AURORA-VERKON TIETOSUOJAN VAIKUTUSTENARVIOINTI

Aurora-verkon tietosuojan vaikutustenarviointi –dokumentaatio (liite 4)

Väestörekisterikeskus

VERSION HALLINTA

versionro	mitä tehty	pvm/henkilö
0.1	Tuotettu dokumentaatio	30.1.19/EL
1.0	Muokattu kommenttien pohjalta	25.2.2019/EL

Sisällysluettelo

KEH/Aurora esiselvitys 28.2.2019

AURORA-VERKON TIETOSUOJAN VAIKUTUSTENARVIOINTI

Aurora on tekoälyjen/autonomisten sovellusten muodostama hajautettu palveluverkko, jolla luodaan edellytyksiä yhteiskunnan palvelujen ihmiskeskeiselle ja ennakointikykyiselle tarjoamiselle. Väestörekisterikeskuksen tehtävänä on toteuttaa korkean tason arkkitehtuuri sekä tekninen perusratkaisu älykkäiden agenttien verkolle. Alusta toteutetaan toimittajariippumattomana ratkaisuna siten, että se mahdollistaa sekä yksittäisten toimijoiden yksinkertaisen liittymisen Aurora-verkkoon että uusien palvelujen ja palveluketjujen rakentamisen alustan päälle. Tekniseen perusratkaisuun kuuluu myös Auroran tietoturva- ja tietosuojaratkaisujen selvittäminen ja testaaminen.

Tietosuojan vaikutustenarviointi eli DPIA (Data Privacy Impact Assesment) on tietosuoja-asetuksen 35 artiklan mukainen arviointi, jonka tarkoituksena on kartoittaa suunniteltujen käsittelytoimien vaikutukset henkilötietojen suojalle. Vaikutustenarviointi tulee tehdä tilanteessa, joissa käsittelytoimiin todennäköisesti liittyy luonnollisten henkilöiden oikeuksiin ja vapauksiin liittyvä korkea riski. Asetuksen mukaan joissain olosuhteissa voi olla järkevää ja taloudellista laatia tietosuojaa koskeva vaikutustenarviointi, jossa tarkastellaan asioita laajemmin kuin yhden projektin kannalta, esimerkiksi kun viranomaiset tai julkishallinnon elimet aikovat luoda yhteisen sovelluksen tai käsittelyalustan tai kun useat rekisterinpitäjät aikovat ottaa käyttöön yhteisen sovelluksen tai käsittely-ympäristön kokonaista teollisuuden alaa tai segmenttiä tai jotakin laajalti käytettävää horisontaalista toimintoa varten.

Vaikutustenarvioinnin johdosta voidaan tehdä tarvittavia korjaavia toimenpiteitä tietosuojan vaatimusten täyttämiseksi. Raportti toimii hyödyllisenä materiaalina toimijoille, jotka osallistuvat arvioinnin kohteena olevan palvelun kehittämiseen. Se toimii myös lähtökohtana sellaisen toimintasuunnitelman laatimiselle, mikä tarvitaan sen varmistamiseksi, että kaikki korjaavat kontrollitoimenpiteet on toteutettu. Vaikutustenarviointi tulisi tehdä säännöllisesti uudelleen ja tarvittaessa päivittää, jotta arvioinnin tuloksena saadut korjaukset on tehty asianmukaisesti.

1 Aurora-verkon tietosuojan vaikutustenarviointi 25.1.2019

Aurora-verkon vaikutustenarviointi tehtiin Väestörekisterikeskuksen tiloissa 25.1.2019. Vaikutustenarvioinnissa läsnä olivat VRK:lta Pekka Ristimäki (tietoturvapäällikkö), Emilia Laitala (erityisasiantuntija), Noora Kallio (johtava asiantuntija) sekä Antti Ahokas (tietoturva-asiantuntija). Cybercomilta paikalla oli Antti Hahto. Noora Kallio sekä Antti Ahokas osallistuivat Skypen välityksellä.

Vaikutustenarviointi suoritettiin VRK:n vakiomuotoisen kysymyspatteriston avulla, jossa käydään läpi tietosuojan vaikutustenarvioimiseksi oleelliseksi katsotut kysymykset. Väestörekisterikeskus on suorittanut myös muihin palveluihinsa vaikutustenarviointia, joten prosessi on sama palvelusta riippumatta.

