Bird & Bird Asianajotoimisto Oy
Mannerheimintie 8
00100 Helsinki

Puh +358 9 622 6670
Faksi +358 9 622 6677

twobirds.com

# MUISTIO

**Vastaanottaja:** Liikenne- ja viestintävirasto Traficom
**Lähettäjä:** Bird & Bird Asianajotoimisto Oy
**Päivämäärä:** 15.4.2021

---

## MÄÄRITELMÄT

| | |
|---|---|
| **EDPB** | Euroopan tietosuojaneuvosto, Euroopan unionin tietosuojaviranomaisten riippumaton yhteistyöelin |
| **GDPR** | Yleinen tietosuoja-asetus (EU) 2016/679 |
| **Liikennepalvelulaki** | Laki liikenteen palveluista (320/2017) |
| **Rajapinnan avaaja** | Rajapinnan avaamiseen Liikennepalvelulain 156 §:n mukaisesti velvoitettu palveluntarjoaja |
| **Rajapinnan hyödyntäjä** | Liikennepalvelulain 156 §:n mukaisesti avattua rajapintaa hyödyntävän liikkumis- tai yhdistämispalvelun tarjoaja |
| **Rekisteröity** | Määritelty GDPR:n 4(1)(1) artiklassa. Puolesta-asioinnin vertailumallin tapauksessa rekisteröityjä ovat käyttäjät, joilla on käyttäjätili sekä rajapinnan avaajan että rajapinnan hyödyntäjän palveluissa, ja joiden henkilötietoja käsitellään käyttäjätilien vertailussa. |
| **Tietosuojalaki** | Tietosuojalaki 1050/2018 |

Yllä määriteltyjä käsitteitä käytetään tässä muistiossa luettavuuden vuoksi pienellä alkukirjaimella kirjoitettuina.

Bird & Bird

# Sisällysluettelo

## 1. JOHDANTO

Tämä muistio perustuu Traficomin julkisena hankintana tilaamaan oikeudelliseen selvitykseen tietosuojalainsäädännön asettamista vaatimuksista, jotka rekisterinpitäjän tulee ottaa huomioon puolesta-asiointiin liittyvän vertailumallin toteuttamisessa. Traficom on aiemmin laatinut kuvauksen kyseisestä vertailumallista[1]. Muistiossa arvioidaan miten liikenteen palveluista annetun lain (jäljempänä myös liikennepalvelulaki) mukainen käyttäjätilien vertailu puolesta-asioinnissa on mahdollista toteuttaa siten, että vertailussa huomioidaan tietosuojalainsäädännön vaatimukset. Muistio käsittelee tietosuojalainsäädännön vaatimuksia vertailumallia hyödyntävässä puolesta-asioinnissa sekä rajapinnan hyödyntäjän että rajapinnan avaajan näkökulmista. Keskeiset rajaukset on esitetty tarkemmin liitteessä 2.

Puolesta-asiointikäytäntö perustuu liikennepalvelulain 156 §:ään ja tätä lakia koskevaan hallituksen esitykseen (HE 145/2017). Tietosuojalainsäädännöllä tässä muistiossa tarkoitetaan GDPR:ää sekä sitä täydentävää Suomen tietosuojalakia.

