UNIVERSITY OF LAPLAND
LAPIN YLIOPISTO

Itsehallittavan identiteetin sääntely EU:n yleisessä tietosuoja-asetuksessa

Lapin yliopisto
Oikeustieteiden tiedekunta
Notaaritutkielma
Uusi tutkintorakenne
Oikeusinformatiikka
Jyrki Pitkänen
Kevät 2018

Sisältö

Lähteet

Kirjallisuus

Aarnio, Aulis: Oikeussäännösten systematisointi ja tulkinta. Teoksessa: Juha Häyhä (toim.): Minun Metodini. 1997. s. 35–56

Abraham, Andreas: Self-Sovereign Identity – Whitepaper about the Concept of Self-Sovereign Identity including its Potential. Itävalta 2017

Crosby, Michael – Nachiappan, Pradhan Pattanayak ym.: BlockChain Technology Beyond Bitcoin. Berkeley 2015

Kugler, Tobias – Rücker, Daniel: New European General Data Protection Regulation – A Practitioner's Guide. 2018

Nurmi, Erkka: Lohkoketjuteknologian hyödyntäminen terveysalalla. Jyväskylä 2017

Poikola, Antti – Kuikkaniemi, Kai – Kuittinen, Ossi: My Data – johdatus ihmiskeskeiseen henkilötiedon hyödyntämiseen. 2014

Reed, Drummond – Law, Jason – Hardman, Daniel: The Technical Foundations of Sovrin. 29.10.2016

Sovrin Foundation: Sovrin™: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust. Tammikuu 2018

Tobin, Andrew – Reed Drummond: The Inevitable Rise of Self-Sovereign Identity. 2016

Warren, Samuel D. – Brandeis, Louis D.: The Right to Privacy. Harvard Law. 1890

Windley, Phillip J: How Sovrin Works. 2016.

Zanol, Jakob – Czadilek, Alexander – Lebloch Kaspar: Self-Sovereign Identity und Blockchain. Teoksessa: *Schweighofer, Erich – Kummer, Franz – Saarenpää, Ahti – Schafer, Burkhard*: Datenschutz / LegalTech 2018, s. 235-242

Virallislähteet ja oikeuskäytäntö

29 artiklan mukainen tietosuojatyöryhmä: Guidelines on consent under Regulation 2016/679. WP259

29 artiklan mukainen tietosuojatyöryhmä: Guidelines on Personal data breach notification under Regulation 2016/679. WP250

29 artiklan mukainen tietosuojatyöryhmä: Guidelines on the right to data portability. WP242

29 artiklan mukainen tietosuojatyöryhmä: Guidelines on transparency under Regulation 2016/679. WP260

California Civil Code §1798, An act to amend Sections 1798.29 and 1798.82 of the Civil Code, relating to personal information.

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 (EU:n yleinen tietosuoja-asetus)

Verkkolähteet

Reed, Drummond – Law, Jason – Hardman, Daniel – Lodder, Mike: DKMS (Decentralized Key Management System) Design and Architecture V3. 2018. Saatavuus: https://github.com/hyperledger/indy-sdk/blob/master/doc/dkms/DKMS%20Design%20and%20Architecture%20V3.md Noudettu 19.4.2018

Statista: Most famous social network sites worldwide as of September 2017, ranked by number of active users (in millions). 2017. Saatavuus: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ Noudettu: 29.3.2018

The Outline: How hackable is bitcoin? 2017 Saatavuus: https://theoutline.com/post/1618/how-hackable-is-bitcoin?zd=1&zi=jtnzottn Noudettu: 24.4.2018

Käsitteet

Hajautettu tunniste	Yksilöllinen pseudonymisoitu tunniste, jonka avulla identiteetin omistaja voi tunnistautua ja joka voidaan liittää *väitteisiin* sekä *julkituonteihin*, mutta jota rekisterinpitäjä tai ulkopuolinen ei voi yksipuolisesti yhdistää luonnolliseen henkilöön. (engl. decentralised identifier)
Identiteetin omistaja, rekisteröity	Luonnollinen henkilö, jota henkilötiedot koskevat ja joka käyttää itsehallittavaa identiteettiä. Kun identiteetin omistaja antaa jollekin rekisterinpitäjälle pääsyn henkilötietoihinsa, tulee hänestä tietosuoja-asetuksessa tarkoitettu *rekisteröity*. (engl. identity owner)
Tunniste	Identiteetin omistajan rekisterinpitäjälle jakama, *väitteisiin* yhdistetty tieto, jonka avulla rekisterinpitäjä tunnistaa rekisteröidyn. (engl. identifier)
Väite	Identiteetin omistajan jakama, tätä koskeva standardimuodossa kerrottu tieto. Oikeellisuus on todennettavissa väitteen myöntäneen tahon sähköisestä allekirjoituksesta (*varmennettava väite*). (engl. verifiable claim, claim)
Julkituonti	Väitteitä yhdistelemällä tai väitettä rajaamalla muodostettu henkilötieto, josta löytyy ainoastaan tapahtuman kannalta tarpeelliset tiedot. (engl. disclosure)

1 Johdanto

Yksityisyyden suoja on Euroopan ihmisoikeussopimuksen sekä EU:n perusoikeuskirjan mukainen perusoikeus, ja sitä on tutkittu oikeudellisesta näkökulmasta 1800-luvulta lähtien.[1] Verkkoyhteiskunnassa yksi yksityisyyden kulmakivistä on henkilötietojen tietoturvallinen käsittely. Internet on mullistanut henkilötietokantojen laajuuden ja henkilötietoja kerätään yritysten rekistereihin ennennäkemätön määrä. Pelkästään Facebookilla on yli 2 miljardia aktiivista käyttäjää[2] ja palvelun luonteesta johtuen kyseessä on laajoja henkilötietoja sisältävä keskitetty tietokanta. Tämä muodostaa merkittävän tietoturvariskin, kun pahimmillaan tietoturvaloukkaus voi vaarantaa yli neljänneksen maailman väestöstä henkilötietojen suojan merkittävälle heikentymiselle.

Viimeaikaisia teknologian kehitysaskeleita on ollut hajautettujen tietokantojen kehitystyö. Tunnetuin esimerkki lienee lohkoketjuteknologialla toteutettu virtuaalivaluutta Bitcoin, jota ei lähes kymmenvuotisen olemassaolonsa aikana ole kertaakaan onnistuttu hakkeroimaan.[3] Lohkoketjuteknologialla voidaan toteuttaa virtuaalivaluuttojen lisäksi myös muunlaisia tietokantoja. Yksi tällainen on My Data -periaatteita[4] noudattava, lohkoketjuteknologialla toteutettu sähköisen identiteetin järjestelmä, eli itsehallittava identiteetti.

Myös Euroopan unionissa on herätty muuttuvaan maailmaan. Henkilötietojen suojaa tulee parantaa, ja tämän vuoksi huhtikuussa 2016 säädettiin Euroopan unionin yleinen tietosuoja-asetus (2016/679). Asetuksen tarkoituksena on yhdenmukaistaa henkilötietojen käsittelyä jäsenvaltioissa ja varmistaa henkilötietojen vapaa liikkuvuus.[5] Tietosuoja-asetuksessa painotetaan digitalouden kehittymistä tietosuojan rinnalla; ilman joustavia, mutta henkilötietojen suojaa tukevia tulkintoja jotkin teknologian kehitysaskeleet voivat jäädä marginaaliseen rooliin Euroopan Unionissa.[6] Tällaisen tulkinnan puute voisi haitata sekä EU:ssa toimivien yritysten kilpailukykyä että henkilötietojen suojaa unionissa. Tietosuoja-asetuksen tavoitteena on jäsenmaiden tietosuojasääntelyn yhtenäistäminen, joten unionin laajuinen tulkinta on yhteismarkkina-alueen sääntelyn kannalta tarkoituksenmukaisinta. Asetuksen soveltaminen alkaa 25. toukokuuta 2018.

[1] Warren, Brandeis 1890.
[2] Statista: Most famous social network sites worldwide as of September 2017. 2017.
[3] The Outline: How hackable is Bitcoin? 2017.
[4] My Data -periaatteet ovat 1. yksilöiden oikeus ja mahdollisuus hallita omaa dataansa, 2. henkilötiedon kattava ja käytännöllinen saatavuus sekä 3. henkilötiedon hallinnan hajauttaminen ja yhteentoimivuus. (Poikola, Kuikkaniemi, Kuittinen 2014 s. 19) Tarkemmin My Datasta ks. Poikola, Kuikkaniemi, Kuittinen 2014.
[5] EU:n tietosuoja-asetus, resitaali 3.
[6] EU:n tietosuoja-asetus, resitaalit 6 & 7.

Tutkimuksen kohteena on itsehallittavan identiteetin yhteensopivuus EU:n yleisen tietosuoja-asetuksen kanssa. Henkilötietojen käsittelyn ollessa tarkasti säädeltyä ja itsehallittavan identiteetin poiketessa aiemmin totutusta on mahdollista, että sääntely ei kaikilta osin kohtele keskitettyä ja hajautettua henkilörekisteriä yhdenmukaisesti. Vaikka asetuksen soveltaminen ei kirjoitushetkellä ole vielä alkanut eikä oikeuskäytäntöä ole, kyseessä on oikeusdogmaattinen tutkimus. Tämä siksi, että lainsäädäntöehdotusten antaminen ei olisi mielekästä, sillä asetuksen teksti on ollut valmis jo toista vuotta. *De lege ferenda* -tutkimus ei siis olisi mielekäs tapa lähestyä kehitysvaiheessa olevan teknologian tarkastelua lainsäädännön näkökulmasta, koska tuolloin tutkielmasta puuttuisi täysin konkreettinen soveltamisala. Oikeusdogmaattisen metodin käytön perusteena onkin käytännönläheisyys.

Oikeuskäytännön puuttuessa täysin tutkielmassa on huomattava määrä omaa tulkintaa. Olen näissä tulkinnoissa pyrkinyt soveltamaan Aulis Aarnion muotoilemaa argumentaation regulatiivista periaatetta, jonka mukaan kannanotot tulee perustella oikeusyhteisön rationaalista hyväksyttävyyttä ajatellen.[7] Tutkielma on siis laadittu lähtökohtaisesti lainoppineita lukijoita varten esittelemään itsehallittavan identiteetin tietosuoja-asetuksen näkökulmasta. Toisaalta myös itsehallittavaa identiteettiä teknologiana tutkivat tahot saavat tutkielman avulla konkreettisen lähestymistavan tietosuoja-asetuksen soveltamiseen. EU:n tietosuoja-asetuksen oikeussääntöjen systematisointi ja tulkinta itsehallittavan identiteetin näkökulmasta on siis mielekästä sekä oikeustieteelliseltä että teknologiselta kannalta. Lähteinä on käytetty asetuksen tekstiä, tulkintoja ja esitöitä sekä selontekoja ja tieteellisiä tutkimuksia itsehallittavasta identiteetistä.