Tietosuojan vaikutustenarvioinnissa arvioitiin VRK:n kehitteillä olevaa Aurora-verkkoa. Kehitystyö tehdään Cybercomin kehittäjien toimesta VRK:n ohjauksessa. Tällä hetkellä ei ole vielä tuotantoversioista Aurora-verkkoa, vaan kaikki toiminta tapahtuu demo-ympäristössä. Lisäksi kehitystyö on vielä olennaisesti kesken, joten tämän hetken Aurora-ympäristössä ei käsitellä oikeita henkilötietoja. Aurora-verkon tämän hetken tavoite on muodostaa rajapinnat, erityisesti älykkäiden agenttien, kuten bottien väliset ja ulkoiset rajapinnat siten, että asiakas keskustelee Aurora-

verkoston älykkäiden agenttien kanssa puhumalla ja vähintään chat-dialogissa kirjoittamalla. Vaikutustenarviointi on tehty tämän hetken tietojen ja käsitysten mukaan siitä, mitä Aurora-verkko on nyt ja mitä se tulee olemaan. Tässä vaikutustenarvioinnissa esitetyt tiedot voivat siis muuttua, mikäli toteutus muuttuu kehityksen edetessä. Tällöin vaikutustenarviointi tulee tehdä tarpeen mukaan uudelleen ja arvioida tietosuojan toteutumisen vaikutukset sen hetkiseen toteutukseen.

Vaikutustenarviointi suuntautuu siten vain Aurora-verkkoon teknisenä ratkaisuna, ei organisaatioihin, jotka toimivat tai tulevat toimimaan Aurora-verkossa palveluntarjoajina. Vaikutustenarvioinnin tulee tehdä sen organisaation toimesta, joka käsittelee henkilötietoja. Vaikutustenarvioinnissa otetaan kantaa myös siihen, miten toteutettavana olevan Aurora-verkon palveluntarjoajien ekosysteemien tietosuojaan tulisi kiinnittää huomiota, jotta kyseinen ekosysteemi voitaisiin toteuttaa. Vaikka ekosysteemien käsittelemät henkilötiedot eivät ole Aurora-verkon käsittelemää tietoa, ekosysteemien ja palveluntarjoajien tietosuojaratkaisut ovat olennaisia Aurora-verkon toteutumisen kannalta.

1.1 Kerätyt henkilötietotyypit

Tietosuoja-asetuksen määrittelyn mukaan henkilötiedolla tarkoitetaan *kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja; tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella.* Henkilötiedon käsite on siten suhteellisen laaja ja jo yksittäisestä tiedosta, joka on yhdistettävissä luonnolliseen henkilöön, tulee henkilötietoa.

Aurora-verkkoon liittyneet palveluntarjoajat tarjoavat palvelujaan kansalaisille elämäntapalähtöisesti. Verkossa asioiminen voi siten liittyä mihin tahansa ihmisen elämän vaiheeseen, sitä ei ole Aurora-verkossa teknisesti erikseen määritelty. Kerätyt henkilötietotyypit ovat henkilön itsensä antamaa tietoa sekä mahdollisesti organisaatioiden rekistereissä jo olevaa henkilötietoa. Kerättävää henkilötietotyyppiä ei tässä vaiheessa ole tarkasti määritelty, sillä Aurora-verkossa olevien palveluntarjoajien toimesta voidaan lähtökohtaisesti käsitellä mitä tahansa henkilön elämään liittyviä tapahtumia.

Tietosuoja-asetuksen 5 artiklan mukaisen käyttötarkoitussidonnaisuusperiaatteen mukaan henkilötiedot on kerättävä *tiettyä, nimenomaista ja laillista tarkoitusta varten, eikä niitä saa käsitellä myöhemmin näiden tarkoitusten kanssa yhteensopimattomalla tavalla; myöhempää käsittelyä yleisen edun mukaisia arkistointitarkoituksia taikka tieteellisiä tai historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten ei katsota 89 artiklan 1 kohdan mukaisesti yhteensopimattomaksi alkuperäisten tarkoitusten kanssa ("käyttötarkoitussidonnaisuus").*

Käyttötarkoitussidonnaisuus edellyttää, että rekisterinpitäjä ennen henkilötietojen keräämistä määrittelee, mitä henkilötietoja on tarkoitus kerätä ja mihin käyttötarkoitukseen. Rekisteröidylle on ilmoitettava kerättävät henkilötiedot hänen asioidessaan palvelussa. Aurora-verkko itsessään ei kerää eikä käsittele henkilötietoja, mutta Aurora-verkon sisällä toimivat palveluntarjoajat sen sijaan käsittelevät ja keräävät henkilötietoa tietyissä tilanteissa, joten palveluntarjoajien tulee määritellä käyttötarkoitussidonnaisuusperiaatteen mukaan se, mihin käyttötarkoitukseen henkilötietoja tullaan keräämään. Aurora-verkko ei aseta teknisesti rajoituksia henkilötiedon keräämiselle palveluntarjoajien toimesta.

