha ostaa tietoja muun muassa eri julkisen sektorin toimijoilta, yhdistää tiedot käytettävään ja luettavaan muotoon, joka taas mahdollistaa tietojen hyödyntämisen eri tavalla. Datschan asiakkaat voivat ostaa tietoa, jota ilman yhdistelyä olisi mahdotonta saada.

hallinnoimista tietotyypeistä, niiden sisällöstä sekä rekisterinpitäjistä. Taulukosta on nähtävissä viranomaisten ylläpitämien henkilötietojen laajuus.

	Sisältö	Rekistereitä
<b>Henkilötiedot</b>	Nimi, henkilötunnus, asuintiedot, yms.	Väestörekisteri (VRK)
<b>Terveystiedot</b>	Potilastiedot, mittaukset, sähköiset reseptit, suostumukset ja tahdonilmaisut	Lukuisia terveyspalvelujen rekistereitä ja yhteinen Kanta-järjestelmä
<b>Taloustiedot</b>	Tulot eri vuosilta, maksetut verot, saadut etuudet	Verotietokanta (Verohallinto), Etuusrekisteri (Kela), Eläketapahtumarekisteri (Eläketurvakeskus), Toimeentulotukirekisteri (THL)
<b>Kiinteistötiedot</b>	Tiedot sijainnista, omistajista, viranomaispäätöksistä, yms.	Kiinteistörekisteri (MML), Rakennus – ja huoneistorekisteri (VRK)
<b>Yritystiedot</b>	Yrityksen yhteystiedot, omistajuus, toimiala, yms.	Kaupparekisteri, säätiörekisteri ja yhdistysrekisteri (PRH)
<b>Liikenne- ja ajoneuvotiedot</b>	Ajoneuvojen omistajuus ja vakuutukset, sekä liikkumistiedot julkisen liikenteen palveluista	Ajoneuvoliikennerekisteri (Trafi), liikennepalvelujen asiakasrekisteri
<b>Oikeustiedot</b>	Rikokset, sakot	Rikosrekisteri, sakkorekisteri (Oikeusrekisterikeskus)
<b>Kulutus- ja asiakastiedot</b>	Esimerkiksi sähkön tai veden kulutus, erilaisten kulttuuripalvelujen käyttö	Kunnallisten palvelujen, liikelaitosten ja yhtiöiden asiakasrekisterit
<b>Koulutustiedot</b>	Tiedot tutkinnoista, opinto-oikeuksista, käydyistä kursseista sekä hakemuksista	Hakija- ja opinto-oikeusrekisterit (Opetushallitus), opiskelijatietojärjestelmät (oppilaitokset)

143

Viranomaisen toiminta sähköisissä palveluissa on sähköistä hallintoa, jolla tarkoitetaan informaatio- ja viestintäteknologian käyttöä julkisessa hallinnossa. Sähköisen hallinnon rakenneosiksi kutsutaan sähköisiä asiointipalveluita, asianhallintajärjestelmiä, viranomaisten operatiivisia järjestelmiä ja niiden taustajärjestelmiä sekä tietoverkkoa.<sup>144</sup> Sähköinen hallinto voidaan toisaalta myös ymmärtää laajana kokonaisuutena, johon kuuluu yksilöiden osallistumismahdollisuuksien parantaminen informaatio- ja viestintäteknologian keinoin<sup>145</sup> Euroopan komissio on määritellyt sähköisen hallinnon seuraavasti:

*Sähköisellä hallinnolla tarkoitetaan tässä tieto- ja viestintäteknologian käyttöä julkisessa hallinnossa yhdistettynä organisaatiomuutoksiin ja uusiin taitoihin siten, että voidaan parantaa julkisia palveluja ja demokraattisia prosesseja ja vahvistaa julkisen politiikan tukea.<sup>146</sup>*

<sup>143</sup> Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 61/2017, s. 14.

<sup>144</sup> Voutilainen 2009, s. 40.

<sup>145</sup> Voutilainen 2009, s. 41. Kansalaisen mahdollisuutta vaikuttaa sähköiseen hallintoon voidaan kutsua eDemokratiaksi.

<sup>146</sup> Komission tiedonanto neuvostolle, Euroopan parlamentille, Euroopan talouskomitealle sekä alueiden komitealle: sähköisen hallinnon merkitys huomisen Euroopassa, KOM (2003) 567, s. 8.

Sähköinen hallinto mahdollistaa aikaisempaa monipuolisemman yhteydenpidon, lisää ihmisläheisyyttä ja läpinäkyvyyttä sekä mahdollistaa hallintorakenteiden väljentämisen.<sup>147</sup> Julkisella sektorilla on merkittävä rooli tiedontuottajana, sillä se tuottaa tietotuotteita ja palveluiden raaka-aineita sekä rakentaa yleisiä toimintaedellytyksiä. Digiteknologia on mahdollistanut julkisen sektorin tuottaman tiedon laajamittaisen saatavuuden ja tiedon käyttömahdollisuudet ovat moninkertaistuneet. Suomessa julkisen sektorin tietovarannot ovat kattavat sekä korkeatasoiset ja niissä on paljon hyödyntämispotentiaalia.<sup>148</sup> Suomessa julkisen sektorin tuottaman tiedon saatavuutta rajoittavat laaja tietoaineistojen tekijänoikeussuoja sekä tietoaineistojen korkea hinnoittelu. Tämä taas aiheuttaa oikeudellista epävarmuutta ja epäselvyyttä käyttöoikeuksista.<sup>149</sup>

Kuronen ryhmittelee julkisin varoin ylläpidettyjen tietovarantojen käyttötarpeet kolmeen osaan: valtion tarpeet, markkinoiden tarpeet ja kansalaisten tarpeet.<sup>150</sup> Lähtökohtaisesti julkishallinnon tarpeet ovat aina olleet etusijalla ja niitä on kerätty julkishallinnon omaa käyttöä varten. Markkinoiden käyttötarpeet julkisin varoin ylläpidettyihin tietovarantoihin taas ovat julkiselle sektorille tärkeää liiketoimintaa ja julkinen sektori ylläpitääkin paljon tietovarantoja markkinoiden käyttöön.<sup>151</sup> Kansalaisten ja kansalaisyhteiskunnan omien, aitojen tarpeiden tunnistaminen on ollut haastavaa suhteessa valtion ja markkinoiden tarpeisiin. Kuitenkin oikeus tietoon on tietoyhteiskunnan jokaisen jäsenen oikeus ja sitä tulisi edelleen korostaa tarkasteltaessa tietovarantojen hyödyntäjiä sekä kansalaisten omia tarpeita.<sup>152</sup>

#### **4.2 Viranomaisen toimintaa ohjaavaan lainsäädännön ja suostumuksen suhde**

Viranomaisen rooli suostumukseen perustuvassa henkilötiedon käsittelyssä on hyvin erilainen kuin yksityisen sektorin toimijan. Pääsääntöisesti yksilö rekisteröitynä hallinnon

<sup>147</sup> Kulla 2011, s. 328.

<sup>148</sup> Koski-Kiuru-Mäkelä-Salokannel 2012, s.3.

<sup>149</sup> Salokannel 2012, s. 2.

<sup>150</sup> Kuronen 1998, s. 30. Kuronen kuitenkin edelleen huomauttaa, että kyseinen kolmeen ryhmään jakaminen on hyvin karkea, ja sitä voidaan tarvittaessa tihentää.

<sup>151</sup> Valtiovarainministeriön 11.2.2010 asettaman Julkishallinnon tietovarantojen saatavuuden ja käytön edistäminen -työryhmän raportissa ilmeni, että julkinen sektori luovuttaa maksua vastaan tietoja myös muille julkisyhteisöille. Vuonna 2009 julkisyhteisöille tehdyistä tietoluovutuksista kertyi vuonna 2009 yhteensä noin 11 miljoonan euron tulot. Raportin jälkeen viranomaisten välisistä tietojenluovutusmaksuista on pääosin luovuttu. Kuitenkin omakustannusarvo peritään yleensä valtion maksuperustelain (Valtiovarainministeriön asetus 1396/2016) perusteella myös julkiselta sektorilta. Ks. lisää viranomaisten välisistä tietojenluovutuksista Tiedonhallinnan lainsäädännön kehittämislinjaukset -työryhmän raportista, alkaen sivulta 155.

<sup>152</sup> Kuronen 1998, s. 30-32.

asiakkaana on heikommassa asemassa suhteessa viranomaiseen, sillä viranomaisen toiminta perustuu lähtökohtaisesti lakiin, eikä rekisteröidyn suostumusta tarvitse erikseen pyytää.<sup>153</sup> Mikäli viranomaisella ei ole lakiin perustuvaa oikeutta käsitellä asiakkaan henkilötietoja, on viranomaisen pyydettävä suostumus rekisteröidyltä itseltään.<sup>154</sup> Hallintosopimusten ulkopuolelle jäävät suhteellisen usein tilanteet, joissa hallinnollisen toimenpiteen kohteena suostumus on päätöksen tekemisen tai toimen suorittamisen välttämätön edellytys.<sup>155</sup> Tyypiesimerkkinä kaksipuolisista hallintotoimista voidaan pitää virkanimitystä, joka edellyttää hallintotoimen täyttämiseen suostumusta virkamiehen osalta.<sup>156</sup> Henkilötietojen käsittelyn osalta julkisuuslaki mahdollistaa tietyiltä osin henkilötietojen luovuttamisen tai käsittelyn rekisteröidyn suostumuksen nojalla. Suostumusta edellyttävien hallintopäätösten tekemiseen voi liittyä samanlaisia piirteitä kuin sopimuksiin,<sup>157</sup> vaikka suostumuksen antaja ei voisi asettaa ehtoja suostumuksen edellytykseksi.<sup>158</sup>

Tietosuoja-asetus lähtee samasta periaatteesta, eli viranomaisen ja rekisteröidyn suhteen välillä on selkeä epäsuhta. Suostumuksen ei voida katsoa olevan vapaaehtoisesti annettu, mikäli rekisterinpitäjänä on viranomainen ja sen vuoksi epätodennäköistä, että suostumus olisi annettu rekisteröidyn omasta vapaasta tahdosta.<sup>159</sup> Tilke-raportissa on katsottu, että viranomaisten välillä tieto tulisi liikkua sujuvasti siten, että tietoa kysytään tiedonkeruun kohteelta vain kerran ja sen jälkeen olisi niiden käytössä, jotka tarvitsevat sitä lakisääteisen tehtävän hoitamiseen. Edelleen raportissa korostetaan sitä, että ” lakisääteisen tehtävän hoitamista varten toiselta viranomaiselta tarvittavat muut kuin salassa pidettävät henkilötiedot on saatava tehtävän hoitamisen kannalta tarvittavilta osin yleislakiin perustuen ilman erityislainsäädännössä olevia tiedonsaanti- tai tiedon luovutus-oikeutta koskevia säännöksiä”.<sup>160</sup> Tuleva tiedonhallinnan lainsäädäntö tulee säätämään julkishallinnon yhtenäisempää tiedonhallintaa. Lain avulla tietoaineistojen muodostamisessa sekä niiden käsittelyssä vahvistettaisiin kokonaisprosessiajattelua viranomaisten välillä. Tällöin

---

<sup>153</sup> Voutilainen 2009, s. 131.

<sup>154</sup> Voutilainen 2009, s. 132.

<sup>155</sup> Mäenpää 1989a, s. 98.

<sup>156</sup> Valtion virkamieslaki (1994/750) säätää suostumuksen edellytyksestä virkaan liittyvien toimien täyttämiseksi. Esimerkkinä lain 6 d §:n mukaan virkaan voidaan nimittää henkilö, joka on antanut nimittämiseen suostumuksensa. Myös 2016 vuonna lakimuutoksen myötä muutettu lain 20 § säätelee virkamiehen siirtoa osin tai kokonaan toiseen virastoon työskentelemään. Siirron edellytyksenä on sekä vastaanottavan viraston että virkamiehen suostumus.

<sup>157</sup> Vilkkonen 1970, s. 57 huomauttaa, miten suostumuksen ja sopimuksen välillä on käytännössä vain hieno ero.

<sup>158</sup> Mäenpää 1989, s.99.

<sup>159</sup> Tietosuoja-asetus, 43 johtolause.

<sup>160</sup> Valtiovarainministeriön julkaisu – 37/2017, s. 23.

tiedonhallinnan vastuu muuttuisi aikaisemmasta siten, että siirryttäessä julkishallinnon prosessissa vaiheesta toiseen, olisi samassa prosessissa jo aiemmin kerätyt tiedot hyödynnettävissä rajapintojen avulla.<sup>161</sup> Lähtökohtana olisi, että viranomaisen saa lakisääteiseen tehtäväänsä perustuen tiedot toiselta viranomaiselta rajapinnan kautta ilman erillistä tietolupapäätöstä. Tällöin lainsäädännössä säädettäisiin lähtökohtaisesti pakolliseksi avoimet rajapinnat sekä niiden määrittely. Rajapintojen avulla tiedon luovutus olisi mahdollista myös muille toimijoille silloin, kun luovutuksen saajalla olisi henkilötietojen suojaa koskevien säännösten mukaan oikeus käsitellä kyseisiä tietoja.<sup>162</sup> Lähtökohtaisesti valmisteilla oleva lainsäädäntö luo viranomaiselle yhä vahvemman oikeuden käsitellä lakisääteisen tehtävän hoitamisen perusteella yksilöiden henkilötietoja. Tiedon saatavuutta parannetaan ja yksittäisten rekisterinpitäjien oikeutta määrätä tiedon käytöstä heikennetään. Lakisääteisen oikeuden nojalla ei yksilön suostumusta tarvita, joten henkilötiedon suostumusperustainen käsittely viranomaisten toimesta on vähäistä.

