Lohkoketju ja henkilötietojen hallinta liittyen MyData -näkökulmaan

Kirjallinen lausunto eduskunnan tulevaisuusvaliokunnalle 3.10.2018
Lausunnon antaja: Antti “Jogi” Poikola antti.poikola@aalto.fi, +358 44 337 5439

	Lausunto pohjautuu Liikenne ja viestintäministeriön kesäkuussa 2018 julkaisemaan *MyData - johdatus ihmiskeskeiseen henkilötiedon hyödyntämiseen* -julkaisuun (2. uudistettu painos), joka kokonaisuudessaan ladattavissa osoitteesta: http://urn.fi/URN:ISBN:978-952-243-554-5 Kuvamateriaali on julkaistu myös uudelleenkäytön sallivalla Creative Commons -lisenssillä osoitteessa: http://okf.fi/mydata-selvitys-2018

Sisällys

MyDatan tavoitteet: Minkä tulee muuttua?

Tiedon hyödyntäminen ja yksityisyydensuoja - molempi parempi

MyData hallitusohjelmassa ja tietopoliittisessa selonteossa

Kansainvälinen laajentuminen

Alustoista verkostoihin

Roolit MyData ekosysteemissä

Identiteetti- ja luottamusverkostot

Lohkoketjuteknologiat ja itsehallittava digitaalinen identiteetti

MyDatan tavoitteet: Minkä tulee muuttua?



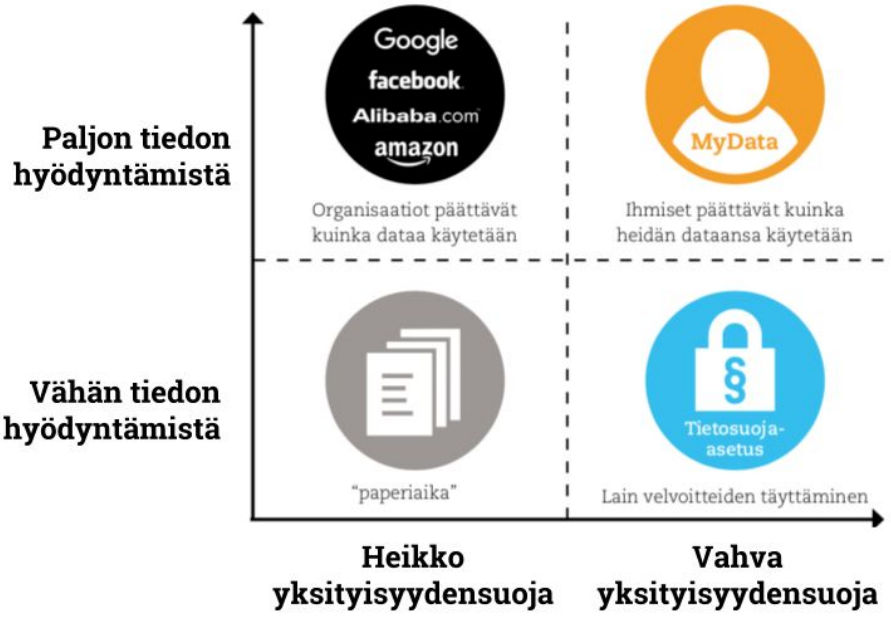
https://mydata.org/declaration

MyDatalla (myös omadata) tarkoitetaan yhtäältä ihmiskeskeisiä henkilötiedon hallinta- ja hyödyntämismalleja, joissa ihmisille annetaan oikeus omaan dataansa ja toisaalta tällaisten mallien mukaisesti hallinnoitua henkilötietoa. Lähtökohtana on, että ihmiset itse voivat hyödyntää, hallita ja luvittaa eteenpäin heistä kerättyä dataa kuten ostos-, liikkumis-, talous- tai terveystietoja. Ihmiskeskeisellä datan hallinnalla luodaan yhteentoimivuutta ja minimoidaan palvelulukkojen syntymistä dataa hyödyntävien alustojen kehittyessä. Malli sovittaa yksilön oikeudet ja korkeat tietosuojavaatimukset yhteen datan saatavuuden edistämisen ja liiketoiminnan kanssa.

MyData on kansainvälinen kehitysvaiheessa oleva ilmiö, malli ja tulevaisuusskenaario, jonka ympärille on kertymässä kasvavaa vauhtia teknologiaa ja liiketoimintaa. Mallin yleistyminen voi merkittävästi nopeuttaa datatalouden kehitystä ja avointen ekosysteemien syntymistä erityisesti vahvan tietosuojan ympäristöissä.