Tutkielmatekstin selkeyden vuoksi käytän ainoastaan suomenkielisiä termejä. Koska tutkielman aihe keskittyy kehitysasteella olevaan teknologiaan, iso osa termeistä on vailla suomenkielistä vastinetta. Näissä tilanteissa olen käyttänyt käännöstä, joka on suorin järkevä käännös englanninkielisestä termistä. Esimerkiksi *decentralised identifier* kääntyy muotoon *hajautettu tunniste*.

Itsehallittavan identiteetin kehittäjiä on useita, joista osa on jo lopettanut kehittämisensä saavuttamatta lopullista käytettävää tuotetta.[8] Useiden eri kehittäjien vuoksi olen rajannut tutkielman käsittelemään Sovrin Foundationin kehittämän itsehallittavan identiteetin palvelua sen ollessa selkeästi laajamittaisin projekti isolla tuella.[9] Tämä voi johtaa eri kehittäjien itsehallittavien identiteettien erojen osalta erilaisiin säännöstulkintoihin joissakin kohdissa, mutta perusperiaate itsehallittavan identiteetin osalta pysyy joka tapauksessa samana. Tietosuoja-asetuksesta käsittelyn ulkopuolelle olen

[7] Aarnio 1997 s. 51
[8] Abraham 2017 s.14.
[9] Sovrinin yhteistyökumppaneita ovat mm. IBM, T-Labs ja Tykn. Lisätietoja ks. www.sovrin.org/stewards/.

rajannut artiklat ja kohdat, jotka eivät selvästi ja olennaisesti liity itsehallittavan identiteetin soveltamisen käsittelyyn.[10]

Tutkielman luvussa 2 kuvataan lyhyesti itsehallittavan identiteetin toimintaperiaate (2.1), sen soveltamisen välttämättömät edellytykset tietosuoja-asetuksessa (2.2) sekä asetuksen tärkeimmät määritelmät itsehallittavan identiteetin kannalta (2.3). Luvussa 3 käsitellään itsehallittavan identiteetin ja tietosuoja-asetuksen keskenään yhteensopivat kohdat ja luvussa 4 ristiriitaiset. Tutkielma päättyy johtopäätöksiin (5).

2 Itsehallittava identiteetti

2.1 Määritelmä

Itsehallittavan identiteetin mallissa luonnollinen henkilö omistaa ja hallinnoi itse omia henkilötietojaan. Käyttäjällä on omien tietojensa osalta suurempi vapaus ja vastuu perinteiseen henkilörekisteriin verrattuna.[11] Koska henkilötiedot on talletettu jokaiselle käyttäjälle itselleen, eli niitä säilytetään hajautetusti, yksittäistä vikaantumispistettä ei ole, toisin kuin keskitetyissä tietokannoissa.[12]

Itsehallitavassa identiteetissä käyttäjällä on tarkoituksena olla laaja, häntä itseään koskevia henkilötietoja sisältävä rekisteri, josta voidaan *julkituoda* tiettyjä seikkoja taikka esittää *väitteitä* tai *varmennettavia väitteitä* käyttäjän identiteetistä.[13] Henkilöä koskevat tiedot itsehallittavan identiteetin järjestelmään tulevat joko käyttäjältä itseltään tai joltakin luotettavalta kolmannelta taholta.[14] Tietojen luotettavuuden vuoksi käyttäjän itsensä lisäämät tiedot, eli *väitteet*, ovat yksinkertaisia, kuten vaikkapa osoite tai puhelinnumero.[15] Kolmansilta tahoilta tulevat varmenteet luovat pohjan

[10] Artiklojen rajaamisperusteet ovat seuraavat: Artiklassa 1 kuvaillaan vain tietosuoja-asetuksen tavoitteita. Artiklat 8-10 koskevat tiettyjen henkilön ominaisuuksiin liittyvien henkilötietojen käsittelyn rajoituksia, joten henkilörekisterin toteuttamistapa ei ole merkitsevä. Artiklassa 12 kuvataan organisatorisia toimenpiteitä. Artiklassa 14 kuvataan toimitettavia tietoja, kun tietoja ei saada rekisteröidyltä; itsehallittavassa identiteetissä tiedot saadaan aina rekisteröidyltä. Artiklan 19 mukainen ilmoitusvelvollisuuden käsittely ei saa merkitystä, sillä rekisterinpitäjällä ei ole mahdollisuutta tehdä artiklan mukaisia toimenpiteitä henkilötiedoille. Artikla 21 koskee vastustamisoikeutta etenkin suoramarkkinoinnin osalta, joten oikeuteen pääsy edellyttää itsehallittavan identiteetin järjestelmän ulkopuolista kommunikointia rekisterinpitäjän kanssa. Artiklat 29-31 koskevat rekisterinpitäjän ja henkilötietojen käsittelijän määrittelyn jakoa, joka ei ole merkitsevä itsehallittavan identiteetin soveltamisen kannalta. Artiklat 35-99 koskevat hallinnollisia, organisatorisia ja muita toimia, jotka eivät liity itsehallittavan identiteetin toteuttamiseen.
[11] Zanol, Czadilek, Lebloch 2018 s. 235.
[12] Nurmi 2017 s.3 Tiedot voidaan myös tallentaa käyttäen ns. Agentuuripalvelua, mutta tämä ei ole pakollista. Agentuuria on verrattu sähköpostilaatikon toteuttamisen: postilaatikon voi perustaa itse tai vaihtoehtoisesti käyttää jonkun palveluntarjoajan sähköpostilaatikkoa.
[13] Windley 2016 s. 2–6.
[14] Windley 2016 s. 4.
[15] Itsehallittavaa identiteettiä esittelevässä julkaisussa Windley 2016 esimerkkinä käytettyjen *väitteiden* sisältönä on nimi ja sukupuoli. Suomessa on kuitenkin olemassa keskushallinnon perusrekistereitä (esimerkiksi VRK:n

varmennetuille väitteille, joiden avulla henkilötiedon vastaanottaja voi olla varma merkittävän henkilötiedon totuudenmukaisuudesta. Tällaisia tietoja voisi Suomessa olla esimerkiksi Väestörekisterikeskuksen antama henkilötunnus, yliopiston antama todistus koulutuksesta tai Poliisin antama tieto ajo-oikeudesta. Näitä tietoja yhdistelemällä tai rajaamalla voidaan luoda kulloinkin tarpeellisia mutta rajattuja henkilötietoja, eli *julkituonteja*. Edellä mainituilla tiedoilla voidaan esittää muun muassa tieto täysi-ikäisyydestä ja sukupuolesta paljastamatta henkilötunnusta tai edes tarkkaa ikää.[16]

Luotettavuus itsehallittaviin henkilötietoihin on toteutettu lohkoketjuteknologialla. Henkilötietoja ei talleta lohkoketjuun, vaan lohkoketjun kautta varmennetaan lähetetty kryptografinen tunniste, jolla sen vastaanottaja voi varmistaa lähetetyn tiedon paikkansapitävyyden ja voimassaolon.[17] Tämä varmentaminen tapahtuu hajautetun julkisen avaimen menetelmällä.[18]

Itsehallittavassa identiteetissä käyttäjän – eli *identiteetin omistajan* – hallinnassa on siis häntä itseään koskevia henkilötietoja. Kun identiteetin omistaja haluaa aloittaa jonkin henkilötietoja vaativan palvelun käytön, kyseinen palveluntarjoaja pyytää identiteetin omistajalta palvelun käyttöön tarvittavat henkilötiedot. Käyttäjä näkee päätelaitteeltaan, mitä henkilötietoja rekisterinpitäjä pyytää. Hyväksymällä rekisterinpitäjän pyynnön identiteetin omistaja antaa tälle pääsyn kyseessä oleviin henkilötietoihin. Näin identiteetin omistajasta tulee rekisteröity ja palveluntarjoajasta rekisterinpitäjä.[19] Rekisterinpitäjän pääsy tietoihin – eli käsittelysuhde – päättyy joko ennalta sovitun määräajan päättyessä taikka rekisteröidyn päättäessä tietoihin pääsyn.

Itsehallittavan identiteetin avulla voidaan toteuttaa esimerkiksi työnhakutilanne, jossa työnhakija vastaa työpaikkailmoitukseen antaen itsestään laajat ja luotettavat tiedot, mutta kuitenkin niin, ettei kyseistä luonnollista henkilöä voida tunnistaa työnhakuprosessin aikana. Tällä metodilla työnantaja saa varmennettavasti tietää esimerkiksi työnhakijan koulutuksen ja luottotiedot saamatta selville työnhakijan sukupuolta, tarkkaa ikää, etnistä taustaa tai edes nimeä.[20]

Alla olevassa kaaviossa on kuvattu yksinkertaisesti tällainen kasvoton työnhaku. Kuvio on laadittu henkilötietojen käsittelysuhteen näkökulmasta, eikä siksi kuvaa muita tasoja, kuten salausavainten

---

Väestötietojärjestelmä), joista nämä molemmat tiedot voidaan johtaa *varmennettaviksi väitteiksi*. Tietojen varmuuden kannalta varmennettavia väitteitä tulisi nähdäkseni käyttää aina, kun sellainen voidaan johtaa luotettavalta taholta.

[16] Julkituonteja on käsitelty myös kohdassa 3.2. Tarkemmin, ks. Windley 2016 s. 5-6.