Yleisen tietosuojasetuksen 20 artiklan mukaisesti rekisteröidyllä on oikeus saada häntä koskevat henkilötiedot, jotka hän itse on toimittanut rekisterinpitäjälle, koneluettavassa muodossa sekä oikeus siirtää kyseiset tiedot toiselle rekisterinpitäjälle. Julkisella sektorilla viranomaisten tietovarannot muodostuvat tarvelähtöisesti ja viranomaisen saa tarvitsemansa henkilötiedot yleensä kolmansilta, tai ne syntyvät viranomaisprosessin seurauksena. Viranomaisen kerää tietoja esimerkiksi hallinnollisen prosessin seurauksena päätöksentekoa varten, erilaisista hakemuksista tai ilmoituksista, perusrekistereistä, tietopalvelurekistereistä tai kehittämis- ja tutkimustoiminnan kautta kerätystä tiedosta.<sup>163</sup> Viranomaisen oikeus taas hyödyntää eri rekistereissä olevia henkilötietoja säädetään yleisimmin lailla. Lainsäädännön nojalla viranomaisella on ensisijainen velvoite kerätä tieto toiselta viranomaiselta, ei kansalaiselta itseltään.<sup>164</sup> Julkishallinnon henkilötietojen käsittelyn malli ei siten suoraan sovellu omadata-malliin, jossa yksilö itse suostumusperusteisesti oikeuttaa henkilötietojensa käsittelyä eri rekisterinpitäjien osalta. Viranomaiset käsittelevät henkilötietoja muutamia

---

<sup>161</sup> Valtiovarainministeriön julkaisu – 37/2017, s. 14.

<sup>162</sup> Ks. Valtiovarainministeriön julkaisu – 37/2017, sivut 14-15 sekä s. 26. Raportissa on selvennetty nykyistä tiedonhallintaa viranomaisten välillä, joka perustuu tietolupapohjaiseen tiedon luovutukseen. Nykykäytännön mukaan tietoja luovutetaan vain erillisillä tietolupapäätöksillä, ja silloinkin luvan saannin edellytyksenä on voimassa olevan lainsäädännön noudattaminen. Työryhmän mukaan viranomaisen tulisi luottaa toiseen viranomaiseen siten, että erillistä tietolupapäätöstä luovutuksen osalta ei tulisi tehdä. Tällöin riittäisi laista johdettava oikeus tietojen käsittelyyn ja tiedon luovutus avoimen rajapinnan kautta.

<sup>163</sup> Ks. lisää viranomaistiedon ryhmittelystä Korhonen 2003, s. 233.

<sup>164</sup> Valtiovarainministeriön julkaisu – 37/2017, s. 23.

poikkeuksia lukuun ottamatta lakiperusteisesti, eikä sitä voida omadatamallin mukaisesti muuttaa.

Eräs viranomaiskäsittelyn poikkeuksista on julkisuuslaissa säädelty salassa pidettävien viranomaisten asiakirjojen tiedonsaantioikeus. Julkisuusperiaatteen mukaan viranomaisten asiakirjat ovat julkisia, jollei toisin laissa säädetä. Lain 26 §:ssä säädetään yleisistä perusteista salassa pidettävän tiedon antamiseen. Pykälän 1-kohdan mukaan viranomaisen voi antaa salassa pidettävästä viranomaisen asiakirjasta tiedon, jos ”se, jonka etujen suojaamiseksi salassapitovelvollisuus on säädetty, antaa siihen suostumuksensa”. Yksityisten etujen suojaamiseksi salassapito on säädetty esimerkiksi silloin, kun kyse on terveydentilasta annettavista todistuksista, verotusasiakirjoista tai liikesalaisuuksista. Henkilö voi antaa suostumuksen vain silloin, kun hän voisi myös itse saada tiedon asiakirjasta.<sup>165</sup> Tällainen suostumus voi perustua myös sopimukseen viranomaisen ja yksityisen asianosaisen välillä.<sup>166</sup> Kyseinen säännös on ristiriidassa tietosuoja-asetuksen johtolauseen 43 sekä Tilke-raportin kanssa, joiden mukaan viranomaisen käsittelyperuste ei voisi perustua suostumukseen.

Tietosuoja-asetuksen johtolauseessa 43 mainitaan, että olisi epätodennäköistä suostumuksen olevan annettu vapaaehtoisesti ”*kaikissa* kyseiseen tilanteeseen liittyvissä olosuhteissa”. Sananmuoto jättää tilaa harkinnalle sen osalta, voisiko olla sellaisia tilanteita viranomaisen ja yksityisen välillä, jolloin myös suostumus voidaan katsoa olevan annettu vapaaehtoisesti. Käytännössä on haastavaa ilman voimassa olevaa lainsäädäntöä tulkita tilanteita, milloin viranomaisen voisi katsoa yksilön antavan suostumuksen vapaaehtoisesti. Julkisuuslain tietojen luovutuksen periaatteet tulevat sovellettavaksi, ellei ole sovellettavaa erityislainsäädäntöä taustalla. Tästä johtuen pääsääntö viranomaisen tietojen käsittelylle tulisi olla lainsäädäntö, jonka pohjalta yksilö voisi antaa suostumuksensa viranomaiselle omadataksi luokitellun henkilötietonsa käsittelyyn. Valmisteilla olevaan tiedonhallintalakiin on tarkoitus koota sääntelyä muun muassa julkisuuslaista, ja siinä yhteydessä on mahdollista tarkastella julkisuuslain 26 §:n suostumusperusteisen käsittelyn edellytyksiä tietosuoja-asetuksen valossa sekä sitä, tulisiko omadataksi luokitellusta tiedosta säätää erikseen myös tilanteista, milloin suostumus voidaan antaa myös julkisen hallinnon toimijalle.<sup>167</sup>

---

<sup>165</sup> Kulla 2015, s. 457.

<sup>166</sup> Mäenpää 2008b, s. 341-342.

<sup>167</sup> Tietosuojalainsäädäntö on muuttumassa, ja tutkielman kirjoitushetkellä ei ole selvää lopullisista lainsäädännön suuntaviivoista. Hallituksen esitykseen uudesta tietosuoja-laista (9/2018) on koottu tietosuoja-asetusta täydentävää sääntelyä.

Edellä kappaleessa 2.2.2 on mainittu julkisuuslain mukaisesta asianosaisen tiedonsaantioikeudesta. Julkisuuslain mukaisesti jokaisella on oikeus saada tieto hänestä itsestään viranomaisen asiakirjaan sisältyvistä tiedoista 11 §:n 2 ja 3 momentissa säädettyin rajoituksin. Tämä oikeus itsessään velvoittaa viranomaista antamaan tiedon kohteelle häntä koskevat tiedot. Rajoituksena kuitenkin sellaiset laissa säädetty tiedot, jotka ovat myös yksilöltä itseltään salassa pidettäviä. Vaikka julkisuuslakiin jo nykyään sisältyy omien tietojen hallintaa, ei se kuitenkaan mahdollista omadatan mukaista henkilötietojen hallintaa, jossa viranomaisen luovuttaisi tiedot suoraan toiselle rekisterinpitäjälle. Tällöin tietoja ei luovutettaisi JulkL:n 12 §:n mukaisesti rekisteröidylle itselleen, vaan hänen osoittamalleen taholle. Kyseistä pykälää ei tämän vuoksi voida soveltaa suoraan omadata-malliin, sillä lain sananmuoto ei vastaa tiedon luovutuksen tarvetta.

Viime aikoina säädettyihin lainsäädäntöihin on kuitenkin jo sisällytetty viranomaisen henkilötiedon käsittelyä suostumukseen perustuen. Esimerkkinä mainittakoon luvussa 3 käsitelty KOSKI-laki. Lain 29.5 §:n mukaan suostumuksen antava henkilö voi antaa yksilöidyn suostumuksensa rekisterissä tai tietovarannossa olevan tiedon luovuttamiseen viranomaiselle tai muulle taholle. Lain hallituksen esityksessä 72/2017 kyseisen pykälän yksityiskohtaisissa perusteluissa edelleen mainitaan, että *henkilön suostumukseen perustuvia luovutuksia ei rajattaisi koskemaan vain viranomaisia*. Kyseinen pykälä ei siis vastaa tietosuoja-asetuksen lähtökohtaa siitä, että viranomaisen käsittely ei lähtökohtaisesti perustu suostumukseen. KOSKI-laissa suostumus annetaan lähtökohtaisesti viranomaiselle, mutta luovutuksia ei ole rajattu koskemaan pelkästään viranomaisia, vaan myös yksityiset voivat olla suostumuksen kohteena. Mikäli omien tietojen hallinnasta säädetään myös jatkossa erityislainsäädännössä, vaarana on omien tietojen hallinnan yhä epäyhtenäisempi ja sekava sääntely.

### **4.3 Suostumukseen liittyvä tarpeellisuusvaatimus**

Tilke-raportissa on huomioitu suostumusperusteinen käsittely viranomaistoiminnassa siten, että jatkossa hallinnon asiakkaiden tietoja tulisi työryhmän mukaan luovuttaa kolmannelle osapuolelle myös suostumuksen perusteella, mikäli luovutuksen kohteena olevan henkilötiedon käsittelylle ei ole olemassa muuta laillista perustetta. Tämä linjaus puoltaa vahvasti kansalaisen omien tietojen hallintaa. Raportissa kuitenkin huomautetaan, että viranomaisissa tapahtuvan henkilötietojen käsittelyn oikeusperusta ei voi perustua



suostumukseen.<sup>168</sup> Tietojen luovuttaminen viranomaisen tietovarannoista muuhun kuin viranomaistoiminnan käyttötarkoitukseen edellyttää sitä, että suostumuksen antajan vapaaehtoisuus ja muut suostumuksen edellytykset täyttyvät.<sup>169</sup>

Viranomaisen velvoite luovuttaa henkilötietoja silloin, mikäli sovellettavana ei ole muuta laillista perustetta mahdollistaisi yksilölle enemmän tosiasiallista hallintaa henkilötietojensa käsittelyyn. Huomattava kuitenkin on se, että rekisterinpitäjä ei voi suostumuksenkaan perusteella käsitellä henkilötietoja sellaisiin käyttötarkoituksiin, joille ei todellisuudessa ole tarvetta. Nykyisessä henkilötietolaissa, säädetään 9 §: ssä henkilötietojen käsittelyn tarpeellisuusvaatimuksesta. Tarpeellisuusvaatimuksen mukaan käsiteltävien henkilötietojen tulee olla määritellyn henkilötietojen käsittelyn tarkoituksen kannalta tarpeellisia. Henkilötietolain 9 §: n 1 momentin perusteella rekisteröidyn suostumuksellakaan ei voida kerätä tarpeettomia henkilötietoja, vaan käsiteltävien henkilötietojen on oltava asianmukaisia ja olennaisia eivätkä saa olla liian laajoja käyttötarkoitukseen näden.<sup>170</sup> Eduskunnan oikeusasiamies on ratkaisussaan katsonut oppilaitoksen suostumukseen perustuvan terveydentilaa koskevan käsittelyn rikkovan henkilötietolain 9 §: ää:

Kantelija oli kirjoituksessaan pyytänyt oikeusasiamiestä tutkimaan, menettelikö oppilaitos lain mukaan velvoittaessaan hakijoita antamaan terveydentilaansa koskevia tietoja ennen kuin tulevat valituksi. Oppilaitos oli vaatinut hakijoita täyttämään hakemuksen yhteydessä lomakkeen, jossa tiedusteltiin terveydentilaa ja sairaushistoriaa. Kyseisiä tietoja käsiteltiin hakijan antaman suostumuksen perusteella. Lain mukaan opiskelijavalintarekisteriin voidaan tallettaa hakijan ilmoituksen mukaisina ammatinvalintaan vaikuttavat terveystiedot. Oikeusasiamies totesi lausunnossaan että, vaikka tietojen antaminen on ollut hakijoille vapaaehtoista ja siten suostumukseen perustuvaa, tietojen kerääminen ei täyttänyt lainsäädännössä asetettujen henkilötietojen tarpeellisuusvaatimuksia eikä näin ollen perustunut siltä osin lakiin.<sup>171</sup>

---

<sup>168</sup> Apulaisoikeuskansleri (AOK) on ottanut kantaa suostumuksen vapaaehtoisuuteen tilanteessa, jossa rekisteröity on alistussuhteessa rekisterinpitäjään nähden. Apulaisoikeuskansleri on todennut, mikäli suostumuksen antamisen kieltäytymisen johdosta olisi seurauksena määräaikaisen työttömyysturvan menettäminen, ei tosiasiallisia edellytyksiä suostumukselle ole olemassa (AOK 947/1/02). Myös Eduskunnan Apulaisoikeusasiamies (AOA) on ottanut kantaa työntekijän ja työnantajan väliseen epätasa-arvoiseen tilanteeseen. Työntekijän suostumusta hankittaessa on kiinnitettävä huomiota tosiasiallisen vapaaehtoisuuden täyttämisen mahdollisuuteen (AOA 2901/2/04).

<sup>169</sup> Valtiovarainministeriön julkaisu – 37/2017, s. 24-25.

<sup>170</sup> Voutilainen 2012, s. 305.

<sup>171</sup> EOAK 1488/1999.

Rekisteröidyn antama suostumus henkilötietojen käsittelyyn ei siten ole muodostanut rekisterinpitäjälle täydellistä vapautta käsitellä henkilötietoja. Rekisterinpitäjän on edellytetty täyttävän henkilötietojen käsittelyn lailliset perusteet, eikä suostumukseen perustuen ole voitu kerätä henkilötietoja ilman tarpeellisuusvaatimuksen täyttymistä.<sup>172</sup> Lainsäädännössä on myös nähty tarpeelliseksi joissain tilanteissa todeta erikseen, ettei suostumuksella voida poiketa lain säädöksistä.<sup>173</sup>

Rekisterinpitäjä ei myöskään voi käsitellä henkilötietoja suostumuksen perusteella perustaen käsittelyä sopimusoikeudellisiin perusteisiin.<sup>174</sup> Sopimuksen teon yhteydessä suostumuksella kerättävät henkilötiedot tulee olla tarpeen kyseisen sopimuksen osalta. Yleisen tietosuoja-asetuksen 7 artiklan 4-kohta säätelee suostumuksen vapaaehtoisuutta:

”Arvioitaessa suostumuksen vapaaehtoisuutta on otettava mahdollisimman kattavasti huomioon muun muassa se, onko palvelun tarjoamisen tai muun sopimuksen täytäntöönpanon ehdoksi asetettu suostumus sellaisten henkilötietojen käsittelyyn, jotka eivät ole tarpeen kyseisen sopimuksen täytäntöönpanoa varten.”