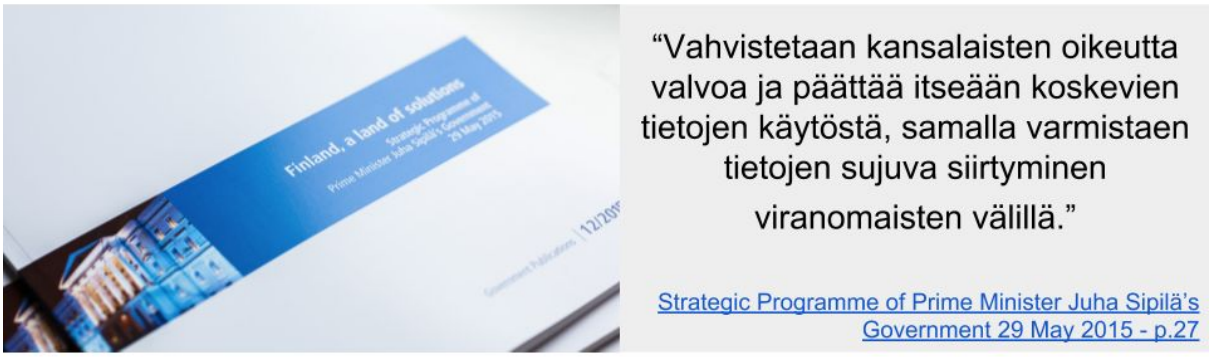
Kansainvälinen MyData-toimijoiden yhteisö julkaisi vuonna 2017 tavoitteet ja periaatteet, joiden kolme pääkohtaa ovat siirtyminen muodollisista oikeuksista käytännöllisiin oikeuksiin (2) laajentaminen tietosuojasta tiedolla voimauttamisen ja (3) siirtyminen suljetuista ekosysteemeistä avoimiin ekosysteemeihin.