Käyttötarkoitussidonnaisuus on tietosuoja-asetuksen mukaan ehdoton, eikä rekisterinpitäjä voi siitä poiketa. Aurora-verkon ekosysteemien toimintaan liittyy olennaisesti se, että verkko oppii tarjoamaan asiakaslähtöisesti palveluita eikä siihen tarvittavaa henkilötietoa voida välttämättä etukäteen määritellä. Tämä ei kuitenkaan ole tietosuoja-asetuksen mukaista, sillä sellainen tietovaranto ei ole vaatimustenmukainen, jossa on kerättynä/säilytettävänä tai muutoin käsiteltävänä aitoa henkilötietoa, mutta jota ei sillä hetkellä hyödynnetä tiettyyn tai tiettyihin käyttötarkoituksiin. Aurora-verkoston henkilötietojen käyttötarkoitussidonnaisuus ja kerättävät henkilötiedot tulisi voida määritellä etukäteen.

Verkko ei vaadi toimiakseen kokonaisuutena yhtään palvelua, joka käsittelee henkilötietoja. Lisäksi Aurora-verkko toteutetaan teknisesti siten, että verkossa toimiva palveluntarjoaja ei toimiakseen lähtökohtaisesti tarvitse asiakkaan henkilötietoja eikä asiakkaan tarvitse tunnistautua chat-palveluun. Tunnistettavuus tarkoittaa, ettei tunnistamista ole vielä tapahtunut, mutta se on kuitenkin mahdollista, esimerkiksi yhdistämällä käsiteltävään tietoon muita tietoja. Henkilötiedot on yleensä kerätty ensin tunnistettavassa muodossa. Näin ollen niiden anonymisointi on jatkokäsittelyä ja tämän käsittelyn tulee lähtökohtaisesti täyttää käyttötarkoitussidonnaisuuteen liittyvä yhteensopivuuden vaatimus.

Henkilötietoja käsitellään edellä mainituissa ekosysteemeissä. Kuten palvelun tarkoitus -kappaleessa tulee ilmi, kerättävää henkilötietoa ei tämän hetken tietojen mukaan käsitellä Aurora-verkon toimesta. Verkko voi sisältää kolmannen osapuolen palveluja, jotka käsittelevät henkilötietoja. Palvelut noudattavat verkon ylätasojen asettamia käsittelyyn liittyviä rajoitteita liittyessään valitsemaansa ylätasoon. Jokaisella palvelulla on taho, joka on laillisesti vastuussa palvelun toiminnasta.

1.2 Palvelun tarkoitus

Aurora-verkko on palveluverkosto, johon liittyneet organisaatiot toimivat palveluntarjoajina. Palveluntarjoajat muodostavat ekosysteemejä, joihin liittyy myös muita palveluntarjoajia. Ekosysteemejä voi olla useampia, jotka toimivat Aurora-verkossa. Yhdessä ekosysteemissä voi olla useampia toimijoita sekä julkisen hallinnon sektorilta että yksityiseltä puolelta. Ekosysteemi voi myös muodostua vain julkisen hallinnon toimijoista tai vaihtoehtoisesti vain yksityisen sektorin toimijoista. Palveluntarjoaja, johon on liittynyt muita palveluntarjoajia on ns. ”pääorganisaatio”, jonka luokse asiakas tulee asioimaan. Asiakkaalle asiointi näyttäytyy siten, että hän tulee asioimaan kyseiseen organisaatioon, jonka taustalla on siihen liittyneitä muita palveluntarjoajia. Asiakas ei siis tule asioimaan Aurora-verkkoon, vaan asiakas tulee asioimaan tietyn Aurora-verkossa olevan palveluntarjoajan luokse. Asiakas keskustelee palveluntarjoajan chat-ikkunassa liittyen hänen asiaansa.