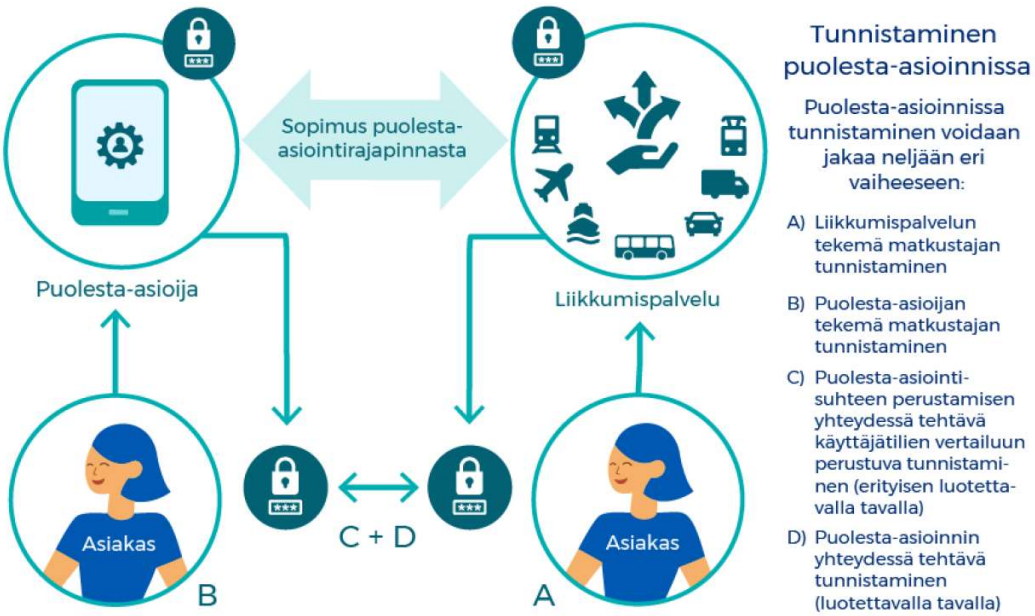
Vertailumallia hyödyntävä puolesta-asiointi etenee seuraavasti:

1. Rajapinnan avaaja ja rajapinnan hyödyntäjä solmivat sopimuksen puolesta-asiointirajapinnan hyödyntämisestä
2. Rekisteröidyllä on käyttäjätili/luo käyttäjätilin rajapinnan avaajan palveluun
3. Rekisteröidyllä on käyttäjätili/luo käyttäjätilin rajapinnan hyödyntäjän palveluun
4. Rekisteröity tekee pyynnön puolesta-asiointipalvelun käyttöönotosta rajapinnan hyödyntäjälle
   - Puolesta-asiointivaltuutus rajapinnan hyödyntäjälle
5. Rajapinnan hyödyntäjä ja rajapinnan avaaja perustavat puolesta-asiointisuhteen ko. rekisteröidyn osalta
   - Tunnistaminen erityisen luotettavalla tavalla saman rekisteröidyn käyttäjätilien tietoja vertailemalla
   - Puolesta-asiointisuhde perustetaan rekisteröidyn antaman puolesta-asiointipyynnön mukaisesti
6. Rajapinnan hyödyntäjä hankkii rekisteröidyn pyynnöstä rajapinnan avaajan liikkumispalvelun käyttäjätiliä hyödyntäen rekisteröidyn henkilökohtaisia matkustusoikeuksia itselleen, ja veloittaa itse rekisteröityä
   - Tunnistaminen luotettavalla tavalla käyttäjätilien tietoja vertailemalla
7. Rajapinnan avaaja toimittaa matkustusoikeudet rajapinnan hyödyntäjälle

Tämä muistio keskittyy tilanteisiin, joissa puolesta-asiointi toteutetaan vertailumallin avulla. Vertailumallin mukaisessa puolesta-asioinnissa puolesta-asiointipalvelun käyttäjä tunnistetaan vertailemalla rajapinnan avaajan ja rajapinnan hyödyntäjän palveluissa olevilla käyttäjätileillä olevia tietoja. Liikennepalvelulain 156 §:n mukainen puolesta-asiointi koskee vain tilanteita, joissa samalla rekisteröidyllä on käyttäjätili sekä rajapinnan avaajan että rajapinnan hyödyntäjän palveluissa. Liikennepalvelulaissa ei ole säädetty, mitä rekisteröidyn tietoja rajapinnan avaaja ja rajapinnan hyödyntäjä saavat kerätä tai mitä tietoja niiden täytyy kerätä. Kukin toimija päättää itse käyttäjätiliensä ominaisuuksista, tietosisällöistä ja käyttäjätilille kirjautumisen tasosta. Liikennepalvelulain 156 §:n 6 momentti kuitenkin velvoittaa

[1] Traficom: Puolesta-asioinnin vertailumallin kuvaus

rajapinnan avaajan ja rajapinnan hyödyntäjän tekemään yhteistyötä rajapinnan hyödyntämisen vaatimien käytännön järjestelyjen mahdollistamiseksi.