Euroopan unionin Tietosuojatyöryhmä<sup>175</sup> on antanut uuden suostumukseen perustuvan lausunnon perustuen tietosuoja-asetukseen. Tietosuojatyöryhmän mukaan ei ole asetuksen suostumusperusteisen käsittelyn mukaista niputtaa suostumus rekisteröidyn hyväksyessä ehtoja sellaisen henkilötietojen käsittelemistä koskevaan pyyntöön, joka ei ole välttämätöntä kyseisen sopimuksen tai palvelun suorittamiseksi. Mikäli tällaisessa tilanteessa annetaan suostumus henkilötietojen käsittelyyn, suostumuksen ei katsota olevan vapaaehtoisesti annettu. Tällaisella sääntelyllä tietosuoja-asetus varmistaa, että sopimuksen osalta suostumukseen perustuva henkilötietojen käsittely ei voi suoraan tai epäsuoraan johtaa sopimuksen vastaisiin toimiin. Tietojen käsittelyn ja sopimuksen toteuttamisen tarkoituksen välillä on oltava suora ja objektiivinen yhteys.<sup>176</sup>

---

<sup>172</sup> Voutilainen 2012, s. 245.

<sup>173</sup> Esimerkiksi lain yksityisyyden suojasta työelämässä (759/2004) 3 §:n mukaan työnantaja saa käsitellä vain välittömästi työntekijän työsuhteen kannalta tarpeellisia henkilötietoja, jotka liittyvät muun muassa työsuhteen osapuolten oikeuksien ja velvollisuuksien hoitamiseen. Edelleen säädetään, ettei työnantaja voi poiketa tarpeellisuusvaatimuksesta työntekijän suostumuksella.

<sup>174</sup> Data Protection Working Party: WP 187, Opinion 15/2011 on Consent, 13.7.2011, s. 9.

<sup>175</sup> Tietosuojatyöryhmä eli WP29 on tietosuojadirektiivin 29 artiklassa asetettu tietosuojatyöryhmä, joka on riippumaton, neuvoa-antava elin tietosuoja koskeissa asioissa. WP29 koostuu jäsenvaltioiden tietosuojaviranomaisista, Euroopan tietosuojavaltuutetusta sekä komission edustajista. WP29 on antanut useita soveltamisohjeita tietosuoja-asetukseen liittyen.

<sup>176</sup> Article 29 data protection working party: WP259, Guidelines on Consent under Regulation 2016/679, s.9.

Yleisin omadata-ajattelua kohtaan esitetty kritiikki on se, että mahdollistettaessa yksilölle oikeus hallita suostumuksella omia henkilötietojaan, kiihdyttäisi se suuntausta, jossa ihmisiltä vaaditaan entistä enemmän henkilötietoa. Esimerkiksi tulevaisuuden skenaarioista on pohdittu, voisiko jatkossa kohtuuhintaista vakuutusta ottaessa annettava ensin kattava ja rikas profiilidata vakuutusyhtiölle.<sup>177</sup> Tällöin omadata-malli voisi kääntyä yksilöä itseään vastaan sen osalta, olisiko tällaisissa tilanteissa tosiasiallinen mahdollisuus vaikuttaa luovuttamaansa henkilötietoon. Tietosuoja-asetuksen 7 artiklan 4-kohdan tarpeellisuusvaatimus näyttäisi kumoavan esitetyn kritiikin rekisterinpitäjän loputtamasta henkilötietojen keräämisestä suostumukseen perustuvan henkilötiedon osalta. Koska tietosuoja-asetuksessa ei katsota suostumuksen olevan vapaaehtoisesti annettu silloin, kun kerätyt henkilötiedot eivät ole tarpeen kyseisen sopimuksen täytäntöönpanemiseksi, ei esimerkiksi vakuutuksenantaja voisi kerätä tarpeettomia henkilötietoja tarjotakseen kohtuuhintaista vakuutusta. Toisaalta taas on perusteltua tarkastella sitä, voidaanko lailla säätää esimerkiksi vakuutuksenantajan keräämien tietojen tarpeellisuudesta suhteessa vapaaehtoisen vakuutuksen antamiseen. Vakuutuksenantaja voi kieltäytyä vapaaehtoisen vakuutuksen myöntämisestä, mutta hylkäysperusteen on oltava lain ja hyvän vakuutustavan mukainen.<sup>178</sup> Tästäkään näkökulmasta tarkasteltuna vakuutuksenantaja ei vapaaehtoista vakuutusta myöntäessään voi kerätä henkilötietoja ilman tarpeellisuusvaatimuksen täyttymistä. Hylkäysperusteen tulee olla lain mukainen, eikä vakuutuksenantajan päätökset voi perustua mielivaltaisuuteen.

---

<sup>177</sup> LVM 2/2014, s. 65.

<sup>178</sup> Finanssivalvonnan www-sivut.

## 5 REKISTERINPITÄJÄN VASTUU

### 5.1 Yleisesti rekisterinpitäjän velvollisuudesta ja vastuusta

Yksityisyyden suoja pohjautuu vanhaan periaatteeseen siitä, että on olemassa julkisen toiminnan piiri sekä oikeusvaltiossa turvattu ja suojattu yksityiselämä. Suomen ensimmäisen tietosuojaan yleislain henkilökisterilain (471/87) eräänä nimenomaisena sääntelytavoitteena oli henkilötietojen suojaamisen ohella kyse myös valtion turvallisuudesta. Yksityisyyden suoja ja muut lainsäädännön tasolla taatut oikeudet on tarkoitettu rajoittamaan julkisen vallan käyttöä yksilön oikeuksien hyväksi. Tämän johdosta perusoikeudet sekä tietosuojalainsäädäntö luovat puitteita julkisen vallan käyttäjien toiminnalle.<sup>179</sup> Viranomaisen on pääsääntöisesti sellaisten julkisen sektorin tietovarantojen rekisterinpitäjä, joka sisältävät henkilötietoja.<sup>180</sup>

Rekisterinpitäjälle on asetettu velvollisuuksia liittyen henkilötietojen käsittelyyn<sup>181</sup>. Henkilötietolaista on johdettavissa perusteet henkilötietojen käsittelylle. Tietosuoja-asetuksen asettamisen myötä yleiset henkilötietojen käsittelyyn liittyvät periaatteet säilyivät pääosin sellaisenaan, mutta rekisterinpitäjälle asetettuja velvollisuuksia myös lisättiin aikaisempaan nähden. Henkilötietolaista on siten edelleen johdettavissa yleiset henkilötietojen käsittelyn perusteet ja siihen lisäksi sovelletaan tietosuoja-asetuksen uusia rekisteröidyn oikeuksia sekä rekisterinpitäjää koskevia velvoitteita. Koska henkilötietolaki tullaan korvaamaan uudella tietosuojalailla, tässä tutkielmassa keskitytään rekisterinpitäjän vastuuseen siltä osin, miten rekisterinpitäjän vastuu on määräytynyt nykyisen henkilötietolainsäädännön ja erityislainsäädännön osalta sekä siihen, miten vastuu jaetaan mahdollisessa suostumushallintapalvelussa ottaen huomioon tietosuoja-asetuksen myötä rekisteröidylle tulleita oikeuksia henkilötietojen hallintaan.

---

<sup>179</sup> Kuopus 2002, s. 234.

<sup>180</sup> EU:n tietosuoja-asetuksen 4 artiklan 7-kohdassa on määritetty rekisterinpitäjä: ”luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot; jos tällaisten käsittelyn tarkoitukset ja keinot määritellään unionin tai jäsenvaltioiden lainsäädännössä, rekisterinpitäjä tai tämän nimittämistä koskevat erityiset kriteerit voidaan vahvistaa unionin oikeuden tai jäsenvaltion lainsäädännön mukaisesti”.

<sup>181</sup> EU:n tietosuoja-asetuksen 4 artiklan 8-kohdassa on määritetty henkilötietojen käsittelijä: ”luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka käsittelee henkilötietoja rekisterinpitäjän lukuun”.

Henkilötietolain lainmukaisuusvelvollisuus voidaan katsoa olevan tietosuojaan perussäännös.<sup>182</sup> Lainmukaisuusvelvollisuuden myötä rekisterinpitäjän on huolehdittava siitä, että henkilötietoja käsitellään laillisesti. Sama vaatimus on yleisen tietosuoja-asetuksen 5 artiklassa, jossa määritellään rekisterinpitäjän velvollisuutta noudattaa henkilötietojen käsittelyssä lainmukaisuutta, kohtuullisuutta sekä läpinäkyvyyttä. Lainmukaisuusvaatimus täyttyy silloin, kun henkilötietojen käsittely perustuu *asianomaisen rekisteröidyn suostumukseen tai muuhun oikeutettuun perusteeseen, josta säädetään lainsäädännössä, joko tässä asetuksessa tai tässä asetuksessa tarkoitettussa muussa unionin oikeudessa tai jäsenvaltion lainsäädännössä, mukaan lukien tarve noudattaa rekisterinpitäjää koskevaa lakisääteistä velvoitetta tai tarve panna täytäntöön sopimus, jossa rekisteröity on osapuolena, tai sopimusta edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä.*<sup>183</sup>

Henkilötietolain huolellisuusvelvoitteen mukaan rekisterinpitäjän tulee henkilötietoja käsitellessään noudattaa huolellisuutta ja hyvää tietojenkäsittelytapaa. Rekisterinpitäjän on toimittava siten, ettei rekisteröidyn yksityiselämän suojaa ja muita yksityisyyden suojaan turvaavia perusoikeuksia rajoiteta ilman laissa säädettyä perustetta. Huolellisuusvelvoite ohjaa rekisterinpitäjää oma-aloitteisesti huolehtimaan siitä, että henkilötietojen käsittely toteutetaan ottaen huomioon yksityisyyden suojaa turvaavat säännökset ja periaatteet.<sup>184</sup> Huolellisuusvelvollisuus konkretisoituu käytännössä yleisinä tietosuoja-säännöksinä mukaan luettuna henkilötietolain säännökset sekä hallinnonalakohtaisina erityissäännöksinä.<sup>185</sup> Huolellisuusvelvoitetta ei yleisessä tietosuoja-asetuksessa ole nimenomaisesti määritelty, mutta sen voidaan katsoa olevan osa tietosuoja-asetuksen vaatimuksia rekisterinpitäjän suhteen siten, että rekisterinpitäjän on oma-aloitteisesti huomioitava henkilötietojen käsittelyssä laissa säädettyt perusteet.

Muita yleisen tietosuoja-asetuksen mukaisia henkilötietojen käsittelyä koskevia periaatteita ovat käyttötarkoitussidonnaisuus, tietojen minimointi, täsmällisyys, säilytyksen rajoittaminen sekä eheys ja luottamuksellisuus. Käyttötarkoitussidonnaisuuden mukaisesti henkilötietoja on kerättävä tiettyä, nimenomaista ja laillista tarkoitusta varten, eikä niitä saa

---

<sup>182</sup> Voutilainen 2007, s. 131.

<sup>183</sup> Tietosuoja-asetus, 40 johtolause.

<sup>184</sup> HE (96/1998) vp, s. 37.

<sup>185</sup> Voutilainen 2007, s. 132. Esimerkkinä tällaisesta säädöksestä on laki yksityisyyden suojasta työelämässä. Lain 2 luvun 3 § säätelee työnantajan oikeutta käsitellä työntekijän henkilötietoja siten, että käsiteltävät henkilötiedot liittyvät työsuhteen osapuolten oikeuksien ja velvollisuuksien hoitamiseen tai työnantajan työntekijöille tarjoamiin etuuksiin taikka johtuvat työtehtävien erityisluonteesta ("tarpeellisuusvaatimus").

käsitellä myöhemmin näiden tarkoitusten kanssa yhteensopimattomalla tavalla. Tietojen minimointi taas tarkoittaa sitä, että henkilötietojen käsittelyn on oltava asianmukaisia ja olennaisia sekä rajoitettuja siihen, mikä on tarpeellista suhteessa niihin tarkoituksiin, joita varten niitä käsitellään. Täsmällisyyden vaatimus edellyttää rekisterinpitäjän toteuttavan toimenpiteet sen varmistamiseksi, että epätarkat ja virheelliset henkilötiedot poistetaan ja oikaistaan viipymättä. Säilytyksen rajoittaminen sekä henkilötietojen eheys ja luottamuksellisuus taas edellyttävät rekisterinpitäjää säilyttämään tunnistettavat henkilötiedot ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten. Henkilötietolain 32 §:n mukaan rekisterinpitäjällä on velvollisuus toteuttaa tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi. Tietosuoja-asetuksen 5 artiklan 1 kohdan f alakohta säätelee vastaavasti henkilötietojen käsittelyä koskevia vaatimuksia suojaamisen osalta:

*”niitä on käsiteltävä tavalla, jolla varmistetaan henkilötietojen asianmukainen turvallisuus, mukaan lukien suojaaminen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta käyttäen asianmukaisia teknisiä tai organisatorisia toimia (”eheys ja luottamuksellisuus”).”*

Edelleen 5 artiklan 2 kohdan osoitusvelvollisuuden mukaan rekisterinpitäjä vastaa siitä, että 1 kohdan vaatimuksia on noudatettu ja rekisterinpitäjän on pystyttävä osoittamaan se.<sup>186</sup>

## 5.2 Henkilötietojen luovuttaminen viranomaisen rekisteristä

Julkisuuslain 5.1 §:n mukaan *asiakirjalla* tarkoitetaan kirjallisen ja kuvallisen esityksen lisäksi sellaista käyttösä vuoksi yhteen kuuluviksi tarkoitetuista merkeistä muodostuvaa tiettyä kohdetta tai asiaa koskevaa viestiä, joka on saatavilla selville vain automaattisen tietojenkäsittelyn tai äänen- ja kuvantoistolaitteiden taikka muiden apuvälineiden avulla. Edelleen lain 5.2 §:n mukaan *viranomaisen asiakirjalla* tarkoitetaan viranomaisen hallussa olevaa asiakirjaa, jonka viranomainen tai sen palveluksessa oleva on laatinut taikka joka on toimitettu viranomaiselle asian käsittelyä varten tai muuten sen toimialaan tai tehtäviin kuuluvassa asiassa. *Henkilörekisteri* taas on käyttötarkoituksen vuoksi yhteenkuuluvista

---

<sup>186</sup> Osoitusvelvollisuus uutena velvollisuutena velvoittaa rekisterinpitäjää tosiasiallisesti toteuttamaan henkilötietojen käsittelyn periaatteita. Tietosuojatyöryhmä on lausunnossaan (WP29 173, s. 3) ilmaissut osoitusvelvollisuuden tarkoituksena olevan rekisterinpitäjän vastuun ja aseman lisääminen ja tietosuojan tuominen käytäntöön. Tietosuojatyöryhmä myös katsoi osoitusvelvollisuuden tukevan tietosuojaviranomaisten työtä.

merkinnöistä muodostuva henkilötietoja sisältävä arvojoukko.<sup>187</sup> Viranomaisen asiakirjan antamisesta päättää se viranomainen, jonka hallussa asiakirja on (JulkL 14.1 §).