Aurora-verkon tavoitteena on tuoda yhteen palveluntarjoajia ja tarjota optimaalinen kokonaispalvelukokemus loppukäyttäjälle. Asiakkaan tarpeesta riippuen kunkin tapauksen käsittelyn yhteydessä voi olla mukana joko yksi tai useampia palveluntarjoajia. Asiakkaan asioidessa palveluntarjoajan kanssa, ei henkilötietoja välitetä Aurora-verkossa, vaan henkilötietojen käsittely tapahtuu suoraan palveluntarjoajien toimesta. Aurora-verkko on tekninen alusta, joka mahdollistaa ekosysteemien toimimisen, mutta verkko itsessään ei tämän hetken toteutuksen ja tietojen mukaan käsittele henkilötietoja.

Ennen henkilötietojen keräämistä rekisterinpitäjän on määriteltävä tietosuoja-asetuksen 5 artiklan periaatteiden mukaiset henkilötiedon käsittelyä koskevat vaatimukset. Näitä periaatteita ovat lainmukaisuus, kohtuullisuus ja läpinäkyvyys, käyttötarkoitussidonnaisuus, tietojen minimointi, täsmällisyys, säilytyksen rajoittaminen sekä eheys ja luottamuksellisuus.

Lainmukaisuus, kohtuullisuus ja läpinäkyvyys edellyttävät, että henkilötietoja on käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi. Henkilötietojen käsittelylle tulee olla lakiperuste, eli henkilötietoja voidaan käsitellä vain tietosuoja-asetuksen 6 artiklan nojalla. Läpinäkyvyyden vaatimus edellyttää, että rekisterinpitäjä käsittelee henkilötietoja siten, että asiakkaalle annetaan kaikki tarvittava henkilötietojen käsittelyyn liittyvä tieto. Henkilötietojen käsittelyyn liittyvä läpinäkyvyys toteutuu muun muassa tietosuojaselosteen kautta, johon kirjataan henkilötiedon käsittelyn perusteet sekä rekisteröidyn oikeudet.

Aurora-verkossa olevat palveluntarjoajat ovat velvollisia riittävällä tavalla informoimaan asiakasta heidän henkilötietojensa käsittelystä käsittelemiensä henkilötietojen osalta. Lisäksi muita periaatteita tulee noudattaa tietosuoja-asetuksen mukaisesti, esimerkiksi kerättävien henkilötietojen määrä tulee määritellä palveluntarjoajien toimesta ja henkilötietojen käsittelylle on määriteltävä menettelytavat. Koska Aurora-verkko itsessään ei henkilötietoja käsittele, vastuu henkilötiedon lainmukaisesta käsittelystä on Aurora-verkossa toimivilla palveluntarjoajilla.

Tietojen minimoinnin osalta Aurora-verkon toiminta on toteutettu siten, että palveluntarjoaja ei lähtökohtaisesti tarvitse henkilötietoa tarjotakseen palvelua asiakkaalle. Lisäksi henkilötietoa pyritään käsittelemään siten, että käyttäjää ei ole tunnistettavissa annetuista tiedoista. Palvelun käyttö ei edellytä tunnistautumista tai muuta vastaavaa identifiointia. Aurora-verkossa asiointi voi tapahtua neljällä eri tasolla; anonyymisti (taso 1), kuulumalla tiettyyn ryhmään (taso 2) tai mahdollisesti tulevaisuudessa heikosti taikka vahvasti tunnistautumalla (taso 3 ja 4). Tunnistautumisratkaisua ei ole tämän hetken versiossa toteutettu, mutta mikäli se tullaan toteuttamaan, tulee vaikutustenarvioinnin kannalta käydä uudelleen läpi se, vaikuttaako tunnistautuminen jotenkin Aurora-verkon toimintaan henkilötiedon käsittelyn suhteen.