*Kaavion lähde: Traficom (2021): Tunnistamisen vaiheet puolesta-asioinnin vertailumallissa. Käyttäjätilien tunnistaminen vertailun avulla tapahtuu kohdissa C ja D.*

Käyttäjätilien vertailussa on kyse GDPR 4(2) artiklan määritelmän mukaisesta henkilötietojen käsittelystä, eli molemminpuolisesta henkilötietojen luovutuksesta rajapinnan hyödyntäjän ja rajapinnan avaajan välillä. Rajapinnan hyödyntäjä ja rajapinnan avaaja toimivat useimmissa puolesta-asiointitilanteissa 4(7) artiklan määritelmän mukaisina rekisterinpitäjinä, mikä tarkoittaa, että niiden on tekemässään henkilötietojen käsittelyssä noudatettava GDPR:n velvoitteita. Erilaisia rekisterinpitäjyyden muotoja käsitellään tarkemmin seuraavassa kappaleessa.
Vuonna 2018 sovellettavaksi tullut GDPR on edelleen uutta lainsäädäntöä, eikä monien sen velvoitteiden soveltamisesta ole syntynyt yksiselitteistä käytäntöä. GDPR:n velvoitteiden toteuttamisessa onkin suurelta osin kyse vastuullisen toimijan itsensä tekemästä tilannekohtaisesta, riskiperusteisesta arvioinnista. Henkilötietojen suoja on Suomen perustuslaissa turvattu perusoikeus, mikä antaa myös tietosuojalainsäädännöstä johtuvien velvoitteiden toteuttamiselle erityisen painoarvon. Henkilötietojen suoja on turvattu perusoikeutena myös EU:n perusoikeuskirjan 8 artiklassa, minkä lisäksi Euroopan ihmisoikeussopimus turvaa 8 artiklassaan oikeuden nauttia yksityis- ja perhe-elämän kunnioitusta. Tilanteessa, jossa kansallinen laki on ristiriidassa perus- ja ihmisoikeuksien kanssa, jälkimmäinen on asetettava etusijalle. Lisäksi, **jos kansallinen laki, kuten liikennepalvelulaki**, on ristiriidassa EU-tason asetuksen, kuten GDPR:n kanssa, EU-asetus saa etusijan.

GDPR:n mukaan rekisterinpitäjien on tahoillaan varmistettava, että niiden tekemä käsittely perustuu 6 artiklan mukaiseen oikeusperusteeseen, kuten rekisteröidyn kanssa solmittuun sopimukseen tai rekisteröidyn suostumukseen. Lisäksi rajapinnan hyödyntäjän ja rajapinnan avaajan on vertailumallin mukaista puolesta-asiointia toteuttaessaan huolehdittava siitä, että rekisteröidyllä on aina mahdollisuus käyttää

GDPR III luvun mukaisia oikeuksiaan sikäli, kun niitä ei ole muualla laissa rajoitettu. Näihin oikeuksiin kuuluvat esimerkiksi rekisteröidyn oikeus saada henkilötietonsa poistettua tai oikaista virheelliset henkilötiedot.