Nykyisen käytännön mukaan henkilötietojen luovutuksen sääntely viranomaisen tietovarannoista on tiukasti säänneltyä. Viranomainen luovuttaa tietoja julkisuuslain, henkilötietojen käsittelyä koskevien lakien sekä mahdollisen erityislain perusteella. Lähtökohtana tietojen luovuttamiselle on julkisuuslain säännökset, sillä julkisuuslaki on henkilötietojen luovutuksen osalta ensisijainen laki, jota noudatetaan viranomaistoiminnassa.<sup>188</sup> Rekisterinpitäjä on vastuussa luovuttamistaan tiedoista, eikä tietojen luovutus voi tapahtua ilman laista johdettavaa perustetta.<sup>189</sup> Lähtökohtana julkisuusperiaatteen mukaisesti on se, että tietopyyntöä ei yleensä tarvitse perustella. Asiakirjan pyytäjältä ei voida edellyttää selvitystä julkisen asiakirjan hyödyntämisen käyttötarkoituksesta. Jos pyyntö koskee salassa pidettävää asiakirjaa, pyyntö on perusteltava huomioiden luovuttamisen edellytysten selvittämiseksi vaaditut seikat. Perusteluvollisuus koskee myös pyyntöä saada tieto viranomaisen henkilörekisteristä, jos tieto siitä voidaan antaa vain erityisin edellytyksin.<sup>190</sup> Vaikka viranomainen olisikin julkisuuslainsäädännön mukaan velvollinen luovuttamaan määrätyt henkilötiedot, rekisterinpitäjän on varmistuttava, että tietojen vastaanottaja käsittelee henkilötietoja lain tarkoittamalla tavalla. Henkilötietolain muuttuessa oikeus saada tieto muuhun, kuin henkilötietolaissa säädettyyn tietojen luovutukseen viranomaisen henkilörekisteristä, sovelletaan edelleen mitä julkisuuslaissa säädetään.<sup>191</sup>

Julkisuuslaissa ei ole säädetty tiedonsaantipyynnön muodosta erikseen, joten pyyntö voidaan esittää kirjallisesti, suullisesti tai sähköisessä muodossa. Kun viranomaiselle esitetään tietopyyntö, on viranomaisen arvioitava tapauskohtaisesti tietoja pyytävän tahon tietojen käyttötarkoitus, lainmukaisuuden varmistus sekä selvittää millä tavoin tiedot suojataan.<sup>192</sup> Henkilötiedot kuuluvat lähtökohtaisesti henkilötietojen suojaa koskevan lainsäädännön piiriin myös silloin, kun kyseessä on julkisen sektorin julkinen asiakirja. Rekisterinpitäjän

---

<sup>187</sup> Voutilainen 2012, s. 75. Huomattava on myös tietosuoja-asetuksen määrittelemä sana ”rekisteri”, jolla tarkoitetaan mitä tahansa jäseneltyä henkilötietoja sisältävää tietojoukkoa, josta tiedot ovat saatavilla tietyin perustein, oli tietojoukko sitten keskitetty, hajautettu tai toiminnallisin tai maantieteellisin perustein jaettu.

<sup>188</sup> Voutilainen 2009, s. 141.

<sup>189</sup> Laista johdettavissa oleva peruste tietojen luovutukseen voi myös olla henkilön antama suostumus.

<sup>190</sup> Mäenpää 2016, s. 264-265.

<sup>191</sup> HE 9/2018, 28 §.

<sup>192</sup> Tietosuojavaltuutetun toimiston opas henkilötietojen luovuttamiseen viranomaisten henkilörekistereistä 27.7.2010, s. 4.

on siten edelleen suojattava henkilötiedot huolimatta tietojen julkisuudesta.<sup>193</sup> Julkisuuslain 13.2 §:n mukaan, jos tietoja voidaan luovuttaa viranomaisen henkilörekisteristä vain tietyin edellytyksin, rekisterinpitäjän on selvitettävä tarpeelliset seikat luovuttamisen edellytyksistä sekä tarvittaessa oikeus saada tiedonsaantipyynnön esittäjältä selvitys tietojen suojauksesta. Hallintovaliokunta on ottanut kantaa tiedonsaantipyynnön selontekovelvollisuuden osalta. Kannanoton mukaan *selontekovelvollisuus koskee tietoja henkilörekisteristä pyydettyäessä vain niitä tilanteita, joissa tietojen antamiselle on säädetty erityiset edellytykset. Näin pyydettyäessä tietoja sellaisesta henkilörekisteristä, joka sitä koskevien säännösten mukaan on tarkoitettu yleiseen käyttöön<sup>194</sup>, ei tietojen pyytäjällä ole velvollisuutta selvittää pyydettyjen tietojen käyttötarkoitusta.*<sup>195</sup>

Tietosuojavaltuutetun toimiston ohjeet koskien henkilötietojen luovuttamista viranomaisten henkilörekisteristä ohjaavat myös julkisuuslain 13.2 §:n tulkintaa. Ohjeen mukaan viranomaisen vastaa luovutuksen laillisuudesta ja tämän vuoksi *henkilötietojen pyytäjältä voidaan ja on syytä julkisuuslain 13.2 §:n mukaisesti aina pyytää asianmukainen selvitys luovutettavaksi pyydettyjen henkilötietojen käyttötarkoituksesta sekä muista tietojen luovuttamisen edellytysten selvittämiseksi tarpeellisista seikoista.*<sup>196</sup> Edelleen tietosuojavaltuutetun toimiston ohjeessa korostetaan viranomaisen roolia huolehtia siitä, että luovutuksensaaja voi käyttää luovutettuja henkilötietoja vain pyydettyyn käyttötarkoitukseen.

Viranomaisella on siis tietopyyntöjä koskeva selvitysvelvollisuus, jos pyyntö kohdistuu henkilörekisteriin, mutta yleiseen käyttöön tarkoitettusta rekisteristä voidaan viranomaisen harkinnan mukaan luovuttaa henkilötietoa ilman lisäselvitystä. Tällöin viranomaisen tulee selvittää tietopyynnön esittäjän oikeus käsitellä rekisteristä saatavia henkilötietoja.<sup>197</sup> Myös Korkeimmassa hallinto-oikeudessa on linjattu rekisterinpitäjän velvollisuuteen huolehtia vastaanottavan tahon tietojen suojaamisesta:

---

<sup>193</sup> WP 203, s. 48.

<sup>194</sup> Voutilaisen mukaan pääosin yleiseen käyttöön tarkoitettuja rekistereitä ovat muun muassa kaupparekisteri, ajoneuvorekisteri, kiinteistörekisteri ja väestötietojärjestelmän rekisterit. Näiden rekistereiden luovutuskäytännöistä säädetään kunkin rekisterin erityislainsäädännössä (Voutilainen 2012, s. 225)

<sup>195</sup> HaVM (26/1998) vp, s. 5-6.

<sup>196</sup> Tietosuojavaltuutetun toimiston opas henkilötietojen luovuttamiseen viranomaisten henkilörekistereistä 27.7.2010, s. 9.

<sup>197</sup> Voutilainen 2012, s. 217.



Tapauksessa Sanomalehti oli pyytänyt yliopistolta toimituksellista tarkoitusta varten tiedot yliopiston palveluksessa olevien professorien kokonaispalkasta eriteltyinä. Tällaiset nimikirjalaisissa olleet palkkatiedot olivat nimikirjalain 7 §:n perusteella julkisia tietoja. Yliopisto oli kieltäytynyt tietojen luovutuksesta ja viitannut Valtiovarainministeriön ohjeeseen VM 46/01/2006, jossa ohjataan huolellisuuteen luovutettaessa palkkatietoja. KHO:n mukaan yliopiston toiminta oli ollut julkisuuslain vastaista, ja sanomalehden tietojen käyttötarkoitus toimituksellisiin tarkoituksiin vastasi lain edellytyksiä. Oikeuden mukaan yksityisyyden suojalla ei voida perustella sitä, että lainsäädännön mukaan julkiseksi säädetty tiedot jätettäisiin antamatta. Päätöksessä mainitaan myös yliopiston rekisterinpitäjän velvollisuuksiin kuuluvana tehtävänä huolehtia henkilötietojen suojaamisesta henkilötietolain 32 §:ssä säädetyllä tavalla. Vaikka henkilötietojen luovutuksen edellytykset lain mukaan täytyisivät, rekisterinpitäjä on velvollinen selvittämään, että henkilötietojen käsittely tapahtuu lain mukaisesti. Tämän johdosta sanomalehden olisi annettava yliopistolle asianmukaiset selvitykset ja sitoumukset henkilötietojen suojaamisesta.<sup>198</sup>

Korkeimman hallinto-oikeuden linjauksen mukaisesti viranomaisen ei voi kieltäytyä luovuttamasta tietoja, vaikka ne eivät olisikaan yleiseen käyttöön tarkoitettu, jos tiedot kuitenkin kuuluvat julkisuuslain piiriin, eivätkä ole salassa pidettäviä. Tällöin rekisterinpitäjän selvitysvelvollisuus korostuu siltä osin, että kenenkään henkilötietojen käsittely ei vaaranna luovutettaessa tietoja julkisuuslain nojalla. Viranomaisen on salassa pidettävien tietojen tai henkilötietojen pyytäjän osalta tosiasiallisesti varmistuttava tiedon luovuttamisen oikeellisuudesta. Pelkkä oletama tiedonsaantiin liittyvästä oikeudesta ei riitä, vaan viranomaisen on selvitettävä henkilötiedon tai salassapidettävän tiedon luovuttamiseen oikeuttava nimenomainen säännös, jonka nojalla tietoja voidaan antaa, ja missä laajuudessa.<sup>199</sup>

#### **AOK 187/1/2009, antopäivä 8.2.2011**

Apulaisoikeuskansleri nimenomaisesti korosti, että salassa pidettäviä tietoja voidaan luovuttaa vain julkisuuslaissa säädettyillä edellytyksillä. Viranomaisen perusteltukaan käsitys siitä, että tiedon saajalla on valtuudet asian hoitamiseen tai että luovutettavat tiedot ovat jo hänen tiedossaan, eivät ole riittävä peruste tietojen luovuttamiseen.

---

<sup>198</sup> KHO 2012:55.

<sup>199</sup> Voutilainen 2012, s. 217.

Ellei toisin säädetä, viranomaisen henkilökisteristä voidaan luovuttaa henkilötietoja kopiona, tulosteena tai sähköisessä muodossa, *jos luovutuksensaajalla on henkilötietojen suoja koskevien säännösten mukaan oikeus tallettaa ja käyttää sellaisia tietoja* (JulkL 16.3). Henkilötietojen antaminen julkisuuslain 16.3 §:n nojalla viranomaisen pitämästä henkilökisteristä on erityisasemassa. Henkilötietojen luovutus viranomaisen henkilökisteristä ei ole rajoituksetonta, vaan luovuttamisen edellytyksenä on luovutuksensaajan oikeus tallettaa ja käyttää pyytämiään viranomaisen henkilökisteriin sisältyviä henkilötietoja. Käytännössä tietoja luovuttavan viranomaisen on selvitettävä, onko tietojen pyytäjällä julkisuuslain 16.3 §:ssä tarkoitettu oikeus henkilötietojen tallettamiseen ja käyttämiseen.<sup>200</sup> Viranomaisella on siten 16.3 §:n mukaan selvittämismääräisyys henkilötietojen luovutuksen yhteydessä, ellei erikseen ole toisin säädetty.<sup>201</sup> Sen sijaan viranomaisen henkilökisterissä oleva julkinen henkilötieto voidaan antaa *henkilökohtaisiin tai tavanomaisiin yksityisiin tarkoituksiin* selvittämättä tarkemmin tiedon pyytäjän käyttötarkoitusta. Perusteluvuorollisuus voi kuitenkin myös tällöin tulla kyseeseen, mikäli henkilötieto pyydetään kopiona, tulosteena tai sähköisessä muodossa.<sup>202</sup>

#### **KHO 4.10.2010 T 2558**

Virasto oli hylännyt pyynnön saada sen henkilöstön yksilöidyt palkkatiedot sillä perusteella, ettei pyytäjällä ollut julkisuuslain 16.3 §:n mukaista oikeutta tallettaa ja käyttää pyytämiään henkilötietoja. KHO:n ratkaisun mukaan 16.3 § ei estä asiakirjan antamista viranomaisen luona nähtäväksi ja jäljennettäväksi. Tiedonsaantipyynnön esittäjä oli ilmoittanut, että pyyntö ei koskenut palkkatietojen ohella henkilöiden nimiä, joten kyse ei ollut henkilötietojen luovuttamisesta, eikä asiaa tullut arvioida julkisuuslain 16.3 §:n nojalla.

Julkisuuslain 13.2 § ja 16.3 § säätelevät henkilötietojen luovuttamisesta viranomaisen rekisteristä hieman eri tavoin. Tiivistettynä voidaan todeta, että 13.2 § oikeuttaa viranomaisen pyytämään aina selvitystä tietoja pyytävältä taholta, mikäli tiedot pyydetään

<sup>200</sup> Wallin – Konstari 2000, s. 214.

<sup>201</sup> Esimerkkinä mainittakoon laki väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista, jota Väestörekisterikeskus soveltaa luovuttaessa henkilötietoja väestötietojärjestelmästä. Lain 28 §:ssä säädetään tietojen luovuttamisen yleisistä edellytyksistä: *Väestötietojärjestelmän tietoja voidaan luovuttaa vain, jos tässä laissa säädetyt edellytykset tietojen luovuttamiselle ovat olemassa eikä henkilön oikeudesta kieltää tietojensa luovuttaminen muuta johdu. Väestötietojärjestelmästä luovutettavan tiedon tulee olla tarpeellinen siihen käyttötarkoitukseen, johon se luovutetaan.* Myös lain 44 §:ssä säädetään rekisterihallinnon viranomaisen oikeudesta pyytää tarvittaessa selvitys tietojen suojauksesta, mikäli pykälän ehdot täyttyvät. Väestörekisterikeskus soveltaa siten erityislakia yli julkisuuslain, eikä julkisuuslain 16.3 §:ää sovelleta luovutettaessa henkilötietoja väestötietojärjestelmästä.