Asiakkaan asioidessa anonyymisti palveluntarjoajan palvelussa, henkilöstä ei kerätä mitään henkilötietoa ja tällöin palvelu pohjautuu yleiseen neuvontaan. Henkilöstä ei tarvita mitään henkilöön itseensä liittyvää tietoa, vaan asiointi voi tapahtua täysin anonyymisti. Aurora-verkon yksi mahdollinen toiminnallisuus on henkilön profilointi siten, että profilointia käytetään häivyttämään alkuperäinen yhteys luonnolliseen henkilöön ja käsittelemään näin anonyymiä henkilötietoa. Tällöin kyseessä olisi 2-taso. Profiloinnissa anonyymit henkilötiedot profiloidaan eri kategorioihin siten, että luonnollinen henkilö voi kuulua kyseiseen kategoriaan. Kun henkilö liitetään johonkin verkossa olevaan kategoriaan, tällöin tiedetään henkilön ID (user ID tai user group ID). ID ei kuitenkaan ole yhdistettävissä suoraan luonnolliseen henkilöön, vaan se on satunnainen numero. User group ID tarkoittaa sitä, että henkilö kuuluu johonkin tiettyyn ryhmään, jonka avulla palveluita voidaan kohdistaa paremmin asiakkaille. Tällä tavalla voidaan personoida palveluita, vaikka henkilöstä itsestään ei olisikaan tallennettu varsinaista henkilötietoa palveluntarjoajan tietoihin. Lähtökohtaisesti user ID ei ole henkilötietoa, sillä se ei ole yhdistettävissä luonnolliseen henkilöön. Toisaalta taas voidaan esittää kysymys siitä, onko sellainen anonyymi tieto henkilötietoa, joka lopulta tiedetään kuuluvan jollekin henkilölle, henkilötietoa. Käytännössä myös sen määrittäminen, onko data riittävästi anonymisoitu vai onko se vielä henkilötietoa, on vaikeaa. Vaikutustenarvioinnin yhteydessä todettiin, että asiaa on syytä vielä selvittää tarkemmin, sillä asia on hie-

man tulkinnanvarainen. Riippumatta siitä, onko user ID tai user group ID henkilötietoa, se ei vaikuta Aurora-verkon vaikutustenarviointiin, sillä Aurora-verkko ei käsittele taikka säilytä user ID tietoa, vaan sekin tapahtuu palveluntarjoajien toimesta. Profilointi tehdään kolmannen osapuolen palveluilla; itse verkko ei sitä suorita. Mahdollinen käyttäjädata tallennetaan kolmannen osapuolen palveluihin, jotka ovat sen asianmukaisesta varastoinnista vastuussa. Verkon sisällä (palveluiden välillä) ei liikuteta käyttäjädataa, ainoastaan henkilön anonymisoitua profiilia joka ei ole yhdistettävissä luonnolliseen henkilöön.

Joissakin tapauksissa kolmannen osapuolen palvelu voi tarvita alkuperäistä ja yksilöivää dataa käyttäjästä. Kolmannen osapuolen tallennuspalvelut noudattavat näissä tapauksissa omadataperiaatteita, kuten luvitusmekanismin käyttöä ja vaativat kirjautumista. Heikolla kirjautumisella käyttäjä voi halutessaan luovuttaa ei-kriittistä dataa (taso 3), viranomaisdatan ja arkaluonteisen datan (sisältää erityistä henkilötietoa) (taso 4) luovuttaminen vaatii vahvan kirjautumisen. Kirjautumiset tehdään kolmannen osapuolen palveluilla.

Mikäli palveluntarjoaja käsittelee henkilötietoja henkilön antaman suostumuksen nojalla, tulee suostumuksista olla erillinen rekisteri. Mikäli rekisteröity myöhemmin peruu antamansa suostumuksen, tulee palveluntarjoajalla olla menettely sille, miten henkilötiedot poistetaan. On kuitenkin huomattava, ettei viranomainen lähtökohtaisesti voi tietosuoja-asetuksen mukaan käsitellä henkilötietoja suostumuksen perusteella. Omadataan liittyvät tekniset toteutukset ja omadatan toteuttaminen Aurora-verkossa on tämän hetken tietojen mukaan vielä avoinna, joten vaikutustenarvioinnissa ei sen osalta voida tehdä tarkempaa selvitystä.

1.3 Tietojen laatu ja elinkaari

Tietojen laatuun liittyy olennaisena osana se, että kerättävät henkilötiedot on valittu, henkilötietojen sijainnit sekä tieto sijaintitiedon käsittelystä tai henkilötiedon rikastamisesta on määritelty. Myös alaikäisten henkilöiden henkilötietojen sekä erityisten henkilötietojen kerääminen ja käsittely tulee olla ennalta tiedossa ja niiden osalta tulee noudattaa tietosuoja-asetuksen 8 sekä 9 artiklan mukaista menettelyä sekä tarvittaessa kansallista tietosuojalainsäädäntöä.