Tiedon hyödyntäminen ja yksityisyydensuoja - molempi parempi

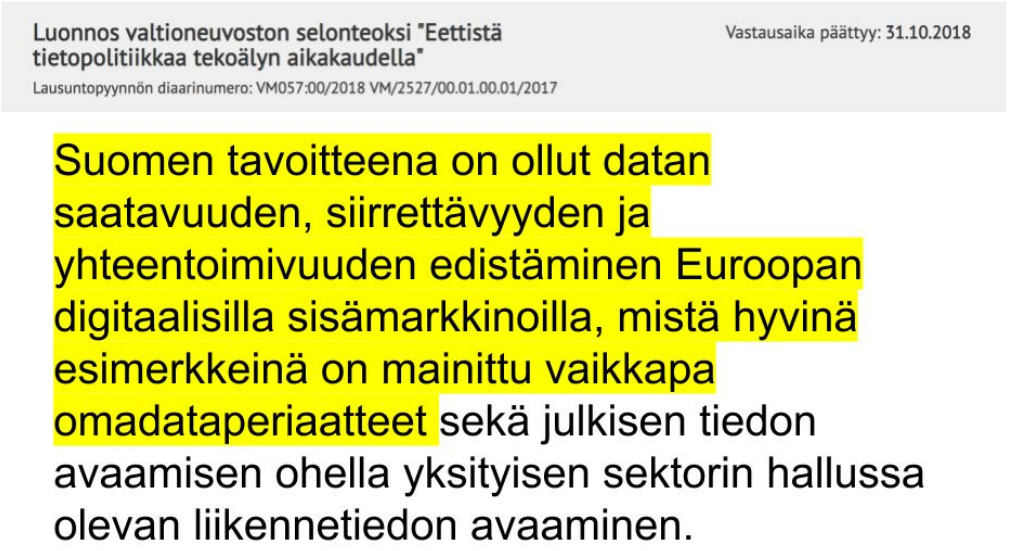


MyData-ajattelu tuo datan hyödyntämisnäkökulman tasavertaisena yksityisyydensuojan rinnalle. Perinteinen yksityisyyden suojaamisen lähtökohta on, että "mitä vähemmän henkilötietoa kerätään ja jaetaan, sen parempi". Tämä jättää kuitenkin huomiotta datasta yksilölle itselleen kertyvän arvon ja on vastakkainen henkilötiedon määrän ja käytön lisääntymisen megatrendille. MyData -ajattelun tavoitteena on henkilötietoon liittyvän liiketoiminnan kehitys ihmiskeskeisesti niin, etteivät monopolistiset skenaariot tietoyhteiskunnan tulevaisuudesta toteutuisi. Se mahdollistaisi henkilötiedon keräämisen ja käytön niin, että hyödyt maksimoidaan ja yksityisyydensuojan heikkeneminen minimoidaan. Keskeinen keino henkilöihin liittyvän datan hyödyntämisen ja tietosuojan yhteensovittamisessa on vahvistaa yksilöiden asemaa, oikeuksia ja käytännön mahdollisuuksia heitä koskevien tietojen hallintaan.

MyData hallitusohjelmassa ja tietopoliittisessa selonteossa

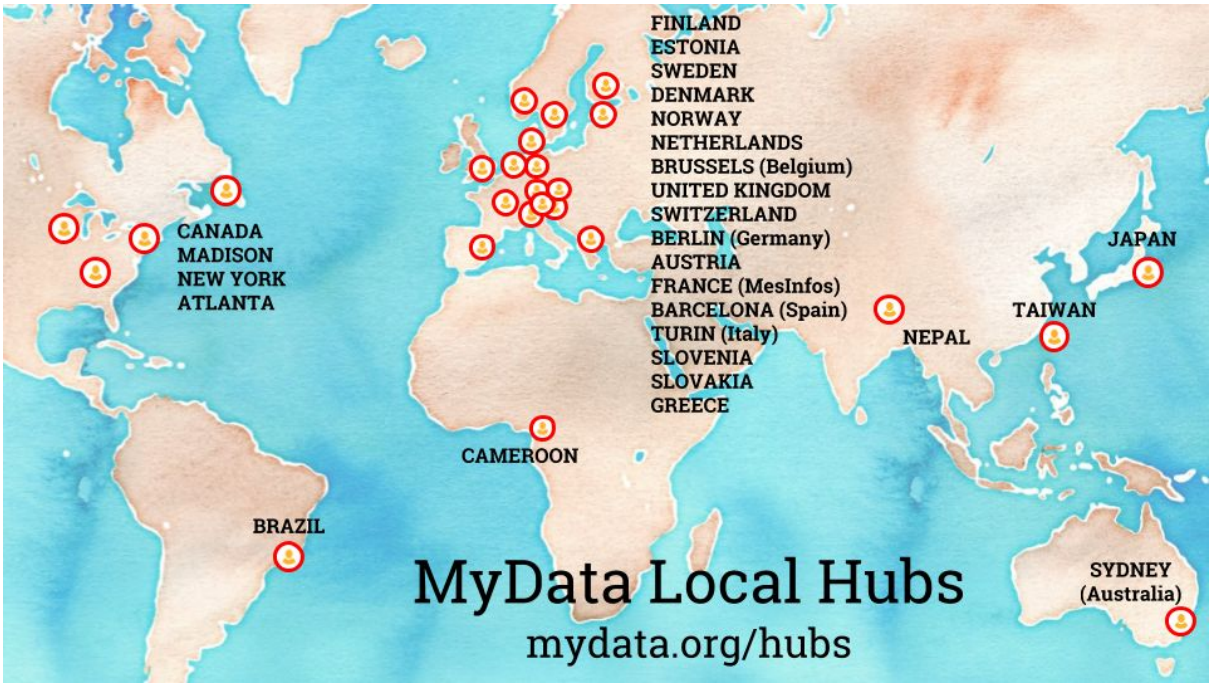


Vuonna 2015 Sipilän hallitus nosti aiheen hallitusohjelmaan seuraavalla linjauksella: “Vahvistetaan kansalaisten oikeutta valvoa ja päättää itseään koskevien tietojen käytöstä” (Valtioneuvosto 2015). Samana vuonna liikenne- ja viestintäministeriö yhdessä Aalto-yliopiston kanssa käynnistivät MyData-palvelupilotteja kehittävien suomalaisten yritysten foorumina toimivan MyData-allianssin. Allianssissa on mukana noin 40 suomalaista organisaatiota: suuria toimijoita kuten kauppaketjuja, pankkeja ja teleoperaattoreita, MyDataan liittyviä startupeja sekä tutkimuslaitoksia ja julkishallintoa (mydata.fi).