<sup>202</sup> Mäenpää 2016, s. 265.

luovutettavaksi otteina, kopiona tai sähköisessä muodossa. Toisaalta taas 13.2 § mahdollistaa tietojen luovutuksen ilman tarkempaa selvitystä, mikäli henkilörekisteri on tarkoitettu yleiseen käyttöön.<sup>203</sup> 16.3 § taas edellyttää viranomaisen varmistuvan siitä, että henkilötietoja luovutetaan vain lailliseen tarkoitukseen eli viranomaisella on selvittämisvelvollisuus henkilötietojen luovutuksen yhteydessä, ellei erikseen ole toisin säädetty.<sup>204</sup> Lain ja oikeuskäytännön valossa on perusteltua todeta julkisen henkilötiedon tarkoittavan eri asiaa kuin yleiseen käyttöön tarkoitettu henkilötieto. Voutilaisen mukaan *viranomaisella on henkilötietojen luovutuksen osalta selvittämisvelvollisuus siitä, että onko luovutuksensaajalla lainmukainen oikeus käsitellä henkilötietoja omassa toiminnassaan, jos henkilötiedot liittyvät tietokokonaisuuteen, joka on salassa pidettävää tai asianosaisjulkisuuden piiriin kuuluvaa tai tiedot ovat julkisia, mutta eivät kuitenkaan ole tarkoitettu yleiseen käyttöön.* Mikäli julkiset henkilötiedot kuuluvat yleissääntelyn piiriin, selonteko- ja selvitysvelvollisuus on aina olemassa. Luovuttaessa tietoja henkilörekisteristä viranomaisen on siten aina tehtävä päätös, jossa otetaan kantaa tietoja pyytävän tahon oikeuteen saada kyseiset tiedot. Päätöstä ei tarvitse tehdä tilanteessa, jossa kyseessä on yksittäinen julkinen henkilötieto, tai laissa on nimenomaisesti säädetty henkilörekisterin yleisestä käytöstä.<sup>205</sup>

### 5.3 Rekisterinpitäjän vahingonkorvausvelvollisuus

Rekisterinpitäjä on vastuussa käsittelemistään henkilötiedoista. Henkilötietolaissa säädetään lain 47 § :n 1 momentissa vahingonkorvausvelvollisuudesta. Pykälän mukaan rekisterinpitäjä on ollut ”velvollinen korvaamaan sen taloudellisen ja muun vahingon, joka on aiheutunut rekisteröidylle tai muulle henkilölle tämän lain vastaisesta henkilötietojen käsittelystä”. Henkilötietolain mukainen korvausvastuu on tarkoittanut ankaraa vastuuta ja siihen on riittänyt pelkästään vahingon aiheuttaminen, olipa se aiheutettu tuottamuksellisesti tai ei. Korvausvastuu on kuitenkin edellyttänyt syy-yhteyttä tietojen lainvastaisen käsittelyn ja aiheutuneen vahingon välillä. Näyttövelvollisuus syy-yhteydestä on kuulunut vahingonkärsijälle.<sup>206</sup>

---

<sup>203</sup> Voutilainen 2007, s. 141.

<sup>204</sup> Tietosuojavaltuutetun toimiston opas henkilötietojen luovuttamiseen viranomaisten henkilörekistereistä 27.7.2010, s. 14.

<sup>205</sup> Voutilainen 2007, s. 224-226.

<sup>206</sup> Pitkänen ym. 2013, s. 278-281.

Tietosuoja-asetuksen tullessa voimaan sovelletaan asetuksen 82 §: ää vahingonkorvauksiin liittyen. Asetuksen 1. kohdan mukaan henkilöllä on oikeus saada rekisterinpitäjältä tai henkilötietojen käsittelijältä korvaus aiheutuneesta vahingosta, mikäli asetusta on rikottu aiheuttaen aineellista tai aineetonta vahinkoa. Artiklan 2 ja 3 kohdat taas säättävät henkilötietolakia väljemmin vahingonkorvausvastuusta:

*2. Kukin tietojenkäsittelyyn osallistunut rekisterinpitäjä on vastuussa vahingosta, joka on aiheutunut käsittelystä, jolla on rikottu tätä asetusta. Henkilötietojen käsittelijä on vastuussa käsittelystä aiheutuneesta vahingosta vain, jos se ei ole noudattanut nimenomaisesti henkilötietojen käsittelijöille osoitettuja tämän asetuksen velvoitteita tai jos se on toiminut rekisterinpitäjän lainmukaisen ohjeistuksen ulkopuolella tai sen vastaisesti.*

*3. Rekisterinpitäjä tai henkilötietojen käsittelijä on vapautettava vastuusta 2 kohdan nojalla, jos se osoittaa, ettei se ole millään tavoin vastuussa vahingon aiheuttaneesta tapahtumasta.*

Asetuksen mukaan rekisterinpitäjä tai henkilötietojen käsittelijä ei automaattisesti ole vastuussa aiheutuneesta vahingosta. Mikäli voidaan osoittaa vastuusta vapautumisen perusteet, ei vahingonkorvausta voida tällöin vaatia. Edelleen artiklan 4 ja 5 kohdissa säädetään vastuun jakautumisesta silloin, kun tietojenkäsittelyyn on osallistunut useampi kuin yksi rekisterinpitäjä tai henkilötietojen käsittelijä. Tällöin kukin vahinkoon liittynyt rekisterinpitäjä tai henkilötietojen käsittelijä on vastuussa koko vahingosta. Vahingonkorvaukseen sovelletaan siis yhteisvastuullista vastuuta.<sup>207</sup>

Hallituksen esityksessä 9/2018 tietosuoja-asetusta täydentäväksi lainsäädännöksi on huomioitu henkilötietolain vahingonkorvausvelvollisuuden lähtökohtien poikkeavuus suhteessa asetukseen. Esityksen mukaan tietosuoja-asetus poikkeaa henkilötietolain lähtökohdista siltä osin, että se olisi riski henkilötietolain aikana voimassaolleille oikeussuhteille ja sopimuksille. Tästä johtuen, jos vahinkoa aiheuttanut teko on tehty ennen uuden tietosuojalain voimaantuloa, lain 38.5 §: n mukaisesti velvollisuuteen korvata vahinko sovelletaan voimassa olleita säännöksiä. Ankaruus vastuu jatkuu edelleen siis siltä osin, kun vahinko on aiheutettu ennen uuden tietosuojalain voimaan tuloa. Hallituksen esityksessä kuitenkin huomautetaan, että viranomaisen ollessa rekisterinpitäjänä, toimivat virkamiehet

<sup>207</sup> Yhteisvastuullinen vahingonkorvaus tarkoittaa sitä, että täyttä korvausta voidaan vaatia jokaiselta vahingonaiheuttajalta yksinään, yli oman osuutensa. Tällöin vahingon maksaneella on oikeus periä muilta vahingonkorvausvelvollisilta se osuus korvauksesta, joka vastaa heidän osuuttaan. Katso lisää tietosuoja-asetuksen 82 artiklan 5 kohta sekä vahingonkorvauslain (412/1974) 6 luku.

virravastuun alla ja henkilötietojen käsittely kuuluu viranomaisissa työskentelevien virkavelvollisuuksiin. Viranomaisia sitoo hallinnon lainmukaisuusperiaate, ja viranomaisen on myös noudatettava hallinnon yleislakeja. Virkamiehen asemaan kuuluu myös muita laajempi vastuu virheistä. Virkavastuu voi toteutua rikosoikeudellisena virkavastuuna, kurinpidollisena virkavastuuna sekä vahingonkorvausvastuuna.<sup>208</sup>

Suostumushallintarekisteriä ja yksilöiden hallinnoimia rekisterinpitäjälle myönnettäviä käyttöluovia harkittaessa on syytä ottaa huomioon mahdolliset tilanteet, joissa asetuksen 82 §: n mukaisia vahingonkorvaustilanteita joudutaan pohtimaan. Rekisterinpitäjän luovuttaessa henkilötietoja oman harkintansa perusteella, on se nykyisen julkisuuslain mukaan vastuussa tiedon luovuttamisen lainmukaisuudesta sekä siitä, mihin tietoja tullaan jatkossa hyödyntämään. Mikäli henkilötiedot luovutettaisiin yksilön antaman suostumuksen perusteella, vastuukysymyksien osalta herää paljon huomiota kysymyksiä: Mikä on luovuttavan rekisterinpitäjän vastuu tilanteessa, jossa luovutetaan vääriä henkilötietoja? Onko vastaanottava rekisterinpitäjä vastuullinen tarkastamaan luovutettujen tietojen oikeellisuuden? Mikä on suostumuksen antaneen henkilön vastuu, mikäli luovutettavia tietoja ei ole yksilöity riittävästi? Onko vastuu suostumuksen yksilöllisyydestä vastaanottavalla vai tietoja luovuttavalla rekisterinpitäjällä? Voiko olla tilannetta, jossa sekä henkilötietoja luovuttava rekisterinpitäjä, että tiedot vastaanottanut rekisterinpitäjä vastaavat rekisteröidylle aiheutuneesta vahingosta yhteisvastuullisesti?

Mikäli suostumushallintarekisterissä yksilö voisi säädellä viranomaisen rekistereissä olevia, myös muiden kuin itsensä tuottamiensa tietojen osalta henkilötietojen käsittelyä, tulisi viranomaisen yksityistä organisaatiota laajempi vastuu ottaa huomioon. Virkamies työskentelee virkavastuulla, joten vastuukysymykset henkilötietojen luovuttamiseen tilanteessa, jossa viranomaisen ei tee arviota luovutuksen mahdollisista seurauksista, olisi hyvä säätää lain tasolla, tai vaihtoehtoisesti mahdollisessa yleisesti säädetyssä käyttöluvassa. Rekisteröidyn oma toiminta ja sen osalta vastuun ulottuvuus on myös näkökulma, joka tulisi ottaa huomioon rekisterinpitäjän ja henkilötietojen käsittelijän vastuun ohella.

---

<sup>208</sup> HE 9/2018, s. 106 ja 123.

#### 5.4 Julkisuuslain soveltaminen suostumushallintarekisteriin

Julkisen hallinnon toiminta on tietointensiivistä. Asian käsittely viranomaisissa on keskeisiltä osin tiedonhallintaa,<sup>209</sup> ja viranomainen tulee jatkossakin luovuttamaan tietoja julkisuuslain nojalla.<sup>210</sup> Hallintovaliokunnan kannanotossa erikseen korostetaan julkisuuslain soveltamista aina silloin, kun luovutetaan tietoja viranomaisen henkilörekisteristä, ellei sovellettavana ole erityislainsäädäntöä.<sup>211</sup> Nykyisen julkisuuslain henkilötietojen luovutus edellyttää viranomaiselta rekisterinpitäjänä velvollisuutta huolehtia siitä, että tietoja todella voidaan lain nojalla luovuttaa ja vastaanottava taho tulee käsittelemään tietoja lain vaatimusten mukaisesti. Viranomaisella on myös tietyissä tilanteissa oikeus, taikka velvollisuus pyytää vastaanottavalta taholta selvitystä siitä, miten tietojen suojaus tullaan järjestämään. Tietoja luovuttava viranomainen voi siten kieltäytyä tietojen luovutuksesta myös sillä perusteella, ettei katso tietojen suojauksen olevan tietoja pyytävällä taholla vaaditulla tasolla. Viranomaisten hallussa olevien tietojen luovutus tapahtuisi suostumushallintarekisteriin tehtyjen suostumusten perusteella myös lähtökohtaisesti julkisuuslain nojalla. Tietojen luovutuksesta voidaan säätää myös rekisterikohtaisesti erityislainsäädännössä, mutta lähtökohtana tulisi olla yhdenmukainen sääntely, jotta henkilötietoja koskeva sääntely ei todellisuudessa hajaantuisi entisestään.<sup>212</sup> Lainsäädännön virtaviivaistaminen ja selkeyttäminen edesauttaa digitalisaation kehittymistä.<sup>213</sup>

Suostumushallintarekisterin lähtökohtana on se, että tiedot luovutettaisiin ilman selvityksiä sen perusteella, että rekisteröity on antanut luovutukseen suostumuksensa. Tällöin

<sup>209</sup> Voutilainen – Huttunen 2015, s. 69.

<sup>210</sup> TATTI-työryhmän mietinnössä ei lopulta päädytty ehdottamaan muutoksia julkisuuslain, mutta työryhmän liitteenä oli julkisuuslain muutoksia arvioitu. Hallituksen esityksessä uudeksi tietosuojalain (HE 9/2018) on mainittu, että suurin osa mietintöä lausuneista tahoista katsoi, että tietosuojalain säätämisen johdosta olisi välttämätöntä tehdä muutoksia myös julkisuuslakiin. Jatkovalmistelun yhteydessä päätettiin, että julkisuuslakiin tehtäviä muutostarpeita arvioidaan myöhemmin erikseen. Valmisteilla olevaan tiedonhallinnan lainsäädäntöön on tarkoitus koota sääntelyä julkisuuslaista, arkistolaista ja tietohallintolaista, mutta sääntelyn sisältö on vielä tarkentamatta tämän tutkielman kirjoitushetkellä syksyllä 2018.

<sup>211</sup> HaVM 26/1998, s. 5.

<sup>212</sup> Juho Salminen kirjoittaa Suomen Kuvalehden artikkelissaan, että tietosuojavaltuutetun mukaan Suomessa on yli miljoona erilaista henkilörekisteriä. Se jo itsessään kuvastaa massaa, jonka sääntelyä tulisi enemmänkin yhdenmukaistaa yleislainsäädännön tasolla sen sijaan, että säädettäisiin erityislainsäädännöllä erilaisista henkilörekistereistä, Salminen 2011.