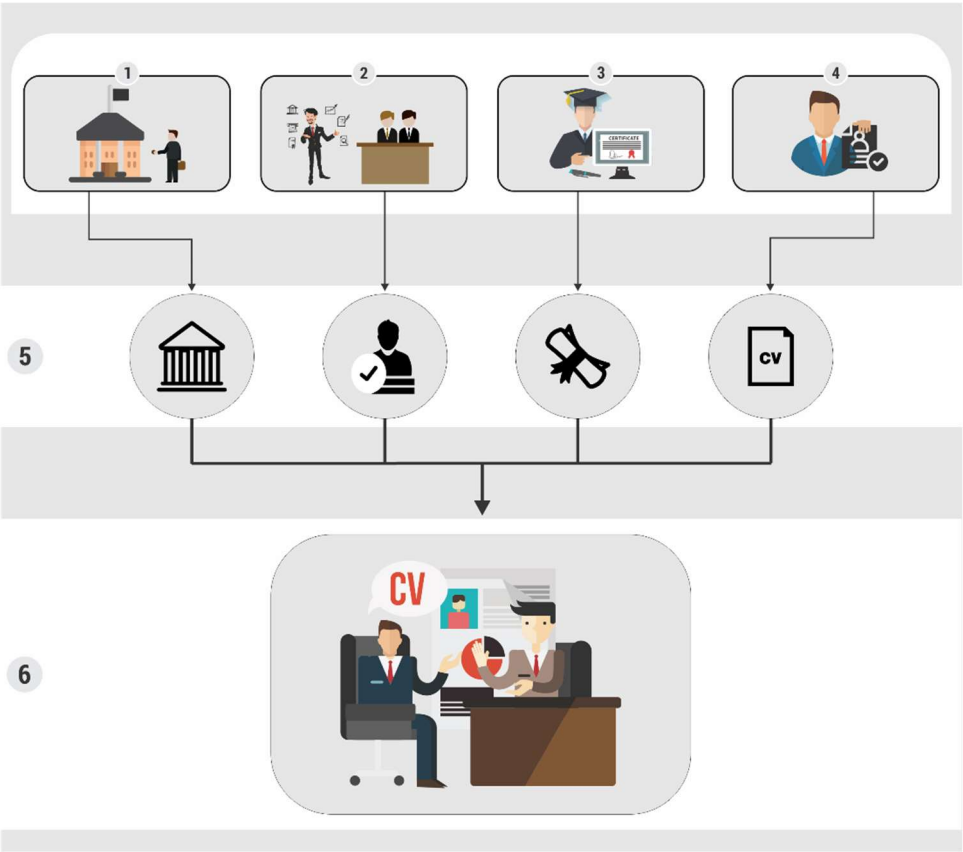
[17] Windley 2016 s. 3.

[18] Hajautetun julkisen avaimen menetelmä on hajautettuun järjestelmään luotu toteuttamistapa julkisen avaimen menetelmästä. Tästä tarkemmin ks. Sovrin Foundation 2018 s. 9 sekä sen sivulla 27 mainittu julkaisu.

[19] Rekisterinpitäjän määritelmästä ks. jakso 2.3.2

[20] Windley 2016 s.5–6.

käsittelyä tai varmenteiden vahvistuksia. Kuvion avulla havainnollistetaan siis yksinkertainen käyttötapa itsehallittavalle identiteetille.



Kuvio 1. Itsehallittavan identiteetin käyttäminen (Shaiq Ahmed, 2018)

1. Käyttäjä saa Väestörekisterikeskukselta *varmennettavan väitteen*, jonka sisältönä on hänen henkilötunnuksensa (josta tässä johdetaan täysi-ikäisyys). **2.** Käyttäjä saa luottotietorekisteriltä *varmennettavan väitteen*, jonka sisältönä on hänen luottotietonsa. **3.** Käyttäjä saa yliopistolta *varmennettavan väitteen*, jonka sisältönä on hänen tutkintonsa. **4.** Käyttäjä luo itse ansioluettelon ja liittää sen identiteettiinsä *väitteenä*. **5.** Käyttäjä yhdistää näistä tiedoista *julkituonnin*. **6.** Käyttäjä vastaa työpaikkahakemukseen käyttäen luotua *julkituontia.*

Jos työnhakijaan halutaan ottaa yhteyttä, työnantaja voi pyytää itsehallittavan identiteetin avulla tähän tarvittavan lisätiedon *väitteen* muodossa, esimerkiksi puhelinnumeron.

2.2 Tietosuoja-asetuksen soveltamisen edellytykset

2.2.1 Aineellinen ja alueellinen soveltamisala

Artiklassa 2 määritellään tietosuoja-asetuksen aineellinen soveltamisala. Asetusta sovelletaan luonnollisten henkilöiden henkilötietojen käsittelyyn kolmannen toimesta.[21]

Itsehallittavassa identiteetissä rekisterinpitäjällä on pääsy rekisteröidyn hallinnoimiin henkilötietoihin.[22] Tämä on henkilötietojen käsittelyä[23], joten asetusta sovelletaan itsehallittavaa identiteettiä käytettäessä asetuksen aineellisen soveltamisalan edellytykset täyttyvät.

Artiklassa 3 määritellään tietosuoja-asetuksen alueellinen soveltamisala. Asetusta sovelletaan, kun käsittely tapahtuu Euroopan unionin oikeudenkäyttöpiirissä olevan rekisterinpitäjän toimesta tai koskee unionissa olevan rekisteröidyn henkilötietoja.[24]

Itsehallittavaa identiteettiä voidaan alueellisesti käyttää missä vain. Tutkielman tarkoituksenmukaisuuden vuoksi alueellisen soveltamisalan oletetaan täyttyvän.

2.2.2 Suostumus käsittelyyn

> ”1. Käsittely on lainmukaista ainoastaan jos ja vain siltä osin kuin vähintään yksi seuraavista edellytyksistä täyttyy:
> a) rekisteröity on antanut suostumuksensa henkilötietojensa käsittelyyn yhtä tai useampaa erityistä tarkoitusta varten;
> b) käsittely on tarpeen sellaisen sopimuksen täytäntöön panemiseksi, jossa rekisteröity on osapuolena, tai sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä;
> c) käsittely on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi;
> d) käsittely on tarpeen rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaamiseksi;
> e) käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi;
> f) käsittely on tarpeen rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi, paitsi milloin henkilötietojen suojaa edellyttävät rekisteröidyn edut tai perusoikeudet ja -vapaudet syrjäyttävät tällaiset edut, erityisesti jos rekisteröity on lapsi.”

Artiklan 6(1) kohta edellyttää vähintään yhden sen vaatimuksista täyttyvän henkilötietojen käsittelyn lainmukaisuuden edellytyksenä. Itsehallittavaan identiteettiin liittyen näistä vaatimuksista olennaisin on alakohdan 1a mukainen suostumus. Koska itsehallittavaa identiteettiä käytettäessä luonnollinen

[21] EU:n tietosuoja-asetus, artikla 2 & resitaali 14.
[22] Windley 2016 s. 3 & 6.
[23] EU:n tietosuoja-asetuksen artikla 4(3) mukaisesti henkilötietojen käsittelyä on mm. haku ja käyttö.
[24] EU:n tietosuoja-asetus, artikla 3 sekä resitaalit 22 & 23.

henkilö hallinnoi henkilötietojaan itse eivätkä ne ole haettavissa ilman tämän suostumusta, katson käsittelyn lainmukaisuuden perustuvan aina vähintään artiklan 6(1)(a) alakohdan mukaiseen käsiteltävän suostumukseen.[25]

Suostumuksen edellytykset todetaan 7 artiklassa, jotka käsittelen kohdittain alla. Koska artiklan 7(2) kohdan mukainen kirjallinen suostumus ei itsehallittavan identiteetin digitaalisen luonteen vuoksi saa merkitystä, olen rajannut tuon kohdan tutkimuksen ulkopuolelle.

2.2.2.1 Suostumuksen osoittaminen

> ”1. Jos tietojenkäsittely perustuu suostumukseen, rekisterinpitäjän on pystyttävä osoittamaan, että rekisteröity on antanut suostumuksen henkilötietojensa käsittelyyn.”

Koska itsehallittavassa identiteetissä rekisterinpitäjä ei saa henkilötietoja käsiteltäväkseen ilman käyttäjän suostumusta[26], rekisterinpitäjä pystyy nähdäkseni osoittamaan rekisteröidyn suostumuksen yksinkertaisesti sillä, että hänellä on pääsy käyttäjän itsensä hallinnoimiin henkilötietoihin ja näin täyttämään kohdan 1 vaatimuksen. Tätä näkemystä tukevat asetuksen esityöt sekä työryhmämietinnöt, joissa on todettu suostumuksen toteutuvan esimerkiksi rekisteröidyn sähköisessä muodossa antamalla vapaaehtoisella, yksilöidyllä, tietoisella ja yksiselitteisellä tahdonilmaisulla.[27] Kun itsehallittavassa identiteetissä kullekin reksiterinpitäjälle annettu tiedonsaantioikeus pohjautuu rekisteröidyn suostumukseen, rekisterinpitäjän kyky käsitellä rekisteröidyn henkilötietoja osoittaa voimassaolevan suostumuksen olemassaolon. Käytän tästä käsittelyn mahdollistavasta suostumuksen osoittamisesta nimitystä *suostumusosoitus*.

2.2.2.2 Suostumuksen peruuttaminen

> ”3. Rekisteröidyllä on oikeus peruuttaa suostumuksensa milloin tahansa. Suostumuksen peruuttaminen ei vaikuta suostumuksen perusteella ennen sen peruuttamista suoritetun käsittelyn lainmukaisuuteen. Ennen suostumuksen antamista rekisteröidylle on ilmoitettava tästä. Suostumuksen peruuttamisen on oltava yhtä helppoa kuin sen antaminen.”

Rekisteröidyn oikeus peruuttaa suostumuksensa saa tukea itsehallittavan identiteetin teknisistä ominaisuuksista, sillä käyttäjä pystyy päättämään suostumuksensa voimassaolosta yksipuolisesti ja määräaikoihin sitoutumatta.[28] Käyttäjä voi siis perua rekisterinpitäjän pääsyn tietoihin milloin vain.

[25] Muut lainmukaisuuden edellytykset voivat saada suurempaa merkitystä teknologian käyttöönoton laajentuessa.
[26] Sovrin Foundation 2018 s. 38.
[27] EU:n tietosuoja-asetus, resitaali 32 sekä WP259 s. 5–20.
[28] Windley 2016 s. 5.

Perumistilanteessa kyseessä on aiemmin kuvatun suostumusosoituksen lakkaaminen, eli suostumuksen peruuttaminen. Peruuttamisen jälkeen käyttäjän henkilötietojen käsittely voi yhä täyttää jonkin muun 6 artiklan mukaisen käsittelyn lainmukaisuusvaatimuksen, mutta nähdäkseni rekisterinpitäjän kannalta ongelmia voi tuottaa se, ettei pääsyä henkilötietoihin enää ole. Jos henkilötietojen käsittely perustuu esimerkiksi rekisterinpitäjän julkisen vallan käyttöön tai luonnollisten henkilöiden elintärkeiden etujen suojaamiseen, itsehallittavan identiteetin käyttäminen ainoana henkilörekisterinä ei ole välttämättä mahdollista. Kuvaamani tilanne edellyttäisi perinteisen henkilörekisterin luomista itsehallittavan rinnalle tai tilalle.

2.2.2.3 Suostumuksen vapaaehtoisuus

> ”4. 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.”