Henkilötiedon elinkaari tulee määritellä ennen kuin rekisterinpitäjä aloittaa tiedon keräämisen. Elinkaaren määrittelyyn liittyy henkilötiedon säilytysaikojen määrittely, tiedon poistamisen menettelyn määrittely, on oltava olemassa varmuus varmuuskopioiden poistamisesta tiedon poiston yhteydessä ja evästeille tulee olla määriteltynä säilytysajat.

Aurora-verkko ei määrittele tiedon laatua taikka tiedon elinkaarta. Toimiakseen Aurora-verkossa palveluntarjoajan ei lähtökohtaisesti tarvitse käsitellä sijaintitietoa eikä henkilötietoja tarvitse rikastaa. Jotta asiakas voidaan määritellä kuuluvaksi tiettyyn ID group:iin tai hänelle voidaan määritellä user ID, käytetään evästeitä. Evästeiden käsittely ja säilyttäminen tapahtuu palveluntarjoajien toimesta, eikä Aurora-verkko rajoita tai säilytä evästeitä. Se kuitenkin mahdollistaa evästeiden keräämisen, joten palveluntarjoajan tulee määritellä evästeiden elinkaari. Myös muut henkilötiedot säilytetään palveluntarjoajan määrittelemällä tavalla palveluntarjoajan järjestelmissä, joten palveluntarjoajan on määriteltävä käsittelemiensä henkilötietojen elinkaari. Aurora-verkko mahdollistaa henkilötiedon keräämisen, mutta ei itse sitä tee.

1.4 Tiedonsiirrot ja rajat ylittävä käsittely

Aurora-verkkoon voi tulevaisuudessa liittyä suostumustenhallintaa, joka tarkoittaa sitä, että asiakas voi antaa suostumuksensa siihen, että hänen henkilötietojaan välitetään edelleen sellaisille toimijoille, joilla ei ole lainsäädäntöön perustuvaa oikeutta käsitellä hänen henkilötietojaan. Tällöin käsittelyperusteeksi muodostuu suostumus, johon liittyy tietosuoja-asetuksen asettamia vaatimuksia siihen, mitä suostumusta pyytäessä tulee henkilölle informoida. Tietosuoja-asetuksen mukaan *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. Toimi voisi esimerkiksi olla se, että 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 koskevan ehdotuksen. Suostumusta ei sen vuoksi pitäisi voida antaa vaikenemalla, valmiiksi rastitetuilla ruuduilla tai jättämällä jokin toimi toteuttamatta. Suostumuksen olisi katettava kaikki käsittelytoimet, jotka toteutetaan samaa tarkoitusta tai samoja tarkoituksia varten. Jos käsittelyllä on useita tarkoituksia, suostumus olisi annettava kaikkia käsittelytarkoituksia varten.*

Tietojen siirtoon liittyy vaatimuksia, jotka tulee huomioida ennen kuin henkilötietoja siirretään edelleen. Aurora-verkossa toimivien palvelutuottajien tulee huomioida muun muassa seuraavat asiat liittyen tiedon välitykseen edelleen toisille palvelutuottajille ekosysteemissä: henkilötietojen käsittelystä tulee olla sovittu tietojenkäsittelysopimuksin tai tietosuojaliittein, tietojen käsittelyyn osallistuvien kolmansien osapuolien valvomiseksi on oltava olemassa tietty menettely, tietojen luovutuksesta kolmansille osapuolille pidetään rekisteriä ja henkilötietovirrasta tulee olla tehtynä kuvaus.

Edellä mainittuja velvoitteita liittyen tiedon siirtoon ei tämän hetken verkon toteutuksessa voida vielä toteuttaa, sillä ekosysteemejä ei ole muodostettu. Tiedonsiirto tapahtuu palveluntarjoajalta toiselle Aurora-verkon sisällä, joten palveluntarjoajan tulee huolehtia edellä mainituista kysymyksistä. Aurora-verkko sen sijaan ei välitä henkilötietoa mihinkään suuntaan tai millekään toimijalle.

Ennen henkilötietojen keräämisen aloittamista kansainväliset henkilötietojen siirrot on oltava tunnistettu, henkilötietojen käsittelyyn osallistuvat kolmannet osapuolet on oltava tunnistettu ja mikäli siirretään EU/ETA-alueen ulkopuolelle, tiedon siirtoon on oltava olemassa perusteet.