<sup>213</sup> Ks. Esimerkiksi Kalle Määtän tekemä selvitys sähköisen asioinnin nykytilasta ja siihen liittyvästä sääntelystä. Selvityksessään Määtä toteaa lainsäädännön olevan osittain esteenä sähköisen asioinnin kehittymiselle. Määtän mukaan erityislainsäädäntöä tulisi karsia ja sähköiseen asiointiin liittyvää lainsäädäntöä tulisi ylipäätään selkeyttää. Valtiovarainministeriön julkaisu 22/2018, s. 253-260.

viranomaisen ei tulisi tarkastaa käyttötarkoitusta tai tietojen suojaamista julkisuuslain edellyttämällä tavalla, vaan suostumus toimisi viranomaiselle hyväksyttävänä perusteena luovuttaa kyseinen henkilötieto. Mikäli kyseessä olisi tietosuoja-asetuksen 20 artiklan mukainen tilanne, jossa luovutuksen kohteena on tieto, jonka rekisteröity on itse toimittanut viranomaiselle ja käsittely on perustunut suostumukseen, ei ongelmaa tule suhteessa julkisuuslain luovutussäännöksiin. Sen sijaan haasteita nykyistä julkisuuslakia sovellettaessa tulisi silloin, kun kyseessä olisi viranomaisen tuottamaa tietoa henkilöstä, jolloin tietosuoja-asetuksen 20 artiklaa ei sovelleta. Tällöin rekisteröidyllä ei olisi automaattisesti asetuksen mukaista oikeutta saada siirtää tiedot järjestelmästä toiseen, joten kyseeseen tulisi julkisuuslain luovutusedellytykset tai vaihtoehtoisesti erityislainsäädäntöä, mikäli luovutettava henkilötieto olisi jonkin erityislainsäädännön piirissä. Tällöin nykylainsäädännön mukaisesti viranomaisen vastuulla olisi tarkistaa pyytävän tahon oikeus käsitellä pyydettyjä henkilötietoja sekä mahdollisesti myös tarkistaa se, miten tietojen suojaus olisi aikomuksena järjestää. Tämä ei kuitenkaan palvelisi omadata-ajatusta, jonka perusideana on henkilön itsemääräämisoikeus omista henkilötiedoistaan. Tällöin yksilön antama suostumus ei todellisuudessa tarkoittaisi sitä, että tiedot luovutettaisiin automaattisesti, vaan välissä tulisi viranomaisen tarkastus luovutettavan tiedon käsittelyoikeudesta sekä muista lainsäädännöllisistä edellytyksistä. Mikäli suostumushallintarekisterin perusteella halutaan mahdollistaa myös viranomaisen henkilötietojen luovuttamista, joka ei ole rekisteröidyn itse toimittamaa tietoa viranomaiselle, tulisi nähdäkseni julkisuuslain säädöksiä tältä osin muuttaa, tai lisätä lainsäädäntöön yksilön omien tietojen luvittamisen mahdollisuus.

Oikeusministeriön TATTI-mietinnössä on otettu kantaa julkisuuslain muutoksiin tietosuoja-asetuksen johdosta. Työryhmä oli yksimielinen siitä, että julkisuuslain uudistamistarvetta olisi syytä arvioida, mutta työryhmä ei päässyt yksimielisyyteen siitä, millä tavoin henkilötietojen suoja ja asiakirjojen julkisuus tulisi sovittaa yhteen, joten varsinaisia muutosehdotuksia ei mietinnössä ole. Sen sijaan mietinnön lopussa on eriteltyinä julkisuuslain muutosehdotuksia siltä osin, kun työryhmä ei ole saavuttanut yhteisymmärrystä.<sup>214</sup> Mietinnön yleisperusteluissa koskien henkilötietojen suojan ja julkisuusperiaatteen yhteensovittamista on kiinnitetty erityisesti huomiota julkisuuslain 16.3 §:ään. Työryhmän mukaan kyseinen luovutusrajoitus on hyvä lähtökohta henkilötietojen suojan ja julkisuusperiaatteen yhteensovittamiselle. Samalla todetaan kuitenkin se, ettei

---

<sup>214</sup> EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmän (TATTI) mietintö 2017, s. 36-37.

nykysääntelyssä oteta riittävällä tavalla huomioon tietosuoja-asetuksen ja käytännön yhteensovittamistilanteita. Koska yleisen tietosuoja-asetuksen myötä käsittelyn lainmukaisuuden edellytykset väljentyvät merkittävästi nykyisestä, julkisuuslain 16.3 § ei suojaa henkilötietoja samalla tavalla kuin pykälää säädettyä.<sup>215</sup>

Mietinnössä on lähestytty julkisuuslain ja henkilötietojen suojan yhteensovittamista perusoikeuskirjan näkökulmasta.<sup>216</sup> Perusoikeuskirjan 8 artiklassa säädetään henkilötietojen suojasta. Artiklan 1. kohdan mukaan jokaisella on oikeus henkilötietojensa suojaan sekä 2. kohdan mukaan tietojen käsittelyn on *oltava asianmukaista ja tapahduttava tiettyä tarkoitusta varten ja asianomaisen henkilön suostumuksella tai muun laissa säädetyn oikeuttavan perusteen nojalla*. Edelleen 52 artiklan nojalla perusoikeuskirjassa turvattuja oikeuksia voidaan rajoittaa ainoastaan lailla ja suhteellisuusperiaatetta noudattaen, eli rajoitusten tulee olla välttämättömiä ja niiden tulee vastata unionin tunnustamia tavoitteita suojella muiden henkilöiden oikeuksia ja vapauksia.

Koska perusoikeuskirjan 8 artiklan mukaan henkilötietojen käsittelyn on tapahduttava tiettyä tarkoitusta varten, henkilötietojen suojan ja julkisuusperiaatteen yhteensovittaminen edellyttää tästä periaatteesta poikkeamista. TATTI-mietinnön mukaan viranomaisen luovuttaessa henkilötietoja julkisuuslain nojalla tiettyä tarkoitusta varten, ei henkilötiedon myöhempi käyttötarkoitus välttämättä vastaa alkuperäistä käyttötarkoitusta. Tällöin tulee arvioida käyttötarkoitusvelvollisuudesta poikkeamista suhteellisuusperiaatteen näkökulmasta, eli onko poikkeaminen välttämätöntä saavutettavaan päämäärään nähden. Keskeisenä ehdotuksena yksityiskohtaisten perustelujen kera mietinnössä ehdotetaan henkilötietojen suojan ja julkisuusperiaatteen yhteensovittamisen lähtökohdaksi yleisen tietosuoja-asetuksen. Tällöin viranomaisen asiakirjasta voitaisiin antaa henkilötietoja vastaanottajalle, jolla on tietosuoja-asetuksen mukainen oikeus käsitellä tietoja.<sup>217</sup>

Mietinnön ehdottama lähtökohta on mielestäni hyvä suunta julkisuuslain muutoksille. Julkisuuslaki on luonteeltaan toissijainen, joten erityislainsäädäntöön mahdollisesti sisältyvät henkilötietojen luovutusta koskevat sääntelyt jäisivät julkisuuslakiin tehtyjen

---

<sup>215</sup> EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmän (TATTI) mietintö 2017, s. 209.

<sup>216</sup> Euroopan unionin perusoikeuskirja (2000/C 346/01) on ollut oikeudellisesti sitova 1.12.2009 lähtien. Perusoikeuskirjan johdannon mukaan siinä muun muassa vahvistetaan yhteisön ja unionin toimivallan ja tehtävien sekä toissijaisuusperiaatteen mukaisesti oikeudet, jotka perustuvat erilaisiin jäsenvaltioiden yhteisiin perinteisiin, kansainvälisiin velvoitteisiin, kansainvälisiin sopimuksiin sekä unionin tuomioistuinten oikeuskäytäntöihin.

<sup>217</sup> EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmän (TATTI) mietintö 2017, s. 210.



muutosten myötä vielä tarkasteltavaksi.<sup>218</sup> Yksilöllä on varsin laaja oikeus saada itseään koskevia tietoja viranomaisilta ja tietosuoja-asetuksen myötä tiedon läpinäkyvyys on entistä tärkeämpää. Omadatan sääntelyn näkökulmasta katsottuna tulee kuitenkin ottaa huomioon myös tietojen luovuttamisen ohella tiedon siirto. Tietosuoja-asetus ei lähtökohtaisesti säädi suostumuksen perusteella luovutettavasta tiedosta aiempaa eri tavalla, lukuun ottamatta asetuksen 20 artiklaa, jossa edellytetään rekisterinpitäjää mahdollistamaan tiedon siirto suoraan toiselle rekisterinpitäjälle rekisteröidyn näin halutessa. Tietosuoja-asetukseen ei siis velvoita viranomaista siirtämään sellaisia tietoja toiselle rekisterinpitäjälle, jotka eivät ole rekisteröidyn itse toimittamaa henkilötietoa. Vaikka julkL:n 16 §:n 3 momentissa on säädetty viranomaiselle mahdollisista tavoista luovuttaa henkilörekisteristä henkilötietoja, ei lainkohdassa ole mainittu teknisen käyttöyhteyden avaamisesta. Henkilötietojen luovuttaminen teknisen käyttöyhteyden avulla vaatii lailla säätämistä.<sup>219</sup>

Suostumushallintarekisterissä olennaista on juuri se, että tietoja haluavan rekisterinpitäjän järjestelmästä tehdään kysely suostumushallintarekisteriin, josta ilmenee, onko suostumus annettu. Mikäli suostumus on annettu, henkilötiedon luovuttavan rekisterinpitäjän on luovutettava tieto suoraan luovutuksen kohteelle. Tällaisesta viranomaisen tuottamasta henkilötiedon luovuttamisesta rekisteröidyn suostumuksen perusteella suoraan toiselle rekisterinpitäjälle ei säädetä juuri missään lainsäädännössä.<sup>220</sup> Lähtökohtaisesti julkisuuslain säädökset velvoittavat rekisterinpitäjää selvittämään henkilötiedon käyttöoikeus sekä käyttötarkoitus. Mikäli viranomaisen tietojen luovutus suostumushallintarekisteriin pohjautuen rajoittuu vain sellaiseen tietoon, jonka rekisteröity on itse toimittanut viranomaiselle, kansalaisen itsemääräämisoikeus omasta henkilötiedostaan kaventuu huomattavasti verrattuna tilanteeseen, jossa suostumuksella voitaisiin hallita myös viranomaisen tuottamaa tietoa.

## **5.5 Vastuu henkilötiedosta siirrettäessä tieto suoraan rekisterinpitäjältä toiselle**

Omadatan luomassa henkilötiedon hallinnassa merkittävä muutos on henkilön itsensä rooli suhteessa rekisterinpitäjiin. Yksityisen henkilön hallinnoidessa omia tietojaan muuttaisi se vahvasti sitä asetelmaa, jossa kaksi rekisterinpitäjää vaihtavat tietoja keskenään

---

<sup>218</sup> Wallin – Konstari 2000, s. 215.

<sup>219</sup> Valtiovarainministeriön julkaisu 22/2018, s. 233-234.

<sup>220</sup> Tästä poikkeuksena kuitenkin muun muassa niin sanottu KOSKI-laki sekä Liikenteen turvallisuusvirastoa koskeva lainsäädäntö, joissa omadata on otettu huomioon siten, että myös viranomaisen tuottama tieto velvoitetaan siirrettäväksi. Katso luku 3.3 omadatasta.

rekisteröidyn tietämättä tai tiedostaen. Rekisterinpitäjää koskevia säännöksiä sovelletaan sekä tietojen luovuttajaan eli viranomaiseen että vastaanottajaan.<sup>221</sup> Uuden mallin mukaisesti henkilötiedon luovuttamiseen liittyisi toteutuksesta riippuen kahden toimija sijaan kolme; alkuperäinen rekisterinpitäjä, henkilötiedon vastaanottava rekisterinpitäjä sekä henkilötiedon kohteena oleva yksilö. Mikäli kyseessä olisi keskitetty suostumushallinta, neljäs toimija olisi palvelu, johon suostumukset keskitetyksi tallennetaan. Tästä keskitetystä suostumushallintarekisteristä tulisi rekisteri, jonka avulla lakisääteinen käsittelyvelvollisuus todennetaan. Rekisterinpitäjällä ei kuitenkaan olisi vastuuta henkilötiedon luovutukseen liittyen, vaan luovutettavana olevat henkilötiedot luovutettaisiin lähderekisteristä, eikä niitä tuotaisi suostumushallintarekisteriin missään vaiheessa.<sup>222</sup>

Vastuukysymykset tulisi olla hyvin selvillä henkilötietoa luovutettaessa, kun kyseessä olisi omadata-mallin mukainen suostumukseen perustuva henkilötiedon luovutus. Valtioneuvoston selvityksessä on ehdotettu uudeksi malliksi yksilöiden hallitsemat käyttöluvat:<sup>223</sup>

*”Väestörekisterikeskus antaa tietojen hyödyntäjälle hallinnollisen päätöksen, ns. tietoluvan. Tämä pitää sisällään tiedon hyödyntäjän oikeudet, velvollisuudet ja mahdolliset maksut. MyData muuttaisi nämä tietoluvat yksilöiden hallitsemiksi käyttöluviksi. Sopimuksen tietojen käytöstä tekisi se henkilö, jonka tiedoista on kysymys. Tämä vähentää tarvetta luvitukselle ja siihen liittyvälle hallinnolle. Kokonaan tietoluvat eivät häviä, mikäli halutaan edelleen mahdollistaa tietojen luovutus maksullisesti ilman yksilötason käyttölupia”.*

Edelleen selvityksessä on esitetty mahdollista ratkaisua liittyen tietoturvan tason valvontaan. Selvityksessä esitetyn käyttöluvan johdosta viranomainen ei voisi enää tarkastaa tietoturvaa, vaan tiedon jakaminen siirtyisi ihmisen itsensä vastuulle:

*Mahdollinen tapa riskien hallintaan olisi se, että laadittaisiin standardisopimus pohjia osaksi MyDataa hyödyntävien palvelujen käyttäjäehtoja. Näin julkinen valta voi vaikuttaa siihen, miten henkilötietoa käytetään myös MyDataan perustuvissa ratkaisuisissa. Sopimus*

<sup>221</sup> Valtiovarainministeriön julkaisu 2/2012, s. 73-80.

<sup>222</sup> Ks. tarkemmin mahdollisesta suostumushallintapalvelun toteutuksesta kappaleesta 3.3.