Henkilötietojen käsittelyn alkaessa itsehallittavan identiteetin käyttäjä saa päätelaitteellaan tietää, mihin henkilötietoihin rekisterinpitäjä vaatii pääsyn palvelun käyttämiseksi.[29] Artiklan 5(1)(c) alakohdan mukaisesti rekisterinpitäjän tulee noudattaa tarpeellisuusvaatimusta (tietojen minimoinnin vaatimusta) valitessaan nämä vaatimansa henkilötiedot. Artiklan 7(4) kohdassa käsitellään tilanteita, joissa rekisterinpitäjä vaatii palvelun käyttöä varten tarpeellisuusvaatimuksen ulkopuolisia tietoja. Keskimääräinen käyttäjä ei todennäköisesti ole tietoinen siitä, mitkä tiedot ovat tarpeellisuusvaatimuksen mukaisia ja mitkä eivät. Rekisterinpitäjän pyytäessä tarpeellisuusvaatimuksen ulkopuolisia tietoja niin sanotulla opt-out-menetelmällä[30] esitöissä mainittu tietoinen tahdonilmaisu ei täyty. Tällaisessa tilanteessa suostumusta ei ole katsottava vapaaehtoiseksi[31], ja henkilötietojen käsittelyn on täytettävä jokin muu 6 artiklan käsittelyn lainmukaisuusperuste. Asetuksen esitöiden mukaan myös epäsuhtaisissa suhteissa suostumuksen tulisi täyttää jokin käsittelyn lainmukaisuusperuste, sillä näissä tilanteissa suostumusta ei todennäköisesti ole annettu vapaaehtoisesti.[32]

[29] Windley 2016 s. 3–9.
[30] Esimerkiksi valmiiksi rastitettu ruutu, joka on kuitenkin mahdollista rastittaa pois, jos kyseisiä tietoja ei halua luovuttaa rekisterinpitäjälle.
[31] EU:n tietosuoja-asetus, resitaali 43: ” Suostumusta ei katsota vapaaehtoisesti annetuksi, jos ei ole mahdollista antaa erillistä suostumusta eri henkilötietojen käsittelytoimille huolimatta siitä, että tämä on asianmukaista yksittäistapauksissa, tai jos sopimuksen täytäntöönpanon, mukaan lukien palvelun tarjoamisen, edellytyksenä on suostumuksen antaminen huolimatta siitä, että tällainen suostumus ei ole tarpeellista sopimuksen täytäntöön panemiseksi.”
[32] EU:n tietosuoja-asetus, resitaali 43.

2.3 Tietosuoja-asetuksen määritelmät

Tietosuoja-asetuksen artiklasta 4 löytyy suurimmaksi osaksi melko notorisia määritelmiä, mutta pseudonymisoinnin ja rekisterinpitäjän määritelmien lähempi tarkastelu on mielekästä itsehallittavan identiteetin keskeisten toimintaperiaatteiden selventämiseksi.

2.3.1 Pseudonymisointi

Pseudonymisointi määritellään artiklan 4(5) kohdassa seuraavasti:

> ”Henkilötietojen käsittelemistä siten, että henkilötietoja ei voida enää yhdistää tiettyyn rekisteröityyn käyttämättä lisätietoja, edellyttäen että tällaiset lisätiedot säilytetään erillään ja niihin sovelletaan teknisiä ja organisatorisia toimenpiteitä, joilla varmistetaan, ettei henkilötietojen yhdistämistä tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön tapahdu.”

Itsehallittavan identiteetin avulla rekisterinpitäjillä on mahdollisuus vähentää merkittävästi henkilörekisterien laajuutta. Kun rekisteröidyltä itseltään voidaan luotettavasti ja helposti pyytää tarvittavat tiedot tarvittaessa, rekisterinpitäjälle ei muodostu tarvetta säilöä henkilötietoja kaiken varalta. Rekisteröity voidaan silti tunnistaa käyttäen *hajautettua tunnistetta*.[33] Tarkastelemalla ylläolevaa EU:n tietosuoja-asetuksen pseudonymisointimäärittelyä havaitaan, että hajautettu tunniste täyttää pseudonymisoinnin vaatimukset, sillä hajautettu tunniste on salattu, ja sen yhdistäminen luonnolliseen henkilöön edellyttää tämän henkilön aktiivisia toimia.[34]

2.3.2 Rekisterinpitäjä

Rekisterinpitäjällä on päävastuu ja -velvollisuus tietosuojavelvoitteiden noudattamisessa, joten rekisterinpitäjän määrittely on tärkeää tietosuojatoimenpiteiden ja sanktioiden kohdentamisen vuoksi.[35] EU:n tietosuoja-asetuksen artiklan 4(7)(1) alakohdan mukaisesti rekisterinpitäjällä tarkoitetaan

> ”luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot”.

Keskeisimpänä osana tätä alakohtaa on henkilötietojen käsittelyn tarkoitukset ja keinot määrittelevä taho. Tietosuoja-asetuksen artiklan 5(1)(c) alakohdan tarpeellisuusvaatimuksen mukaisesti käsiteltävien henkilötietojen tulee rajautua siihen, mikä on tarpeellista käsittelyn tarkoituksien kannalta. Toteuttaakseen nämä edellytykset ja ylipäätään käsitelläkseen henkilötietoja rekisterinpitäjän tulee olla

[33] Tobin, Reed 2017 s.11.
[34] Windley 2016 s.3.
[35] Rücker, Kugel s. 24.

tietoinen mitä varten hän tietoja pyytää sekä mihin tarkoitukseen hän aikoo tietoja käyttää. Tietojenkäsittelyn aloittamiseksi nämä käsittelyn tarkoitukset ja keinot on siis edellä mainitun artiklan mukaisesti määriteltävä.

Koska itsehallittavaa identiteettiä käytettäessä artiklan 2 mukainen aineellinen soveltamisala täyttyy[36], henkilötietoja käsittelevän tahon tulee määritellä henkilötietojen käsittelyn tarkoitukset ja keinot. Itsehallittavassa identiteetissä rekisterinpitäjäksi muodostuu siis se taho, jolla on pääsy identiteetin omistajan tietoihin. EU:n tietosuoja-asetuksen mukainen rekisterinpitäjän määritelmä on siis yhtäläinen perinteisen henkilörekisterin ja itsehallittavan identiteetin henkilörekisterin osalta: rekisterinpitäjä on kummassakin se taho, joka käsittelee henkilötietoja ja määrittelee tuon käsittelyn tarkoitukset ja keinot.

3 Yhteensopivat osat

Suurin osa itsehallittavan identiteetin ominaisuuksista on yhteensopivia tietosuoja-asetuksen kanssa. Nämä ominaisuudet käsitellään järjestyksessä käsittelyn vaatimukset – rekisteröidyn oikeudet – rekisterinpitäjän velvollisuudet.

3.1 Rekisteröidylle toimitettavat tiedot

Artiklassa 13 luetellaan tiedot, jotka rekisteröidylle tulee toimittaa henkilötietojen käsittelysuhteen alussa, sekä perusteet, joilla tiedon toimittamisvelvollisuutta ei muodostu. Toimitettavat tiedot on jaettu organisatorisiin ja teknisiin, joista jälkimmäiset ovat relevantteja itsehallittavan identiteetin kannalta. Lähtökohtaisesti rekisterinpitäjän tulee toimittaa rekisteröidylle kaikki käsittelyä koskevat tarpeelliset tiedot, ellei rekisteröidyllä jo ole näitä tietoja.[37]

Käsittelyn tarkoituksen vaihdellessa henkilörekistereittäin, laillisuusperusteena itsehallittavaa identiteettiä käytettäessä on aina vähintään käsiteltävän suostumus.[38] Käsittelyn alkaessa rekisteröity antaa rekisterinpitäjälle pääsyn hallitsemiinsa tietoihin, eli suostumuksensa. Mikäli rekisterinpitäjä ei käsittelysuhteen alkaessa toimita rekisteröidylle artiklan 13(1)(c) alakohdan mukaista tietoa käsittelyn laillisuusperusteesta sekä tarvittaessa 1d alakohdan mukaista lisätietoa oikeutettujen etujen sisällöstä, katson käsittelyn laillisuuden perustuvan vain suostumukseen. Nähdäkseni pelkkään suostumukseen

[36] Tarkemmin ks. jakso 2.2.1.
[37] EU:n tietosuoja-asetus, artikla 13.
[38] Suostumuksesta tarkemmin ks. jakso 2.2.2.

perustuvan käsittelyn laillisuusperustetta ei tarvitse itsehallittavaa identiteettiä käytettäessä ilmoittaa, sillä käyttäjä on käsittelysuhteen alkaessa artiklan 13(4) kohdassa tarkoitetusti tietoinen suostumuksestaan käsittelyyn sekä tuon suostumuksen alaisista henkilötiedoista. Jos käsittelyn lainmukaisuus kuitenkin perustuu muuhun kuin suostumukseen, tiedot laillisuusperusteesta tulee toimittaa rekisteröidylle. Tämä todetaan myös artiklan 13(2)(e) alakohdassa, jossa lakisääteiseen velvollisuuteen tai sopimuksen täyttämiseen perustuvasta käsittelystä säädetään tietojen toimittamisvelvollisuus.

Rekisteröidylle tulee myös toimittaa tieto henkilötietojen säilytysajasta. Tulkitsen artiklassa käytettyä sanamuotoa ”säilytysaika” laajasti, sillä vaikka itsehallittavan identiteetin järjestelmässä rekisterinpitäjä ei säilytä tietoja vaan ainoastaan käyttää niitä, molemmissa on kyse artiklan 4(2) kohdan mukaisesta henkilötietojen käsittelystä. Itsehallittavaa identiteettiä käytettäessä henkilötietojen käsittelyaika määritellään ja siihen annetaan suostumus käsittelysuhteen alkaessa.[39] Käyttäjällä on siis tieto käsittelyajasta käsittelysuhteen alusta alkaen, joten katson myös tässä käyttäjän olevan artiklan 13(4) kohdassa tarkoitetusti tietoinen, eikä tietojen toimitusvelvollisuutta muodostu.

Rekisterinpitäjälle on myös asetettu velvollisuus toimittaa rekisteröidylle tiedot tämän tietyistä oikeuksista. Nämä tiedotusvelvollisuuden alaiset oikeudet ovat lueteltu artiklan 13(2)(b–d) alakohdissa. Ne vastaavat artiklojen 7, 15-22 sekä 77 mukaisia oikeuksia.[40] Itsehallittavan identiteetin järjestelmässä ei oletusarvoisesti anneta tietoa näistä oikeuksista, joten katson rekisterinpitäjälle muodostuvan tiedotusvelvollisuuden näistä tiedoista.