Aurora-verkon kautta voidaan välittää henkilötietoja edelleen myös kansainvälisesti. Lähtökohtaisesti jokainen palveluntarjoaja vastaa itse siitä, välitetäänkö henkilötietoja EU/ETA-alueella tai EU/ETA-alueen ulkopuolelle. Aurora-verkon toiminnan osalta on vielä epäselvää, määritelläänkö verkon käyttöön yleiset ohjeet/linjaukset, jossa otetaan kantaa esimerkiksi tietojen siirtoon ulkomaille. On myös pohdittava, mikäli yleisiä ohjeita/linjauksia ei ole, aiheuttaako se jotain vaaraa henkilötietojen käsittelylle. Aurora-verkon toiminnallisuudet eivät rajoita tiedon siirtoa kansainvälisesti.

1.5 Tietoturva

Tietoturvan tosiasiallinen toteutuminen on yksi tietosuojan edellytyksistä. Kehitystyössä tulisi olla oletusarvoinen ja sisäänrakennettu tietosuoja, jolloin myös tietoturva toteutuu lain edellyttämällä tavalla. Tietoturvallisuuden vaatimuksiin tietosuojan näkökulmasta kuuluu muun muassa

henkilötiedon käytön valvonta, henkilötiedot on oltava saatavilla turvallisen yhteyden kautta, tallennetut henkilötiedot oltava salattu, henkilötietojen suojaamiseksi on oltava olemassa tietoturvapolitiikka, kerätyt henkilötiedot oltava anonymisoitu tai pseudonymisoitu tarpeen mukaan sekä tallennetuista henkilötiedoista on saatavilla varmuuskopio.

Tietoturvan toteutuminen on Auroran kannalta ensiarvoisen tärkeää. Verkko on tehty tietoturvalliseksi siten, että palveluntarjoajien käsittelemiä henkilötietoja ei vuoda verkon ulkopuolelle. Palveluntarjoajien on omalta osaltaan toteutettava henkilötiedon suojaamiseen liittyvät tietoturvavaatimukset.

Tietosuoja-asetus soveltuu vain henkilötietoihin, joilla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja. Toimiakseen Aurora-verkossa tietoturva toteutuu myös anonymisoinnin kautta. Palveluntarjoajan ei välttämättä tarvitse käsitellä henkilötietoja, sillä tiedot ovat anonymisoitu kuten edellä on kerrottu personal ID:stä ja ID-group:sta. Anonymisoinnin osalta tietosuoja-asetuksen johdantokappale 26 mukaan anonymia henkilötietoa on arvioitava kattavasti:

”Jotta voidaan määrittää, onko luonnollinen henkilö tunnistettavissa, olisi otettava huomioon kaikki keinot, joita joko rekisterinpitäjä tai muu henkilö voi kohtuullisen todennäköisesti käyttää mainitun luonnollisen henkilön tunnistamiseen suoraan tai välillisesti, kuten kyseisen henkilön erottaminen muista. Jotta voidaan varmistaa, voidaanko keinoja kohtuullisen todennäköisesti käyttää luonnollisen henkilön tunnistamiseen, olisi otettava huomioon kaikki objektiiviset tekijät, kuten tunnistamisesta aiheutuvat kulut ja tunnistamiseen tarvittava aika sekä käsittelyajankohtana käytettävissä oleva teknologia ja tekninen kehitys.”

Vaikka nyt anonyymina pidettävä tieto olisikin mahdotonta yhdistää luonnolliseen henkilöön, kehittyvä teknologia saattaa tehdä anonymisoidusta tiedosta taas henkilötietoa johon asetus taas soveltuu. Aurora-verkossa toimivien palveluntarjoajien toimintaan liittyy oleellisesti anonymisoidun tiedon käsittely, joten nyt anonymisoituna pidettävä tieto voi muodostuakin henkilötiedoksi.

1.6 Rekisteröidyn oikeudet

Rekisteröidyn oikeudet ovat korostuneet tietosuoja-asetuksen voimaantulon myötä. Rekisterinpitäjän on huolehdittava asianmukaisesti. Rekisteröidyn oikeuksista tulee huolehtia muun muassa siten, että asiakkaalla on oikeus päästä omiin tietoihinsa, virheet asiakkaan tiedoissa voidaan korjata, tiedon siirto on huomioitu sekä profiloinnista on mahdollista kieltäytyä.