<sup>223</sup> Myös SITRA on aloittanut IHAN-hankkeen, jonka tarkoituksena on luoda kokonaan uusi datatalouden malli vuoteen 2021 mennessä. Hankkeessa on tarkoitus rakentaa MyWallet -niminen omadata-tili, jossa säilytetään yksilölliset tunnisteet kutakin datakokonaisuutta koskien. Yksilö antaa luvan, jonka perusteella palvelutuottaja saa käyttää luvassa määriteltyä henkilötietoa. Hankkeen tavoitteena on määritellä yhteiset, EU-tason periaatteet ja hallintamalli, Sitra 2018.

*tehtäisiin kuitenkin aina palveluntarjoajan ja henkilön välillä, ja sopimus pohja olisi ennen kaikkea suositus käyttöehdoiksi.*<sup>224</sup>

Vastuukysymyksiä omadataan perustuvan henkilötiedon luovutuksen osalta on hyvä tarkastella tietosuoja-asetuksen 20 artiklan valossa. Kyseinen artikla luo rekisteröidylle omadata-mallin mukaista oikeutta siirtää tiedot järjestelmästä toiseen. Siirto-oikeus ei kuitenkaan luo subjektiivista oikeutta siirtää tietoja suoraan järjestelmästä toiseen, vaan siirto-oikeus on olemassa silloin, kun se teknisesti on mahdollista. Vaikka siirto-oikeus rajoittuu henkilön itsensä tuottamaan tietoon, tietosuoja-asetusta voidaan kuitenkin pitää lähtökohtaisesti pohjana myös tilanteelle, jossa viranomaisen luovuttaa viranomaisen omassa rekisterissä olevaa, viranomaisen itsensä tuottamaa henkilötietoa. Nykyinen julkisuuslain mukainen rekisterinpitäjän vastuu ei sovellu omadatan edellyttämään tiedon luovutukseen, johtuen alkuperäisen rekisterinpitäjän pääasiallisesta vastuusta.<sup>225</sup>

Tietosuojatyöryhmä on julkaissut ohjeita tietosuoja-asetuksen mukaisesta oikeudesta siirtää henkilötietoja järjestelmästä toiseen. Työryhmän mukaan uusi tiedonsiirtokelpoisuus pyrkii vahvistamaan yksilön oikeuksia omiin henkilötietoihinsa siten, että se helpottaa yksilön kykyä siirtää tai kopioida tiedot helposti yhdestä IT-ympäristöstä toiseen. Vahvistamalla yksilöiden henkilökohtaisia oikeuksia artikla edustaa mahdollisuutta tasapainottaa rekisteröidyn ja rekisterinpitäjän välistä suhdetta. Rekisterinpitäjä, joka vastaa pyyntöön siirtää tiedot edelleen, ei ole vastuussa tietojen käsittelystä rekisteröidyn tai toisen rekisterinpitäjän taholta tapahtuvasta tietojen käsittelystä. Tietoja siirtävä rekisterinpitäjä toimii rekisteröidyn lukuun myös silloin, kun tiedot siirretään suoraan rekisterinpitäjän järjestelmästä toiselle rekisterinpitäjälle. Tiedon luovuttaja ei myöskään ole vastuussa vastaanottavan rekisterinpitäjän toimimisesta tietosuojalain mukaisesti, kun otetaan huomioon myös se, että luovuttava taho ei ole valinnut sitä kenelle tiedot luovutetaan. Samaan aikaan tietojen luovuttajan tulee kuitenkin varmistaa, että se toimii rekisteröidyn tahdon mukaisesti. Edelleen tietosuojatyöryhmä on linjannut, että rekisterinpitäjä, joka luovuttaa tietoa artiklan 20 nojalla, ei ole varsinaista velvollisuutta tarkistaa ja yksilöidä siirrettävän tiedon laatua ennen tiedon siirtämistä edelleen.<sup>226</sup> Kuitenkin henkilötietojen tulee olla tarkkoja ja täsmällisiä artiklan 5 mukaisesti. Tietojen siirrettävyys ei

---

<sup>224</sup> Knuutila ym. 2017, s. 48.

<sup>225</sup> Sekä Valtioneuvoston että Liikenne- ja viestintäministeriön selvityksissä koskien Mydataa on korostettu yksilön ja vastaanottavan rekisterinpitäjän välistä suhdetta. Tässä suhteessa alkuperäisen rekisterinpitäjän vastuu jäisi nykyistä rekisterinpitäjän vastuuta huomattavasti kevyemmäksi.

<sup>226</sup> WP29 242 rev.01, s.6.

automaattisesti poista siirrettäviä henkilötietoja alkuperäisen rekisterinpitäjän järjestelmistä, vaan siirrettäviin tietoihin sovelletaan alkuperäistä säilytysaikaa.<sup>227</sup> Siirrettävät henkilötiedot sijaitsevat siirron jälkeen useammassa eri rekisterissä, ellei rekisteröity pyytä tietojen poistamista.

Siirto-oikeuden nojalla saatu henkilötieto siirtää vastuun uudelle rekisterinpitäjälle tietojen käsittelyn osalta. Tietoja luovuttanut rekisterinpitäjä ei ole enää vastuussa siitä, mihin tarkoitukseen vastaanottava taho tietoja käyttää, vaan vastuu on tiedot saaneella organisaatiolla.<sup>228</sup> Uusi rekisterinpitäjä ei voi käyttää saatua tietoa omaan tarkoitukseensa esimerkiksi markkinoidakseen palvelujaan kolmansille osapuolille. Mikäli siirretyt tiedot ovat sisältäneet kolmannen osapuolen henkilötietoja, näitä tietoja ei pitäisi käyttää rikastuttamaan kolmannen osapuolen profiilia, tai muokkaamaan hänen sosiaalista ympäristöään ilman hänen tietämystään ja suostumustaan, vaikka rekisterinpitäjällä olisikin jo valmiiksi ollut tietoja hänestä. Rekisterinpitäjän tulisi säilyttää henkilötiedoista vain ne tiedot, jotka ovat oleellisia kyseessä olevan palvelun kannalta. Tiedot vastaanottanut organisaatio tulee siis uudeksi rekisterinpitäjäksi siirrettyjen henkilötietojen osalta, ja sen on noudatettava tietosuoja-asetuksen 5 artiklan henkilötiedon käsittelyperusteita.<sup>229</sup>

Tietoturvallisuus on otettava huomioon tietojen siirrossa. Yleisesti ottaen rekisterinpitäjän olisi taattava ”henkilötietojen asianmukainen turvallisuus, mukaan lukien suojele luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta käyttäen asianmukaisia teknisiä tai organisatorisia toimia” tietosuoja-asetuksen 5 artiklan 1 kohdan f alakohdan mukaisesti. Koska tietojen siirrettävyys pyrkii saamaan henkilökohtaisia tietoja järjestelmästä, siirto voi olla mahdollinen riski kyseisille henkilötiedoille. Rekisterinpitäjä vastaa kaikista tarvittavista turvatoimista, joilla varmistetaan henkilötietojen siirto turvallisesti oikeaan määränpäähän.<sup>230</sup> Tietosuoja-asetus ei aseta erityisiä suosituksia toimitettavien henkilötietojen muodolle. Sopivin muoto vaihtelee organisaatiokohtaisesti, eikä

---

<sup>227</sup> Tietosuoja-asetuksen 5 artikla säätelee henkilötietojen käsittelyä koskevia periaatteita. Artiklassa on lueteltu vaatimukset, joita rekisterinpitäjän tulee noudattaa, ja lisäksi rekisterinpitäjälle on artiklan 2. kohdan mukaisesti säädetty osoitusvelvollisuus, jonka mukaan rekisterinpitäjä pystyy osoittamaan, että 1 kohtaa on noudatettu (=osoitusvelvollisuus).

<sup>228</sup> Myös Big Dataa koskevissa vastuukysymyksissä vastuu datasta olisi tarkoituksenmukaista kohdentaa sille taholle, joka tiedoista hyötyy. Lisäksi uudella rekisterinpitäjällä on tieto siitä, mihin tietoa on tarkoitus käyttää ja millä perusteella, ks. Mayer – Schönberger & Cukier 2013, s. 173-174, Big Datasta ks. 1 luku.

<sup>229</sup> WP 242 rev.01, s. 6-7, 11-12.

<sup>230</sup> WP 242 rev.01, s. 18-20.

rekisterinpitäjällä ole velvollisuutta hyväksyä tai ylläpitää tietojenkäsittelyjärjestelmiä, jotka ovat teknisesti yhteensopivia.<sup>231</sup> Mikäli siirto tehdään, tulee siirrossa käytetty muoto olla tietoturvallinen.

Rekisteröidyn tiedollinen itsemääräämisoikeus on tietojen luovuttamisen kohdalla suhteellisen vahva. Tietoja luovuttava rekisterinpitäjä toimii tällöin rekisteröidyn lukuun, eikä ota vastuuta siirrettävistä tiedoista. Tästä uudesta rekisteröidyn oikeudesta voi siten myös muodostua riski rekisteröidylle, jos rekisteröity ei ole tarkistanut riittävässä määrin luovutettavia tietoja. Uusi mahdollisuus rekisteröidylle tuo siten myös uusia velvoitteita tai vähintäänkin uutta vastuuta. Mikäli 20 artiklan mukaisia periaatteita sovelletaan omadatan mukaiseen suostumusperusteiseen henkilötietojen hallintaan, luovuttavan rekisterinpitäjän vastuu on vähäinen. Luovuttava rekisterinpitäjä huolehtii siitä, että suostumus kyseessä olevien tietojen osalta on olemassa ja että se luovuttaa ne henkilötiedot, jotka rekisteröity haluaa. Lisäksi sen tulee varmistua tietojen tietoturvallisesta luovutuksesta. Tämän jälkeen alkuperäisen rekisterinpitäjän vastuu päättyy, eikä se ota kantaa siihen, mihin käyttötarkoitukseen vastaanottava taho tietoja käyttää, käsitelläänkö tietoja tietosuoja-asetuksen mukaisesti tai ovatko tiedot asianmukaisesti suojattuja.

Tiedot vastaanottavan rekisterinpitäjän tulee huolehtia siitä, että se ei käsittele enempää tietoja kuin on tarpeellista. Rekisterinpitäjä ei voi tietosuoja-asetuksen minimivaatimusta noudattaen pyytää yksilön suostumusta sellaisiin henkilötietoihin, joita se ei tarvitsisi toiminnassaan. Rekisterinpitäjän on myös käsiteltävä henkilötietoja tietosuoja-asetuksen 5 artiklan mukaisesti. Sen tulee suojata tiedot asianmukaisesti sekä varmistua käsittelyn asianmukaisuudesta. Yksilön antama suostumus koskee vain nimenomaista käyttötarkoitusta, johon tiedot ovat pyydetty. Mikäli tietojen käyttötarkoitus muuttuu, suostumus tulee pyytää uudelleen. Rekisterinpitäjä ei voi käsitellä suostumuksen perusteella henkilötietoja unohtamatta alkuperäistä käsittelytarvetta.<sup>232</sup>

Liikenne- ja viestintäministeriön selvityksessä tuodaan esille ajatus, jossa rekisteröidyn henkilön ei tarvitsisi luovuttaa tietojaan laissa tarkoitettulla tavalla, vaan palveluntarjoajalle voitaisiin yksilön luvalla antaa pääsy käyttämään dataa. Kirjoittajien mukaan tällöin rekisteröity toimisi itse näiden tietojensa suhteen rekisterinpitäjänä ja olisi vastuussa omasta

---

<sup>231</sup> Tietosuoja-asetus, 68 johtolause.

<sup>232</sup> WP 259 s. 9.

datastaan. Tämä voisi kirjoittajien mukaan ”avata innovaatiolukkoja monilla alueilla”.<sup>233</sup> Juridisten vastuukysymysten osalta ehdotettu malli olisi ongelmallinen. Nykyinen lainsäädäntö ei tunnista tilannetta, jossa yksilö itse on rekisterinpitäjänä omien tietojen osalta ja palveluntarjoaja voisi yksilön antaman luvan nojalla saada pääsyn tietoihin. Toisaalta taas tietosuoja-asetuksen 4 artiklan määritelmässä sanalla ”rekisterinpitäjä” tarkoitetaan myös luonnollista henkilöä, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Tulisiko tällöin yksilön itsensä rekisterinpitäjänä noudattaa tietosuoja-asetuksen mukaisia henkilötiedon käsittelylle asetettuja vaatimuksia, kun kyse olisi pelkästään hänen tiedoistaan? Vai voisiko yksilö omalla toiminnallaan laiminlyödä tietosuojaaja, sillä kyse olisi vain häneen itseensä liittyvistä mahdollisista tietosuojaloukkauksista, eikä kolmas osapuoli kärsisi vahinkoa? Voidaan myös perustellusti epäillä sitä, mikä tosiasiallinen mahdollisuus ihmisillä on ryhtyä omien tietojensa rekisterinpitäjäksi ja sääntelijäksi. Tämä malli olisi kenties seuraava askel suostumushallintarekisteristä, mutta ei mielestäni ensisijainen keino lähteä toteuttamaan omien tietojen hallintaa.

Nykyinen lainsäädäntö ei mahdollista selvityksissä kuvattua yksilöiden hallinnoimia käyttölupia liittyen viranomaisten hallussa olevaan henkilötietoon siten, että tavoiteltu tiedonhallinta toteutuisi, pois lukien yksilön itsensä viranomaiselle toimittama henkilötieto. Aikaisemmin luvussa 5.2 on käsitelty sitä, mikä vastuu on viranomaisella sen luovuttaessa henkilötietoja rekisteristään. Tällöin artiklan 20 mukaista henkilötietojen luovutusta ei sellaisenaan voida soveltaa viranomaisen henkilötietojen luovuttamiseen. Yksilö ei tällä hetkellä ole aktiivinen henkilötietojensa suhteen siten, että hän voisi viranomaiselle ilmoittaa mihin hänen tietojaan tulisi siirtää. Vaikka julkisuuslaissa sekä tietosuoja-asetuksessa säädetään suostumuksen olevan yksi henkilötiedon käsittelyperusteista, ei se vielä velvoita viranomaista siirtämään tietoja suoraan toiselle rekisterinpitäjälle. Yleisesti on ajateltu rekisteröidyn olevan alisteisessa asemassa rekisterinpitäjään nähden, etenkin, kun kyseessä on vastapuolena viranomainen. Tästä johtuen sopimussuhde yksilön ja rekisterinpitäjän välillä siten, että yksilöllä on vastuu huolehtia tietyistä tiedon luovuttamiseen liittyvistä toimista, on hyvin poikkeuksellinen. Liikenne- ja viestintäministeriön MyData-selvityksen mukaan teknisesti ja oikeudellisesti yksilön antama suostumus vastaisi lupaa.<sup>234</sup> Yksilöllä ei ole samanlaisia keinoja valvoa rekisterinpitäjää kuin esimerkiksi viranomaisilla. Niin sanotun käyttöluvan myöntäminen omiin henkilötietoihinsa vaatisi yleistä käyttölupapohjaa,

---

<sup>233</sup> Poikola ym. 2014, s. 68.