Lopuksi artiklassa 13 rekisterinpitäjälle asetetaan velvollisuus toimittaa rekisteröidylle tiedot automaattisen tietojenkäsittelyn käytöstä sekä ennakollinen tiedottamisvelvollisuus muuhun, kuin alkuperäiseen tarkoitukseen perustusvasta käsittelystä. Näissä kohdissa 2f sekä 3 mainituissa tiedottamisvelvollisuuden muodostavissa tilanteissa on kyse rekisterinpitäjän henkilötietojen käsittelytoimista. Itsehallittavaa identiteettiä käytettäessä rekisteröity päättää, mihin tietoihin rekisterinpitäjällä on pääsy, mutta ei tietojen käyttötarkoitusta. Katsoakseni rekisterinpitäjälle muodostuu tämän vuoksi tiedotusvelvollisuus näistä tiedoista.

Vaikka itsehallittavaa identiteettiä käytettäessä rekisterinpitäjä pystyy välttämään joidenkin tietojen toimitusvelvollisuuden artiklan 13(4) kohdan mukaisesti, työryhmämietintöjen mukaan hyvää käsittelytapaa noudattavan rekisterinpitäjän olisi kuitenkin hyvä toimittaa nämä tiedot uudelleen.[41]

[39] Windley 2016 s.7.
[40] Artiklan 7 mukaisesta suostumuksen peruuttamisoikeudesta ks. 2.2.2.2, artiklojen 15–22 mukaisista oikeuksista ks. 3.3, 4.1, 4.2 ja 4.3. Artiklan 77 mukainen oikeus tehdä ilmoitus hallintoviranomaiselle on rajattu tutkimuksen ulkopuolelle.
[41] WP260 s. 24–25.

Artiklaa 13 läheisesti muistuttavassa artiklassa 14 kuvataan rekisterinpitäjän tietojen toimitusvelvollisuutta silloin, kun henkilötietoja ei ole kerätty rekisteröidyltä. Itsehallittavassa identiteetissä henkilötiedot kerätään aina rekisteröidyltä. Tämän vuoksi artiklan 14 mukainen tietojen toimitusvelvollisuus ei liity itsehallittavaan identiteettiin, enkä sitä siksi käsittele.

3.2 Käsittely, joka ei edellytä tunnistamista

Artiklassa 11 kuvataan käsittelyä, joka ei edellytä tunnistamista. Artiklan kohta 1 määrittelee tämän seuraavasti:

> ”Jos tarkoitukset, joihin rekisterinpitäjä käsittelee henkilötietoja, eivät edellytä tai eivät enää edellytä, että rekisterinpitäjä tunnistaa rekisteröidyn, rekisterinpitäjällä ei ole velvollisuutta säilyttää, hankkia tai käsitellä lisätietoja rekisteröidyn tunnistamista varten, jos tämä olisi tarpeen vain tämän asetuksen noudattamiseksi.”

Itsehallittavan identiteetin palvelussa on mahdollista, että käsiteltävät henkilötiedot ovat niin rajattuja, ettei luonnollinen henkilö ole tunnistettavissa. Esimerkiksi ikärajattuun verkkopalveluun voidaan osoittaa tieto ”olen yli 18-vuotias” todeksi kuitenkaan paljastamatta ikää.[42] Tällainen *julkituonti* ei mahdollista luonnollisen henkilön tunnistamista ja artiklan 11(1) kohdan määritelmä täyttyy. Täyttyminen saa merkitystä saman artiklan kohdasta 2:

> ”Jos tämän artiklan 1 kohdassa tarkoitetuissa tapauksissa rekisterinpitäjä pystyy osoittamaan, ettei se pysty tunnistamaan rekisteröityä, rekisterinpitäjän on ilmoitettava asiasta rekisteröidylle, jos tämä on mahdollista. Tällaisissa tapauksissa 15–20 artiklaa ei sovelleta, paitsi jos rekisteröity näiden artikloiden mukaisia oikeuksiaan käyttääkseen antaa lisätietoja, joiden avulla hänet voidaan tunnistaa.”

Pelkkää julkituontia käytettäessä rekisterinpitäjän tulee siis ilmoittaa rekisteröidylle tästä. Merkittävämpi osa tätä kohtaa on kuitenkin jälkimmäinen virke. Koska artiklan 11(1) kohta täyttyy, rekisteröidylle ei nähdäkseni tällaisissa tapauksissa automaattisesti muodostu artiklojen 15–20 mukaista oikeutta tietoihin, tiedon oikaisemiseen, tiedon poistamiseen, käsittelyn rajoittamiseen, eikä oikeutta siirtää tietoja järjestelmästä toiseen. Tietosuoja-asetuksen esitöiden mukaan rekisterinpitäjän tulisi kuitenkin sisällyttää tällaiseen rekisteriin mekanismi, jolla rekisteröity voidaan tunnistaa uudelleen.[43] Kun käytetään itsehallittavaa identiteettiä, tämä mekanismi toteutetaan *hajautetun tunnisteen* avulla. Sitä käyttämällä rekisteröity voi myöhemmin tunnistautua ja osoittaa, että rekisterissä oleva

[42] Windley 2016, s. 5–6. Vrt. vahva sähköinen tunnistaminen osoittaessa täysi-ikäisyys: käyttäjä joutuu jakamaan henkilötunnuksensa. Sen sijaan, että pelkkä täysi-ikäisyys osoitetaan, jaettujen henkilötietojen määrä on tarkoitusta suurempi, sillä henkilötunnuksesta selviää tarkka ikä ja sukupuoli. Lisäksi henkilötunnus itsessään on yhdistettävissä tiettyyn luonnolliseen henkilöön.
[43] EU:n tietosuoja-asetus, resitaali 57.

henkilötieto koskee häntä. Näin rekisteröity voi myös tällaisessa tietojen käsittelyssä, joka ei edellytä tunnistautumista vaatia artikloissa 15–20 kuvattuja oikeuksiaan.

3.3 Oikeus tulla unohdetuksi

Artiklassa 17 kuvataan rekisteröidyn oikeus tätä koskevien tietojen poistamiseen henkilörekisteristä sekä poistamisen edellytykset.[44] Oikeus tulla unohdetuksi ei siis ole absoluuttinen. Näistä edellytyksistä itsehallittavan identiteetin kannalta merkittävin on 1b kohdan mukainen suostumuksen peruuttaminen, sillä itsehallittavassa identiteetissä käsittely perustuu aina vähintään suostumukseen.[45] Suostumuksen peruuttamisen tulisi johtaa tietojen poistamiseen, ellei jokin 3 kohdan mukainen edellytys täyty.

Itsehallittavassa identiteetissä oikeus tulla unohdetuksi toteutuu vahvemmin kuin artikla 17 edellyttää, sillä käyttäjä pystyy milloin vain peruuttamalla suostumuksensa peruuttamaan rekisterinpitäjän pääsyn tietoihin, eli tosiasiallisesti poistamaan häntä itseään koskevat tiedot rekisterinpitäjän rekisteristä.[46] Käyttäjä pystyy siis ”itse unohtamaan itsensä”. Tämä voi muodostaa ongelman muun laillisuusperusteen, kuin suostumuksen perusteella käsiteltävän tiedon osalta.[47]

Jos rekisterinpitäjä on siirtänyt tietoja itsehallittavan identiteetin henkilörekisteristä toiseen henkilörekisteriin, nämä tiedot ovat myös kohtuullisuuden rajoissa itsehallittavan identiteetin tietoja koskevan poisto-oikeuden alaisia.[48] Suostumuksen peruuttamisen tuleekin johtaa myös itsehallittavan identiteetin henkilörekisteristä kopioitujen tietojen poistamiseen tästä toisesta rekisteristä.

3.4 Rekisterinpitäjän vastuu sekä sisäänrakennettu ja oletusarvoinen tietosuoja

24 artiklassa kuvataan rekisterinpitäjän tietoturvan toteuttamista ja sen osoittamisvelvollisuutta viitaten vahvasti muihin artikloihin, kuten 30 artiklaan sekä käytännesääntöjä ja sertifikaatteja koskeviin 40 ja 42 artikloihin. Etenkin artiklan 24(1) kohta on hyvin abstrakti, eikä anna edes esimerkkejä näistä toteutustavoista. Nähdäkseni merkittävin osa tätä artiklaa on rekisterinpitäjän osoitusvelvollisuus siitä, että tekniset ja organisatoriset menettelytavat on toteutettu. Myös osoittamisen osalta viitataan

[44] EU:n tietosuoja-asetus, artikla 17.
[45] Tarkemmin ks. 2.2.2.
[46] Windley 2016 s.5.
[47] Tarkemmin ks. 2.2.2.2.
[48] EU:n tietosuoja-asetus, artikla 17(2) & resitaali 66.

artikloihin 40 ja 42.[49] Arviointia itsehallittavan identiteetin osalta tulee siis tehdä näiden artiklojen pohjalta tulevaisuudessa annettavien käytännesääntöjen ja sertifikaattien kautta.

25 artikla kuvaa yleisesti rekisterinpitäjän teknistä ja organisatorista menettelyä henkilötietojen käsittelyn toteutuksessa, kuitenkaan antamatta varsinaisesti konkreettisia toteutustapoja muutoin, kuin esimerkkien muodossa ja viitaten tietosuojaperiaatteisiin.[50] Tarkoituksena onkin, että sertifikaattien avulla annetaan tulevaisuudessa tarkemmat ohjeet sisäänrakennetun ja oletusarvoisen tietosuojan menetelmistä eri sovellutuksissa.[51] Koska itsehallittava identiteetti on tekninen sovellutus henkilötietojen käsittelylle, organisatoristen menetelmien käsittely rajautuu tutkimuksen ulkopuolelle.

Sisäänrakennettu ja oletusarvoinen tietosuoja merkitsee sitä, että rekisterinpitäjä huolehtii yksityisyyden sekä artiklan 5 mukaisten tietosuojaperiaatteiden toteutumisesta teknisin ja organisatorisin menetelmin henkilötietojen käsittelyn alusta alkaen. Esimerkiksi pseudonymisointi on sisäänrakennettua tietosuojaa ja rajattu käsittelijäpiiri oletusarvoista tietosuojaa[52], ja nämä molemmat toteutuvat teknisin menetelmin itsehallittavassa identiteetissä.[53] Muita oletusarvoisen tietosuojan teknisiä toteutustapoja itsehallittavassa identiteetissä ovat muun muassa julkituonnit[54] ja hajautetut tunnisteet.[55]

Sisäänrakennetun tietosuojan kannalta tulee myös huomata henkilötietojen käsittelyn yksi yleisistä vaatimuksista, tietojen minimoinnin vaatimus (tarpeellisuusvaatimus), joka rajoittaa henkilörekisterin sallittujen tietojen laajuutta niin, että ainoastaan tarpeelliset tiedot ovat rekisterissä.[56] Rekisterinpitäjän toteuttaessa rekisterin itsehallittavan identiteetin avulla tarpeellisen tiedon määrä voi selvästi rajautua, sillä jokaisella rekisteröidyllä on henkilökohtainen tunniste, jonka avulla palaava rekisteröity tunnistetaan samaksi, ja tässä yhteydessä rekisteröidylle voidaan esittää vaatimus tarpeellisten tietojen esittämisestä. Jokaisessa tiedonsiirtotilanteessa on myös mahdollista toteuttaa tarpeellisuusvaatimus, sillä julkituontien avulla henkilötiedoista voidaan paljastaa pienin tarvittava määrä.[57] Itsehallittavan identiteetin järjestelmässä tietojen minimoinnin vaatimus on siis sisäänrakennettuna ominaisuutena.