Aurora-verkon palveluntarjoajien joukossa voi olla sekä julkisen sektorin että yksityisen sektorin toimijoita. Tämä voi aiheuttaa haasteen rekisteröidyn oikeuksille ja sille, miten rekisteröidyn oikeudet toteutetaan, mikäli henkilötiedot on kerätty useasta eri lähteestä eri perustein. Rekisteröidyllä ei ole samoja oikeuksia silloin, kun henkilötietoja käsitellään lain nojalla. Viranomaiset käsittelevät henkilötietoja lähtökohtaisesti laista johdettavissa olevan käsittelyperusteen mukaisesti, jolloin rekisteröidyn oikeudet ovat vähäisemmät.

Palveluntarjoajien on huomioitava Aurora-verkossa toimiessaan myös rekisteröidyn oikeuksista. Aurora-verkon teknisiin toiminnallisuuksiin rekisteröidyn oikeudet eivät kuitenkaan vaikuta sen pidättäytyessä käsittelemästä henkilötietoja. Tällöin vastuu jää kunkin palvelutarjoajan henkilötiedon käsittelyn varaan.

1.7 Johtopäätökset

Aurora-verkon vaikutustenarvioinnin johtopäätöksenä on, että tämän hetken parhaimman tietämyksen mukaan Aurora-verkko itsessään ei käsittele henkilötietoja. Verkko ei toimiakseen tarvitse henkilötietoja, eikä siellä tämän hetken toteutuksessa ole näin tehty. Verkon sisällä tulee toimimaan useita eri palveluntarjoajia, jotka muodostavat ekosysteemin, jonka avulla palveluja kansalaisille tarjotaan. Henkilötietoja käsitellään palveluntarjoajien toimesta ja palveluntarjoajat ovat vastuussa henkilötietojen lainmukaisesta käsittelystä.

Vaikka Aurora-verkko ei tämän hetken tietojen mukaan käsittele henkilötietoja, tulee verkon kehitystyössä edelleen huomioida henkilötietojen käsittelyyn liittyvät vaatimukset ja se, missä vaiheessa tieto muuttuu henkilötiedoksi. Kehitystyön edetessä tai Aurora-verkkoon liittyvien edellytysten myötä voi tulla tilanne, jolloin verkko käsitteleekin henkilötietoja. Tällöin kaikki tietosuojalain vaatimukset tulee huomioida entistä tarkemmin ja mahdollisesti toteuttaa uudelleen vaikutustenarviointi. Aurora-verkko tarjoaa alustan palveluntarjoajille, joten kehitystyötä tulee tehdä yhteistyössä palveluntarjoajien kanssa.

Aurora-verkon toiminnallisuuksiin liittyy niin sanottu ”digikaksonen”. Digikaksonen tulee olemaan tiivistelmä henkilön tiedoista, joka on henkilön itsensä hallussa. Digikaksoseen kootaan henkilöstä tietoja, joita hän voi itse hallita. Digikaksoseen liittyvä konseptointi on vielä Auroran esiselvitysvaiheen aikana avoinna siten, että sitä voitaisiin verkkoon toteuttaa. Digikaksoseen liittyvä kehitys tulee huomioida Aurora-verkon kehitystyön yhteydessä ja toteutuksesta riippuen arvioida, tuleeko se vaikuttamaan verkkoon liittyvään henkilötiedon käsittelyyn.

Vaikka Aurora-hankkeen esiselvityksen aikana tietosuojan vaikutustenarvioinnissa nyt todetaankin, ettei verkko käsittele henkilötietoja, voi tilanne vielä muuttua. Vaikutustenarvioinnin tekeminen kehitystyön hyvin varhaisessa vaiheessa ei välttämättä anna lopullisen toteutuksen lopullista kuvaa henkilötietojen käsittelystä. Myöhäisemmässä vaiheessa, kun toteutuksesta tiedetään enemmän ja muiden Auroran työpakettien tietosuojavaikutuksista on saatu riittävä kuva, olisi tarkoituksenmukaista Aurora-verkon tietosuojaratkaisut arvioida VRK:n prosessin mukaisesti tähän tarkoitukseen laadituilla tietosuojan työkirjoilla. Nämä työkalut auttavat selvittämään muun muassa oletusarvoisen ja sisäänrakennetun tietosuojan tilanne.