<sup>234</sup> Poikola ym. 2015, s. 7.

sillä ei voida olettaa jokaisen yksilön tiedostavan sitä, mitä mahdollisessa luvassa tulisi ottaa huomioon. Yksityishenkilöllä ei myöskään ole kaupallisiin toimijoihin verrattuna samanlaista ymmärrystä omien tietojen uudelleenkäytön arvosta.<sup>235</sup>

Edellä mainittu rekisterinpitäjän valvominen henkilötiedon käsittelyn suhteen mahdollistetaan lokituksen avulla. Lokitieto tarkoittaa tietojärjestelmän henkilötiedon käsittelystä kerättävää käyttäjäkohtaista merkintää, eli sitä, mihin tarkoitukseen henkilötietoja on käsitelty ja kuka niitä on käsitellyt.<sup>236</sup> Suostumushallintarekisterin osalta lokitus on tärkeässä asemassa, jotta mahdolliset väärinkäytöstilanteet voidaan jäljittää ja saada vastuussa oleva organisaatio tai henkilötiedon käsitelijä selvitettyä. Rekisterinpitäjän on käsiteltävä henkilötietoja tavalla, jolla varmistetaan tietojen asianmukainen turvallisuus käyttäen asianmukaisia teknisiä ja organisatorisia toimia. Organisatorisilla suojauskeinoilla tarkoitetaan käyttäjille annetut ohjeet ja määräykset henkilötietojen käsittelystä. Tekniset keinot liittyvät yksilön tunnistamiseen ja yksilöintiin, käyttöoikeuksien määrittelyyn sekä tietojen jälkikäteiseen selvittämiseen lokitietojen avulla.

Mikäli yksilö voisi päättää henkilötiedoistaan, tulisi lain tasolla säätää omadataoikeuksista. Hallituskauden tavoite on digitalisoida julkiset palvelut. Sen yhteydessä rakennetaan julkiset palvelut käyttäjälähtöisiksi ja samalla vahvistetaan kansalaisten oikeutta valvoa ja päättää itseään koskevien tietojen käytöstä.<sup>237</sup> Tämän hetkinen hallitus on sitoutunut vahvistamaan kansalaisten oikeuksia omiin henkilötietoihinsa. On siis nähtävissä suuntausta, jonka mukaan myös omadatan tavoitteet voisivat jossain määrin toteutua.

---

<sup>235</sup> Heinonen 2001, s. 35.

<sup>236</sup> Tietosuojavaltuutetun toimiston ohje, 12.11.2012, s. 2-3.

<sup>237</sup> Hallituksen julkaisusarja 10/2015, s. 26.

## 6 LOPUKSI

Yleinen tietosuoja-asetus vahvistaa tiedollista itsemääräämisoikeutta ja sen toteutumista. Myös hallinnollisten sakkojen mahdollistaminen asetuksen nojalla antaa signaalin siitä, että tietosuoja on tärkeä osa rekisterinpitäjän velvollisuuksia. Rekisterinpitäjälle on asetuksen nojalla lisätty velvollisuuksia muun muassa osoitusvelvollisuuden muodossa. Rekisterinpitäjän tulee voida osoittaa tarvittaessa sekä tarkastusviranomaiselle että rekisteröidylle se, miten tietosuoja on rekisterinpitäjän toimesta toteutettu. Tiedollisen itsemääräämisoikeuden vahvistumisen myötä omadatan mukainen ajattelumalli on luonnollinen jatkumo henkilötietojen käsittelyn kehittyessä. Yksilöllä on oikeus hallita omia tietojaan ja saada rekisterinpitäjältä tietoa hänestä kerätyistä henkilötiedoista. Suostumus osana käsittelyperustetta mahdollistaa yksilölle mahdollisuuden määrätä siitä, kuka hänen henkilötietojaan käsittelee. Toteutuessaan täysimääräisesti omadatan voidaankin ajatella olevan seuraava askel tiedollisesta itsemääräämisoikeudesta. Tällöin omadataan sisältyy kaikki tiedollisen itsemääräämisoikeuden elementit.

Julkisen hallinnon kehittäessä uusia digitaalisia palveluita on myös viranomaisen osalta tullut ajankohtaiseksi tarkastella yksilön oikeuksia omiin tietoihinsa. Vaikka viranomaisen lähtökohtaisesti luovuttaa henkilötietoja julkisuuslain sekä mahdollisen erityislainsäädännön nojalla, ei omadataan pohjautuvaa henkilötiedon hallintaa tarvitse rajata viranomaisen käsittelemän tiedon piiristä kokonaan pois. Omadatan soveltuminen julkiseen hallintoon vaatii lailla säätämistä sen osalta, mitä henkilötietoja viranomaisen voisi luovuttaa rekisteröidyn antaman suostumuksen perusteella. Viranomaisella on yleisesti korostettu velvollisuus tietyissä tilanteissa tarkistaa se, mihin tarkoitukseen luovutettavia henkilötietoja tullaan käsittelemään ja kuinka tietojen suojaus on järjestetty. Omadata-mallin mukaisesti tällainen viranomaisen tekemä tarkistus ei palvelisi sitä ajatusta, että rekisteröidyn antama yksiselitteinen suostumus olisi riittävä peruste tietojen luovuttamiselle. Mikäli tietojen luovutuksen yhteydessä viranomaisen pyytäisi selvitystä henkilötiedon käyttötarkoitukseen liittyen, ei omadatan mukainen tiedon luovutus toteutuisi.

Julkisuuslaki säätelee yleislakina henkilötietojen luovutusta viranomaisen rekisteristä. Mikäli asiaa koskien ei ole erikseen säädettyä erityislainsäädäntöä, sovelletaan julkisuuslain säädöksiä. Julkisuuslaki asettaa viranomaiselle suhteellisen korkean velvollisuuden huolehtia siitä, kenelle henkilötiedot luovutetaan ja millä perusteella. Mikäli omadatan



mukainen malli halutaan sisällyttää poikkihallinnollisesti koko julkiseen hallintoon, ei julkisuuslaki yleislakina sitä tällä hetkellä täysimääräisesti mahdollista. Vaihtoehtona on säätää kunkin viraston omassa lainsäädännössä henkilötietojen luovutuksesta suostumuksen perusteella. Näin on käytännössä jo tehtykin esimerkiksi Koski-rekisterin kohdalla, jota koskevassa lainsäädännössä säädetään erikseen tietojen luovutuksesta suostumuksen perusteella. Riskinä omadataan perustuvalla erityislainsäädännöllä on se, että henkilötietojen käsittelyn sääntely hajautuu useaan erityislainsäädäntöön. Jo nykyisessä lainsäädännössä henkilötietojen käsittelystä säädetään yli 800:ssa eri laissa, jonka vuoksi tarkempi selvitys erityislainsäädännön sisällöstä ei ollut esimerkiksi tämän tutkielman yhteydessä mahdollista.<sup>238</sup> Uudella, valmisteilla olevalla tiedonhallintalainsäädännöllä pyritään yhtenäistämään viranomaisten tietojen hallintaa siten, että henkilötietojen käsittelystä säätämiseen erityislainsäädännössä ei olisi aina tarvetta. Tavoitteena on purkaa turhaa sääntelyä, ei lisätä sitä. Tämän vuoksi lailla tulisi säätää niistä viranomaisen rekisterissä olevista tiedoista, jotka voidaan luokitella yksilön omadataksi. Näiden tietojen osalta viranomainen voisi luovuttaa henkilötiedot jo pelkästään yksilön antaman suostumuksen perusteella, eikä viranomaisella olisi vastuuta henkilötiedon vastaanottavan rekisterinpitäjän suorittamasta henkilötietojen käsittelystä. Myös rajapintojen avaamisesta on säädettävä erikseen ei vain viranomaisten, vaan myös viranomaisten ja yksityisten toimijoiden välillä.

Viranomaisten rekistereissä olevat henkilötiedot ovat yksilön kannalta hyvin tärkeitä tietoja, joten rekisterinpitäjän vastuu ja tiedon suojaus tulee olla varmistettu. Mikäli uuden mallin mukaisesti viranomainen luovuttaisi henkilötietoja tarkistamatta tiedon käyttötarkoitusta tai tietojen suojausta, tulisi vastaanottava rekisterinpitäjä sitouttaa esimerkiksi käyttö lupaan. Käyttölupaan sitoutuminen olisi ehtona sille, että henkilötietoja voitaisiin rekisteröidyn antaman suostumuksen perusteella käsitellä. Tällöin käyttöluvassa tulisi esimerkiksi määritellä vakioehdot tietojen käytölle sekä tietoturvallisuudelle. Yksilön asema suhteessa rekisterinpitäjään on alisteisessa asemassa myös jatkossa, joten omadata-malliin tulisi kehittää säännöt sen osalta, miten tietoja voidaan käsitellä ja kerätä. Tämä ei vähentäisi yksilön tiedollista itsemääräämisoikeutta, vaan sillä turvattaisiin se, että omadata-malli ei kääntyisi itseään vastaan sen osalta, että tietosuoja ei toteutuisi puutteellisten käytäntöjen myötä. Yritykset kokevat usein julkishallinnon tietojen luovutukset kankeaksi prosessiksi, joka taas voi jopa hidastaa kansantalouden kehittymistä.<sup>239</sup> Mikäli

---

<sup>238</sup> Oikeusministeriön julkaisu 35/2017, s. 21.

<sup>239</sup> Ks. Kiuru ym. 2012, s. 5-6. Tutkimuksen tarkoituksena oli selvittää avoimen julkisen tiedon hyödyntämisen potentiaalia suomalaisissa yrityksissä. Yritysten mukaan julkisen tiedon saatavuus on monimutkaista ja tiedon

julkishallinnon tietojenluovutuksen rinnalle tulisi yksilöiden hallinnoimat käyttöluvat, voisi se pidemmällä aikavälillä luoda uusia innovaatioita ja edesauttaa myös yksilön omien henkilötietojen tehokasta hyödyntämistä.

Omadata-malli toteutuessaan voisi mahdollistaa tulevaisuudessa uusia palveluita, siirtäisi valtaa takaisin yksilölle itselleen ja pakottaisi organisaatiot toimimaan enemmän käyttäjälähtöisesti. Nykymuotoinen henkilötietojen hallinta, jossa henkilötietoja liikkuu yritysten välillä ilman että yksilöllä itsellään on mitään näkyvyyttä tai kontrollia omiin tietoihinsa, ei ole kestävä. Henkilötietojen arvo kasvaa mitä enemmän dataa ladataan internettiin. Tietoja voidaan yhdistellä eri käyttötarkoituksiin ja hyödyntää edelleen, mikä taas voi aiheuttaa henkilötietojen hyödyntämisen laitonta käsittelyä. Tämä altistaa yksilöiden tietosuojan vaaraan, mikäli henkilötietojen hyödyntämisestä yritysten toimesta ei ole mitään tietoa. Yksilöt eivät nykyäänkään tiedosta maksavansa usein ilmaisista palveluista, kuten esimerkiksi Facebookin käytöstä omalla datallaan. Henkilötietoja hyödyntävät palvelut verhotaan usein ilmaisen käytön suojaan, mutta todellisuudessa yksilön luovuttama tieto on yritykselle erittäin arvokasta. Henkilötietoa voidaan myydä edelleen suurella voitolla.<sup>240</sup>

Omadata on myös herättänyt perusteltua huolta siitä, miten tietosuoja toteutuisi, mikäli rekisteröity olisi itse henkilötietojensa käsittelyn oikeuttajana. On huomioitava yksilöiden erilaiset tarpeet sekä valmiudet suostumuksensa perusteella luvittaa omien henkilötietojensa käyttöä. Kaikilla ei tähän ole mahdollisuutta erilaisista rajoitteista johtuen, joten omadatan mukainen malli tulisi olla mahdollisuus yksilölle, mutta sen ei tulisi asettaa ihmisiä eriarvoiseen asemaan sen perusteella, onko yksilöllä valmiuksia omien henkilötietojen hallintaan.<sup>241</sup> Rekisterinpitäjän ei myöskään tulisi edellyttää suostumusta sellaisten henkilötietojen käsittelyyn, jotka eivät olisi tarpeellisia kyseessä olevan palvelun kannalta. Lainsäädännön sanotaan usein olevan esteenä digitalisaatiolle, ja näin varmasti onkin useassa tapauksessa. On kuitenkin huomioitava lainsäädännön olevan ensisijainen keino yksilöiden henkilötietojen suojaamisessa, ja tietosuoja tarvitaankin entistä enemmän henkilötietojen asianmukaisen käsittelyn varmistamiseksi. Nykyinen lainsäädäntö vaatii

---

luovutusperiaatteet hidastavat innovatiivisuutta. Useat yritykset olivat sitä mieltä, että lisääntynyt innovaatiotoiminta edesauttaisi myös asiakkaille kehitettäviä lisäarvopalveluita. Myös eurooppalaisen datatalouden kasvun yksi suurimmista esteistä on hajallaan oleva data. Datan saatavuus on avaintekijä innovaation ja kasvun lisäämiseksi, European Commission 2017.

<sup>240</sup> Kauppalehti 2018.

<sup>241</sup> Yle Uutisten mukaan vuonna 2018 jopa miljoona suomalaista seuraavat digitalisaation kehittymistä sivusta, eivätkä ole kykeneväisiä käyttämään kehittyviä digitaalisia palveluita. Mikäli kaikki palvelut siirtyvät sähköisiin palveluihin, vaarantaa se jo perusoikeuksien toteutumista, Yle Uutiset 2018.

muutoksia, mutta muutoksia tehtäessä on otettava huomioon henkilötietojen käsittelyn kannalta olennaisin tekijä – yksilön oikeudet.