Lausuntokierroksella 31.10.2018 olevassa luonnoksesa valtioneuvoston selonteoksi “Eettistä tietopolitiikkaa tekoälyn aikakaudella” mainitaan suomen vahvuutena edelläkävijyys omadata-ajattelussa ja linjataan, että vahvistetaan yksilön oikeutta omien tietojen hallintaan eli omadataan. Lisäksi selontekoluonnoksesa huomioidaan: *“Tiedon laajan ja monipuolisen hyödyntämisen näkökulmasta on tiedon omistajuuden sijaan tärkeämpää keskustella oikeuksista käyttää tietoa, sillä tiedon arvo kasvaa vasta sitä käytettäessä.”*

Kansainvälinen laajentuminen



Kansainvälisten tapaamisten ja MyData-konferenssien ympärille on muodostunut kasvava globaali yhteisö, jolla on paikallistoimintaa jo yli 20:ssä paikallisessa MyData-hubissa (mydata.org). Euroopan ulkopuolella hubeja on mm. Japanissa, Brasiliassa ja Pohjois-Amerikassa. Suurin osa hubeista on toistaiseksi vielä pieniä ja vapaamuotoisia paikallisyhteisöjä, mutta esimerkiksi Hollannissa, Ranskassa ja Tanskassa toiminta on tavoitteellista ja säännöllistä ja mukana on paikallisia yrityksiä vastaavasti kuin suomalaisessa MyData-allianssissa. Kansainvälinen verkoston tavoitteena on perustaa MyDatan edistämiseen ja yhteistoiminnan rakenteita kehittämään MyData Foundation, jonka kotipaikaksi on tulossa Suomi (perustamiskokous 11.10.2018 Helsingissä).

Suomella on hyvä mahdollisuus asemoitua kansainväliseksi ajatusjohtajaksi henkilötiedon hallinnan ja ihmiskeskeisen datatalouden alueilla. Tämä edellyttää aktiivista verkostoitumista ja kansainvälistymistä esimerkiksi EU-tason yhteistyöhankkeissa ja kansainvälisillä standardointi- ja teknologiafoorumeilla. Esimerkiksi Sitran IHAN®-hankkeessa on otettu lähtökohdaksi EU:n alue ja käynnistetään standardointityö CEN-CENELEC:ssä.

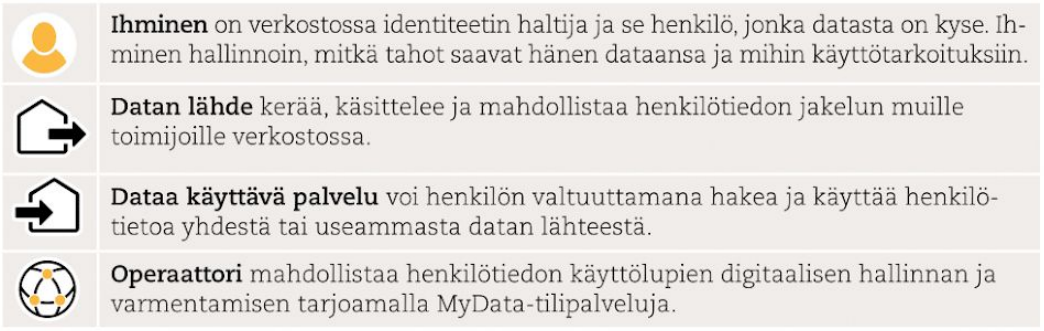
Alustoista verkostoihin



Teknisesti MyDatan on visio globaalista ihmiskeskeisen henkilötiedon jakamisen infrastruktuurista, joka pohjautuu alustojen sijaan verkostoihin. Organisoitumistapa vaikuttaa siihen, kuinka helposti hyödynnettävää henkilötieto on, kuinka läpinäkyvää tiedon käyttö on, kuinka hyvin rakenteet tukevat avointa kilpailua sekä kuinka ihmiskeskeistä henkilötiedon hyödyntäminen tulevaisuudessa on. Olennaista on, että kontrolli omaan dataan on ihmisillä itsellään, infrastruktuuripalvelujen tarjoajia on useita ja palvelut ovat yhteentoimivia ja vaihdettavissa.