[49] EU:n tietosuoja-asetus, artikla 24.
[50] EU:n tietosuoja-asetus, artikla 25.
[51] EU:n tietosuoja-asetus, resitaali 78.
[52] EU:n tietosuoja-asetus, resitaali 78.
[53] Sovrin Foundation 2018 s. 20. Julkituonneista tarkemmin ks. 3.2.
[54] Abraham 2017 s. 34.
[55] Sovrin Foundation 2018 s. 20.
[56] EU:n yleinen tietosuoja-asetus, artikla 5(1)(c).
[57] Windley 2016 s.5–6. Aiheesta tarkemmin ks. 3.2.

3.5 Henkilötietojen käsittelyn turvallisuus

Rekisterinpitäjälle ja henkilötietojen käsittelijälle on artiklan 32(1) kohdassa annettu esimerkkejä velvollisuuksista, jotka tulee toteuttaa riskien minimoimiseksi. Näitä toimenpiteitä ovat

> ”1.
> a) pseudonymisointi ja salaus,
> b) kyky taata käsittelyjärjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus,
> c)kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa sekä
> d)menettely, jolla testataan, tutkitaan ja arvioidaan säännöllisesti teknisten ja organisatoristen toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi.”

Velvoitteiden konkreettiset toteuttamistavat selkeytyvät tulevaisuudessa kattojärjestöjen käytännesääntöjen tai sertifikaattien avulla[58]. Käsittelyn ulkopuolelle jää alakohta d), sillä sen velvoitteet liittyvät enemmän rekisterinpitäjän tietosuojan varmistaviin organisatorisiin toimenpiteisiin kuin itsehallittavan identiteetin toteutustapoihin ja sääntelyyn.

3.5.1 Pseudonymisointi ja salaus

Henkilötietojen pseudonymisointi ja salaus onnistuu hajautetun tunnisteen avulla ensinnäkin sen ollessa jokaisen rekisterinpitäjän kohdalla sekä uniikki että salattu, ja toisekseen hajautetun tunnisteen sisältäessä vain salausavaimen rekisteröidyn uudelleentunnistamiseksi, eli minimimäärän tietoa. Tietosuoja-asetuksen esitöissä pseudonymisoitu henkilötieto olisi katsottavissa luonnollista henkilöä koskevaksi tiedoksi, jos se voidaan yhdistää luonnolliseen henkilöön lisätietoja käyttämällä. Yhdistettävyys luonnolliseen henkilöön tulee määrittää sen mukaan, onko luonnollinen henkilö kohtuullisen todennäköisiä keinoja käyttämällä tunnistettavissa suoraan tai välillisesti.[59] Luonnollisen henkilön tunnistamiskeinona hajautetussa tunnisteessa on rekisteröidyn sähköinen tunnistautuminen käyttäen omaa päätelaitettaan.[60] Koska kyseisestä tiedosta ei ole poistettu yhdistettävyyttä luonnolliseen henkilöön, se ei ole anonyymi tieto. Hajautettu tunniste lukeutuu pseudonymisoidun henkilötiedon määritelmään, joten tietosuojaperiaatteita on noudatettava, vaikka rekisterinpitäjä tai kolmas taho ei pysty tunnistamaan luonnollista henkilöä hajautetusta tunnisteesta edes yhteistoiminnassa muiden rekisterinpitäjien kanssa.[61]

---

[58] EU:n tietosuoja-asetus, artiklat 40 & 42.
[59] EU:n yleinen tietosuoja-asetus, resitaali 26.
[60] Tobin, Reed 2016 s. 11.
[61] Hajautetun tunnisteen ominaisuuksiin kuuluu yhdensuuntainen salaus ja rekisteröidyn mahdollisuus luoda eri tunniste kaikkiin eri rekistereihin. Rekisterinpitäjällä ei ole keinoja yhdistää hajautettua tunnistetta tiettyyn luonnolliseen henkilöön ilman rekisteröidyn omia toimia tunnistamisen edistämiseksi. Lisätietoja ks. Windley 2016 s. 3.

3.5.2 Luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus

Rekisterinpitäjän vastuu luottamuksellisuudesta ja eheydestä rajautuu tämän henkilörekisteriin talletettuihin tietoihin. Koska itsehallittavassa identiteetissä tällaista tietoa on vain hajautettu tunniste, rekisteröityjen henkilötietojen luottamuksellisuus on vahvaa. Tilanteissa, joissa hajautettuja tunnisteita sisältävä rekisteri on tietoturvaloukkauksen kohteena, kyseiset hajautetut tunnisteet voidaan sulkea ilman vaikutusta käyttäjän muihin palvelusuhteisiin.[62] Rekisterinpitäjän hallitsemien tietojen joutuminen vääriin käsiin luo kyllä tietoturvariskin, mutta tietojen hyödynnettävyys on milloin vain päätettävissä käyttäjän toimesta. Käsittelen tietoturvaloukkauksia tarkemmin artikloja 33 & 34 käsittelevässä jaksossa 3.6.

Käytettävyys ja vikasietoisuus ovat sisäänrakennettuja ominaisuuksia itsehallittavassa identiteetissä. Rekisterinpitäjällä on pääsy rekisteröidyn itsensä hallinnoimiin tietoihin – eli tiedot ovat käytettävissä – niin kauan, kun käyttäjä sallii pääsyn. Koska varmenteiden vahvistukset toteutetaan lohkoketjuteknologialla, on palvelun toimivuus katkeamatonta ja vikasietoista. Tämä johtuu lohkoketjuteknologian ominaisuuksista. Hajautettu solmuverkosto merkitsee sitä, että yksittäisen solmun poistuminen verkosta ei johda verkon kaatumiseen, vaan se edellyttäisi kaikkien solmujen käytöstä poistumista. Verkon kaatuminen tai vikaantuminen ovat kyllä teoriassa mahdollisia, mutta solmunverkon ollessa tarpeeksi laaja nämä ongelmat ovat käytännössä mahdottomia.[63]

3.5.3 Tietoihin pääsyn pysyvyys ja palautettavuus

Tätä vaatimusta tutkittaessa havaitaan perinteisen henkilörekisterin mallin vaikuttaneen sen muotoon. Tuollaisen tietokannan yleisenä piirteenä on henkilötietojen pitkäaikainen säilytys. Itsehallittavan identiteetin järjestelmässä rekisteröity itse päättää, kuinka pitkään rekisterinpitäjällä on pääsy tietoihin.[64] Kun tiedot eivät ole rekisterinpitäjän - vaan käyttäjän - hallussa, käyttäjällä on jatkuva tietojen saatavuus ja pääsy tietoihin. Vaatimukset kyvystä palauttaa tietojen saatavuus ja pääsy tietoihin vikatilanteissa eivät siis konkreettisesti muodosta itsehallittavan identiteetin järjestelmässä samanlaista vaatimusta rekisterinpitäjälle, koska tietojen säilytystapa poikkeaa merkittävästi tavanomaisesta henkilörekisteristä.

[62] Sovrin Foundation 2018 s. 21.
[63] Nurmi 2017.
[64] Windley 2016 s. 5 & 7. Käyttäjä voi antaa rekisterinpitäjälle pääsyn tietoihin määräajaksi tai toistaiseksi. Käyttäjällä on mahdollisuus peruuttaa rekisterinpitäjän pääsy tietoihin milloin vain.

3.6 Tietoturvaloukkauksesta ilmoittaminen

3.6.1 Tietoturvaloukkauksesta ilmoittaminen valvontaviranomaiselle

Artiklan 33(1) kohdasta on luettavissa rekisterinpitäjän ilmoitusvelvollisuus tietoturvaloukkaustilanteessa:

> ”Jos tapahtuu henkilötietojen tietoturvaloukkaus, rekisterinpitäjän on ilmoitettava siitä ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa sen ilmitulosta 55 artiklan mukaisesti toimivaltaiselle valvontaviranomaiselle, paitsi jos henkilötietojen tietoturvaloukkauksesta ei todennäköisesti aiheudu luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä. […]”

Itsehallittavaa identiteettiä käytettäessä rekisterinpitäjä tallettaa hajautettuja tunnisteita ja hakee niiden avulla tarpeelliset tiedot rekisteröidyltä. Rekisterinpitäjään kohdistuva tietoturvaloukkaus koskee siis hajautettujen tunnisteiden vaarantumista. Tietoturvaloukkaustilanteet voidaan objektiivisesti jakaa siis kahteen tilanteeseen: pelkän hajautetun tunnisteen (eli julkisen salausavaimen) vaarantuminen tai rekisterinpitäjän hajautettua tunnistetta koskevan yksityisen salausavaimen vaarantuminen. Ensin mainitun vaarantuminen ei johda pseudonymisoinnin kumoutumiseen, sillä pelkästä hajautetusta tunnisteesta ei ole yksisuuntaisesti mahdollista päätellä luonnollisen henkilön identiteettiä. Jälkimmäinen tilanne - yksityisen salausavaimen vaarantuminen - voi aiheuttaa kuitenkin merkittävän tietoturvariskin. Riskin suuruus riippuu täysin siitä, mihin tietoihin tuolla salausavaimella on pääsy ja kuinka nopeasti tietoturvaloukkaus havaitaan.

Koska hajautetut tunnisteet ovat pseudonymisoituja, niitä tulee käsitellä kuten henkilötietoja.[65] Pelkkiin hajautettuihin tunnisteisiin kohdistuva tietoturvaloukkaus on siis artiklan 4(12) kohdan määritelmän mukainen henkilötietojen tietoturvaloukkaus. Artiklassa 33 tietoturvaloukkauksen ilmoitusvelvollisuutta ei kuitenkaan ole sidottu pelkästään henkilötietojen tietoturvaloukkaukseen, vaan edellytyksenä on lisäksi luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuva riski. Tietoturvaloukkauksen kohdistuessa pelkkään hajautettuun tunnisteeseen potentiaalinen vaara rekisteröidylle on pieni, koska pseudonymisoinnin luvaton kumoutuminen on epätodennäköistä[66]. Tästä syystä katson, että artiklan 33 mukaista rekisterinpitäjän ilmoitusvelvollisuutta valvontaviranomaiselle ei

[65] Ks. kohta 2.3.1.

[66] Luvaton kumoutuminen voisi tapahtua esimerkiksi rekisterinpitäjän yksityisen salausavaimen ollessa myös tietoturvaloukkauksen kohteena. Hajautetusta tunnisteesta yksinään luonnollisen henkilön henkilöllisyyden selvittäminen on nykytiedon valossa lähes mahdotonta. Ks. The Sovrin Foundation 2016 s. 16

synny, sillä luonnollisen henkilön oikeuksiin ja vapauksiin kohdistuvaa riskiä ei varsin todennäköisesti muodostu.[67]

Yksityisen salausavaimen paljastuminen luo kuitenkin erilaisen tilanteen. Tuollaisen salausavaimen joutuessa tietoturvaloukkauksen johdosta vääriin käsiin on riskin suuruus riippuvainen kyseessä olevan yksityisen salausavaimen tärkeydestä. Itsehallittavassa identiteetissä salausavaimen merkittävyys on tulkittavissa suoraan sen sallimista rekisterinpitäjän tiedonhakuoikeuksista. Vaarantuvat tiedot voivat vaihdella yksinkertaisesta julkituonnista (esimerkiksi tieto ”rekisteröity on yli 18-vuotias”) arkaluonteisiin henkilötietoihin. Tietoturvaloukkauksen mahdollinen riski määräytyy siis sen mukaan, millaiseen tietoon salausavaimella päästään.

Pseudonymisoinnin luvaton kumoutuminen on erityisesti mainittu tietosuoja-asetuksen esitöissä sellaisena tietoturvaloukkauksena, josta aiheutuu luonnollisen henkilön oikeuksiin ja vapauksiin kohdistuva riski.[68] Hajautetun tunnisteen ollessa pseudonymisoitu tieto jonka tiedonhakuoikeuksiin päästään yksityisellä salausavaimella, pseudonymisoinnin luvattoman kumoutumisen vaara toteutuu tämän salausavaimen ollessa tietoturvaloukkauksen kohteena. Tietosuoja-asetuksen työryhmämietinnöissä ilmoituskynnys on kuitenkin sidottu tietoturvariskin potentiaaliseen suuruuteen.[69] Tarkoituksena on siis arvioida potentiaalisia haittavaikutuksia luonnollisen henkilön oikeuksien ja vapauksien toteutumiselle, eikä vain tietyn teknisen seikan toteutumista. Tämän vuoksi katson, että ilmoitusvelvollisuuden syntyminen edellyttää yksittäistapauksellista arviointia kulloisestakin tietosuojaloukkauksesta ja sen potentiaalisista haittavaikutuksista. Esimerkiksi artiklan 11 mukaisessa käsittelyssä, joka ei edellytä tunnistautumista pseudonymisoinnin kumoutuminen ei todennäköisesti johda sellaisiin riskeihin luonnollisten henkilöiden vapauksille ja oikeuksille, joissa ilmoitusta tietosuojaviranomaiselle tarvittaisiin.

3.6.2 Tietoturvaloukkauksesta ilmoittaminen rekisteröidylle

Artiklan 34(1) kohdasta on luettavissa ilmoitusvelvollisuus rekisteröidylle:

> ”Kun henkilötietojen tietoturvaloukkaus todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille, rekisterinpitäjän on ilmoitettava tietoturvaloukkauksesta rekisteröidylle ilman aiheetonta viivytystä.”

[67] Koska hajautettua tunnistetta tulee käsitellä kuin henkilötietoa, tietoturvaloukkaustilanteissa voi olla hyvä pyytää rekisteröityjä antamaan uusi hajautettu tunniste vanhan tilalle, jolloin vanhoista tunnisteista poistuu yhdistettävyys luonnolliseen henkilöön, eikä kyseessä ole enää henkilötieto, joten henkilötietojen tietoturvaloukkaustila päättyy.
[68] EU:n tietosuoja-asetus, resitaali 75.
[69] WP250 s.15.

Merkittävin ero edellisessä kappaleessa kuvailtuun 33 artiklaan on korkeampi ilmoituskynnys. Artikla 34 edellyttää luonnollisten henkilöiden oikeuksiin ja velvollisuuksiin kohdistuvan riskin sijasta *korkean* riskin aiheutumista. Tietosuoja-asetus ei määrittele, mikä on korkea riski luonnollisen henkilön oikeuksille ja vapauksille. Ilmoitusta pienemmän riskin tietoturvaloukkauksista tulisi kuitenkin välttää, sillä tämä voisi johtaa useisiin tietoturvaloukkausilmoituksiin, joissa riski ei lopulta konkretisoitunut. Tästä voisi seurata rekisteröityjen passiivisempi asennoituminen näihin ilmoituksiin, jolloin korkean riskin tilanteissa rekisteröity ei välttämättä suojaakaan etujaan.[70]

Edellä todetun mukaisesti tietoturvaloukkauksien osalta voidaan itsehallittavassa identiteetissä keskittyä yksityisiä salausavaimia koskievien loukkausten tarkasteluun, sillä pelkän hajautetun tunnisteen väärinkäyttö ei muodosta riskiä luonnolliselle henkilölle. Hajautettu tunniste täyttää myös artiklan 34(3)(a) alakohdan mukaiset tekniset toimenpiteet (henkilötiedon muuttaminen muotoon, jossa oikeudeton osapuoli ei niitä kykene lukemaan) sillä hajautettu tunniste on pseudonymisoidussa muodossa.[71] Tämän tietosuoja-asetuksen alakohdan täyttäminen poistaa rekisterinpitäjän ilmoitusvelvollisuuden, eli tietoturvaloukkauksen kohdistuessa pseudonymisoidussa muodossa olevaan hajautettuun tunnisteen ilmoitusvelvollisuutta ei ole. Toinen nähdäkseni saman alakohdan täyttävä toimenpide on säännöllinen salausavaimien kierrätys[72], sillä näin myös havaitsemattomien tietoturvaloukkauksien riskiä saadaan pienennettyä merkittävästi. Vaikka yleislinjauksia on jossain määrin mahdollista tehdä, korkeaa riskiä tulee artiklan 33 riskin tavoin tarkastella yksittäistapauksittain. Selviä tapauksia ovat tietoturvaloukkaukset, jotka koskevat pääsyä artiklan 9 mukaisiin arkaluonteisiin tietoihin. Näissä tilanteissa voidaan suurella varmuudella puhua korkeasta riskistä, jolloin ilmoitusvelvollisuus rekisteröidylle täyttyisi.

Yksityisten salausavaimen tietoturvaloukkaustilanteissa, joissa ilmoitusvelvollisuus artiklan 34(1) kohdan mukaan täyttyisi, rekisterinpitäjä voi artiklan 34(3)(b) alakohdan mukaisesti välttää ilmoitusvelvollisuutensa, jos tämä on ”toteuttanut jatkotoimenpiteitä, joilla varmistetaan, että 1 kohdassa tarkoitettu rekisteröidyn oikeuksiin ja vapauksiin kohdistuva korkea riski ei enää todennäköisesti toteudu”. Tietosuoja-asetuksessa ei määritellä konkreettisesti näitä jatkotoimenpiteitä, mutta itsehallittavan identiteetin osalta tällainen toimenpide voisi olla vaarantuneen yksityisen salausavaimen tekeminen käyttökelvottomaksi. Pääsy tietoihin ja tietojen vahvistaminen riippuvat voimassa olevista pääsyoikeuksista, jotka allekirjoitetaan identiteetin omistajan avaimilla. Tämän vuoksi näiden avaimien mitätöinti riittää tietojen käyttökelvottomaksi tekemiseen.[73] Ei ole vielä täysin selvää, onko

[70] Kugel, Rücker 2018 s. 152–153.
[71] Ks. kohta 2.3.1.
[72] Reed, Law, Hardman, Lodder 2018 kappale 8 ja erityisesti 8.1.
[73] Windley 2016 s.5.

rekisterinpitäjän teknisesti mahdollista toteuttaa sama toimenpide ilman omistajan toimia, mutta tällaisen mekanismin lisääminen rekisterinpitäjän toimintamahdollisuuksiin olisi periaatteessa mahdollista, kunhan se on rajattu.[74] Nähdäkseni kyseessä olevan mekanismin kehittämismotivaation taustalla olisi tietoturvan lisäämisen lisäksi EU:n tietosuoja-asetuksen 34(3)(b) alakohta. Merkittävimmässä yhdysvaltalaisessa lainsäädännössä ei ole vastaavanlaista poikkeusta ilmoitusvelvollisuudesta,[75] joten EU:n tietosuoja-asetuksen tarkempi tutkiminen itsehallittavan identiteetin kehitystyötä tehtäessä voisi olla hyväksi tietosuojan kehittämisen kannalta.

4 Ristiriitaiset osat

Itsehallittava identiteetti ei kaikilta osin ole täysin yhteensopiva EU:n tietosuoja-asetuksen kanssa. Ristiriitaiset ominaisuudet ovat rajautuneet rekisteröidyn oikeuksiin, ja ristiriitaisuus johtuu joko tietosuoja-asetuksen vaatimustason ylittävistä tai teknologian toteuttamistavasta johtuvista ominaisuuksista. Ne eivät kuitenkaan estä itsehallittavan identiteetin käyttämistä, sillä rekisteröidyllä on silti pääsy näihin oikeuksiinsa.

4.1 Oikeus saada pääsy tietoihin

Artiklasta 15 on luettavissa rekisteröidyn oikeus saada vahvistus siitä, käsitelläänkö tietoja, oikeus saada pääsy käsiteltäviin tietoihin sekä lista tiedoista, jotka rekisteröidyllä on oikeus saada.[76] Lista vastaa artiklan 12 mukaisia rekisteröidylle toimitettavia tietoja.[77]

Itsehallittavassa identiteetissä rekisteröidyllä on jatkuva pääsy tietoihinsa, sillä hän hallinnoi niitä itse.[78] Kun rekisteröity voi myös päätelaitteeltaan tarkastaa, mitä tietoja kukin rekisterinpitäjä hänestä käsittelee, pääsy tietoihin sekä tieto siitä, käsitelläänkö tietoja toteutuvat oma-aloitteisesti. Artiklan 15(1)(a-h) alakohdissa listatut oikeudet saada tieto käsiteltävistä tiedoista toteutetaan kuten tavanomaisessa henkilörekisterissä: rekisteröity esittää pyynnön ja rekisterinpitäjän tulee ne toimittaa.