Nykyisessä infrastruktuurittomassa API-ekosysteemissä, jos palvelujen määrä kasvaa, niin yhteyksien määrä kasvaa vielä nopeammin (vasen). Datan hallinnan keskittäminen helpottaa sovellusten kehittämistä, mutta eri alustatoimijoilla ei ole lähtökohtaisesti motiivia pyrkiä alustojen väliseen yhteentoimivuuteen (keskellä). Alustamalliin verrattuna MyData-infrastruktuuri on kestävä ja joustava, koska se ei ole riippuvainen yksittäisestä organisaatiosta (oikealla).

Roolit MyData ekosysteemissä



Henkilötiedon jakamisen ekosysteemissä on neljä roolia: ihminen, datan lähde, dataa käyttävä palvelu sekä operaattori. Toimijat voivat olla samanaikaisesti useammissa rooleissa. Esimerkiksi yritykset ovat tyypillisesti sekä datan lähteitä että dataa hyödyntävien palvelujen tarjoajia. Myös muissa rooleissa olevat toimijat voivat ottaa lisäksi operaattorin roolin ja ylläpitää itse MyData-tiliä, jota kautta ne kytkeytyvät verkostoon.

Identiteetti- ja luottamusverkostot



Sähköinen luotettava ja helposti käytettävä identiteetti on tärkeä mahdollistaja toimivalle henkilötiedon ekosysteemille. Yksittäisistä identiteetintarjoajasta riippumattomat hajautetut identiteettiratkaisut mahdollistavat MyData-mallissa palvelujen vaihdettavuuden sekä tunnistautumis- ja käyttöoikeusratkaisujen yhteentoimivuuden eri palvelujen välillä.

Tiedon luovutus rajapintojen kautta edellyttää, että ihmiset ja organisaatiot pystyvät tunnistautumaan ja antamaan lupia tietojensa siirtoon. Mikäli luottamus toisen osapuolen sähköiseen identiteettiin puuttuu, organisaatiot eivät uskalla luovuttaa mitään tietoja rajapintojen kautta. Tämä ei kuitenkaan tarkoita, että kaikissa tapauksissa pitäisi käyttää esimerkiksi pankki- ja mobiilitunnisteisiin pohjautuvaa vahvaa tunnistautumista.

MyData-malli on verkostopohjainen, eikä siinä oleteta, että kaikki ihmiset, datan lähteet ja dataa käyttävät palvelut kytkeytyisivät yhteen datan jakamisen alustaan. Keskeinen ajatus on, että ihmisille on tarjolla useita yhteentoimivia, mutta kilpailevia tilipalveluja. Tämä edellyttää, että identiteetinhallinnan, tunnistautumisen ja tilitietoon liittyvän tietoturvan kysymykset ratkaistaan tiettyyn tasoon saakka yhteisen mekanismin mukaisesti, muutoin MyData-tilin vaihtaminen palveluntarjoajalta toiselle ja yhteentoimivuus ei ole mahdollista. Yhteinen perusta voi kuitenkin olla ohut, mikäli se mahdollistaa tarkemmin määriteltyjen luottamuspalvelujen rakentamisen perustan päälle.

Lohkoketjuteknologiat ja itsehallittava digitaalinen identiteetti

Lohkoketjuteknologiat mahdollistavat hajautettujen sähköisen identiteetin järjestelmien kehittämisen. Näissä identiteetin omistaja voi hallita omaa digitaalista identiteettiään itsenäisesti ulkoisista identiteetintarjoajista riippumatta. Itsehallittavan identiteetin (self sovereign identity) mallissa luonnollinen henkilö tai organisaatio hallinnoi itse omia tietojaan ja niiden jakamista.

Itsehallittavan identiteetin kehittäjiä ovat muiden muassa Sovrin, uPort, Veres One ja Blockstack. Eri kehittäjien toteutukset poikkeavat toisistaan, mutta yhteistä kaikille on, että luotettavuus itsehallittaviin henkilötietoihin toteutetaan lohkoketjuteknologialla.

Henkilötietoja ei talleta lohkoketjuun, vaan lohkoketjua ja krytografisia tunnisteita käytetään siihen, että tiedon vastaanottaja voi varmistaa muuta kautta lähetetyn tiedon paikkansapitävyyden ja voimassaolon. Itsehallittavan identiteetin malli nähdään keskeisenä teknisenä mahdollistajana tulevaisuuden MyData-infrastruktuurissa, mutta toistaiseksi (kesällä 2018) tarjolla olevat teknologiat eivät ole vielä kypsiä laajamittaisiin toteutuksiin.