[74] Sähköpostihaastattelu Tieto Finland oy:n Antti Kettusen kanssa 13.4.2018 & 10.5.2018.
[75] Tutkimuksen kohteena olevan Sovrin Foundationin itsehallittavan identiteetin kehitystyö on keskittynyt vahvasti Yhdysvaltioihin. Organisaatio ei kirjoitushetkellä ole saattanut päätökseen EU:n tietosuoja-asetuksen tutkimista, vaan lainsäädäntötutkimus on keskittynyt enemmän Yhdysvaltioihin. Yhdysvaltojen väkiluvultaan suurimman osavaltion Kalifornian tietosuojasäädöksen ilmoitusvelvollisuutta käsittelevässä kohdassa (California Civil Code §1798.82) ilmoitusvelvollisuuteen ei ole annettu poikkeuksia. Säädöstä tulee soveltaa, jos henkilörekisterissä on Kaliforniassa pysyvästi asuvan luonnollisen henkilön henkilötietoja (§1798.81.5). Tästä syystä useat Yhdysvalloissa toimivat yritykset joutuvat noudattamaan sen käytäntöjä; erittäin todennäköisesti myös Sovrin Foundationin itsehallittava identiteettijärjestelmä.
[76] EU:n tietosuoja-asetus, artikla 15.
[77] EU:n tietosuoja-asetus, artikla 12.
[78] Zanol, Czadilek, Lebloch 2018 s. 235.

Koska tietojen siirtäminen toiseen järjestelmään ei itsehallittavassa identiteetissä onnistu rekisterinpitäjän aloitteesta[79], artiklan 15(2) kohdan mukainen oikeus saada ilmoitus suojatoimista, jotka toteutetaan siirrettäessä tietoja kolmansiin maihin ei saa edes teoreettisia toteutumistilanteita.

Artiklan 15(3) kohdan mukainen rekisterinpitäjän velvollisuus toimittaa jäljennös käsiteltävistä henkilötiedoista on itsehallittavan identiteetin kannalta erikoinen, sillä tämä jäljennös sisältäisi tiedot niistä henkilötiedoista, joihin rekisteröity on sallinut rekisterinpitäjälle pääsyn. Jos rekisteröity vaatii rekisterinpitäjää toimittamaan kopion näistä tiedoista, se lienee teknisesti kyllä mahdollista. Koska kohdan sanamuoto on ehdoton ”toimitettava” eikä sisällä poikkeusta[80], nähdäkseni rekisterinpitäjän olisi rekisteröidyn niin vaatiessa toimitettava sähköisessä tai muussa muodossa jäljennös näistä tiedoista.

4.2 Oikeus tietojen oikaisemiseen

Artiklassa 16 todetaan rekisteröidyn oikeus vaatia rekisterinpitäjää oikaisemaan virheelliset ja epätarkat henkilötiedot sekä rekisteröidyn oikeus saada puutteelliset henkilötiedot täydennettyä.[81] Oikaisuoikeuden taustalla on henkilötietojen täsmällisyysperiaate, jonka mukaan ”on toteutettava kaikki mahdolliset kohtuulliset toimenpiteet sen varmistamiseksi, että käsittelyn tarkoituksiin nähden epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä”.[82] Tarkoituksena on siis se, ettei virheellisiä tai epätarkkoja henkilötietoja käsitellä.

Itsehallittavassa identiteetissä käsiteltävien henkilötietojen sisältö tulee häneltä itseltään tai kolmansilta osapuolilta näiden varmentamina.[83] Koska rekisterinpitäjä ei voi muokata näitä rekisteröidyltä vastaanotettuja henkilötietoja, rekisterinpitäjällä ei ole mahdollisuutta oikaista virheellisiä henkilötietoja. Tästä huolimatta rekisteröidyllä on artiklan 16 mukainen oikeus vaatia oikaisua. Oikaisuvaatimuksen saatuaan rekisterinpitäjän toimintamahdollisuudeksi jää nähdäkseni ainoastaan oikaisuvaatimuksen kohteena olevan tiedon käsittelyoikeuden peruuttaminen ja tietojen oikaisun jälkeinen uuden käsittelyoikeuden pyytäminen rekisteröidyltä. Näin toiminta on täsmällisyysperiaatteen mukaista, sillä rekisterinpitäjä tekee mahdolliset kohtuulliset toimenpiteet virheellisten tai epätarkkojen

[79] Ks. kappale 4.3.
[80] EU:n tietosuoja-asetus, artikla 15(3): ”Rekisterinpitäjän on toimitettava jäljennös käsiteltävistä henkilötiedoista. Jos rekisteröity pyytää useampia jäljennöksiä, rekisterinpitäjä voi periä niistä hallinnollisiin kustannuksiin perustuvan kohtuullisen maksun. Jos rekisteröity esittää pyynnön sähköisesti, tiedot on toimitettava yleisesti käytetyssä sähköisessä muodossa, paitsi jos rekisteröity toisin pyytää.”
[81] EU:n tietosuoja-asetus, artikla 16.
[82] EU:n tietosuoja-asetus, artikla 5(1)(d).
[83] Tästä tarkemmin ks. kappale 2.1.

henkilötietojen käsittelyn lopettamiseksi ja virheellisten henkilötietojen käsittely päättyy. Myös esityöt tukevat tätä tulkintaa, sillä oikeuksina virheellisten tietojen oikaisu ja poistaminen ovat vahvasti kytkettyjä toisiinsa useissa kohdissa.[84]

4.3 Oikeus siirtää tiedot järjestelmästä toiseen

Artiklan 20(1) kohdasta on luettavissa rekisteröidyn oikeus saada häntä koskevat henkilötiedot rekisterinpitäjältä ja siirtää nämä tiedot toiselle rekisterinpitäjälle, jos käsittely perustuu suostumukseen ja on toteutettu automatisoidusti.[85] Kohdan 1 muistuttaessa läheisesti artiklan 15 mukaista oikeutta päästä tietoon, kohta 2 kuvastaa rekisterinpitäjien välistä tiedonsiirtoa:

> ”Kun rekisteröity käyttää 1 kohdan mukaista oikeuttaan siirtää tiedot järjestelmästä toiseen, hänellä on oikeus saada henkilötiedot siirrettyä suoraan rekisterinpitäjältä toiselle, jos se on teknisesti mahdollista.”

Itsehallittavassa identiteetissä henkilötietoja hallinnoi rekisteröity itse, eikä rekisterinpitäjä pysty siirtämään näitä tietoja tätä järjestelmää käyttäen toiselle rekisterinpitäjälle.[86] Koska rekisterinpitäjä kuitenkin pystyy lukemaan näitä tietoja, tiedot on mahdollista kirjata käsin tai automaattisesti erilliseen henkilörekisteriin ja siirtää toiselle rekisterinpitäjälle. Tämä toimenpide mahdollistaisi kohdan 2 mukaisen tiedon siirtämisen, mutta olisi nähdäkseni rekisteröidyn yksityisyydensuojan kannalta paras vaihtoehto lähinnä tilanteissa, joissa toinen rekisterinpitäjä ei käytä itsehallittavan identiteetin henkilörekisteriä.[87] Rekisteröidyn yksityisyys toteutuu paremmin luomalla uusi hajautettu tunniste toiselle rekisterinpitäjälle ja antamalla tälle pääsy haluttuihin tietoihin, jolloin tietoja ei voida korreloida rekisterinpitäjien kesken.[88] Tietojen siirto-oikeutta ei siis voida teknisesti toteuttaa itsehallittavaa identiteettiä käyttäen, mutta koska rekisterinpitäjällä on pääsy rekisteröidyn tietoihin, hän voi laatia näistä kopion ja siirtää sen toiselle rekisterinpitäjälle käyttäen muita menetelmiä. Katson kuitenkin paremmaksi ratkaisuksi edellä mainitun uuden hajautetun tunnisteen luomisen.

[84] EU:n tietosuoja-asetus, resitaalit 39, 59, 65, 73 sekä 156.
[85] EU:n tietosuoja-asetus, artikla 20.
[86] Käyttäjä ei koskaan jaa allekirjoitusavaintaan, jolla uudet käsittelysuhteet luodaan. Windley 2016 s. 3.
[87] Tietosuoja-asetus ei edellytä samalla toimialalla toimivia rekisterinpitäjiä käyttämään yhteensopivia henkilörekistereitä, joten vastaava tilanne voisi syntyä myös toisen rekisterinpitäjän käyttäessä kilpailevaa itsehallittavan identiteetin järjestelmää, joka ei ole yhteensopiva. Lisätietoja teknisistä vaatimuksista ks. WP242 s.5.
[88] Windley 2016 s.3.

5 Johtopäätökset

Teknologia kehittyy huimaa tahtia, ja itsehallittavan identiteetin kehittäjiä on useita. Kun tutkimus on tehty tukeutuen vahvasti tämänhetkisen markkinajohtajan, Sovrin Foundationin, teknologiaan, tulee huomata, ettei edes Sovrin ole kirjoitushetkellä avannut palveluaan yleisölle saatavaksi, vaan on vasta beeta-asteella. Lähihistoria on osoittanut, että markkinajohtaja voi vaihtua nopeasti. Myös teknologian kehityssuunta voi muuttua radikaalisti ja nopeasti. Euroopan unionin tietosuoja-asetuksen tarkkarajaiset säännökset kuitenkin luovat pohjaa tietynsuuntaiselle kehitykselle tietojenhallintateknologioiden saralla. Yhteismarkkina-alueen ollessa suuri ja sääntelyn mahdollisimman yhdenmukainen on EU:n tietosuoja-asetuksen huomioon ottaminen tärkeää henkilötietojen käsittelyä koskevan teknologian kehitystyössä. Kun tämä teknologia aikanaan tulee käyttöön, lainsäätäjiltä ja -soveltajilta tulee edellyttää teknologian tuntemusta, sillä muutoin tulkinnat saattavat olla kummallisia tai ristiriitaisia.

Tutkimukseni perusteella itsehallittava identiteetti on yhteensopiva EU:n yleisen tietosuoja-asetuksen kanssa. Ristiriitaisuudet rajoittuvat lähinnä tiettyjen rekisteröidyn oikeuksien käyttämismuotoihin, mutta rekisteröidyllä on silti pääsy näihin oikeuksiinsa. Koska kyseessä oleva teknologia pystyy tietyiltä osin ylittämään selvästi asetuksessa vaaditun minimitason, mainitut ongelmat eivät estä itsehallittavan identiteetin käyttöä, mutta voivat edellyttää rekisterinpitäjältä ylimääräisiä toimia. Näiden johtopäätösten nojalla havaitaan, että EU:n yleinen tietosuoja-asetus ei kaikilta osin ole teknologianeutraali. Täydellisen teknologianeutraalisuuden saavuttaminen ei kuitenkaan laajan soveltamisalan ja teknologian nopean kehityksen vuoksi liene mahdollista.