Molempien toimijoiden on tahollaan myös taattava GDPR 5 artiklan tietosuojaperiaatteiden, kuten rekisteröidyn selkeää informointia vaativan läpinäkyvyyden periaatteen, toteutuminen. Rekisterinpitäjän on myös pystyttävä osoittamaan, että tietosuojaperiaatteita on noudatettu. Tämän osoittamisvelvollisuuden toteuttaminen vaatii rekisterinpitäjältä henkilötietojen käsittelyn suunnittelua ja dokumentointia. Erityishuomiota vertailumallia hyödyntävässä puolesta-asioinnissa vaatii tietojen minimoinnin periaatteen sekä eheyden ja luottamuksellisuuden periaatteen yhteensovittaminen. Tämä johtuu siitä, että tietojen minimointi edellyttää, että myös käyttäjän tunnistamisessa on käsiteltävä niin vähän henkilötietoja kuin mahdollista, mikä taas voi hankaloittaa rekisteröidyn riittävän luotettavaa tunnistamista ja johtaa väärien käyttäjätilien yhdistämiseen ja siten vaarantaa eheyden ja luottamuksellisuuden periaatteen.

Vertailumallia hyödyntävän puolesta-asioinnin osalta voidaankin katsoa, että suurimmat riskit rekisteröidyille syntyvät tietoturvaloukkausten lisäksi väärien tunnistusten mahdollisuudesta. GDPR 32 artikla velvoittaa rekisterinpitäjät toteuttamaan asianmukaiset tekniset ja organisatoriset toimenpiteet riskiä vastaavan turvallisuustason varmistamiseksi. Viime kädessä kussakin puolesta-asiointitapauksessa saatavilla olevat tiedot sekä tekniset ratkaisut määrittävät keinot käyttäjän riittävän tarkkaan tunnistamiseen, joka kuitenkin perustuu mahdollisimman vähäiseen henkilötietojen käsittelyyn.

Kuten tästä johdannosta on käynyt ilmi, vertailumalliin perustuvaa puolesta-asiointia toteuttavien rekisterinpitäjien on huolehdittava useiden tietosuojalainsäädännöstä johtuvien velvoitteiden toteuttamisesta. Tämä muistio käsittelee ensin rajapinnan avaajan ja rajapinnan hyödyntäjän tietosuojaoikeudellista roolijakoa (kappale 2) sekä vertailumallia hyödyntävässä puolesta-asioinnissa käsiteltäviä henkilötietotyyppejä (kappale 3). Tämän jälkeen käydään läpi tietosuojalainsäädännön puolesta-asioinnin osapuolille asettamia olennaisimpia vaatimuksia: käsittelyn oikeusperuste (kappale 4), läpinäkyvyys ja asianmukaisuus (kappale 5), käyttötarkoitussidonnaisuus (kappale 6), tietojen minimointi (kappale 7), täsmällisyys (kappale 8), eheys ja luottamuksellisuus (kappale 9), osoitusvelvollisuus (kappale 10), rekisteröidyn oikeuksien toteuttaminen (kappale 11) sekä tietosuojan vaikutustenarvioinnin laatiminen (kappale 12). Muistion liite 1 sisältää tiivistelmän tietosuojalainsäädännön ydinvaatimuksista sekä rajapinnan avaajalle ja rajapinnan hyödyntäjälle muistiossa annetuista toimintaohjeista. Lopuksi muistion liite 2 käsittelee tämän selvityksen alaa ja rajauksia.

## 2. OSAPUOLTEN TIETOSUOJAROOLIT JA VASTUUT

GDPR 4(7) artiklan mukaan rekisterinpitäjä on luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muuta elin, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Puolesta-asioinnissa lähtökohtana voidaan pitää, että rajapinnan avaaja ja rajapinnan hyödyntäjä käsittelevät kumpikin henkilötietoja omien päämääriensä toteuttamiseksi, eli rajapinnan avaaja mahdollistaakseen puolesta-asioinnin liikennepalvelulain vaatimalla tavalla ja rajapinnan hyödyntäjä tarjotakseen rekisteröidyille puolesta-asiointipalvelua. Siten molemmat toimivat tyypillisesti rekisterinpitäjinä. Tämä tarkoittaa, että molemmat

ovat oman toimintansa osalta vastuussa kaikista GDPR:n rekisterinpitäjälle asettamista velvoitteista.[2]

Oman palvelunsa järjestämistä ja tarjoamista varten tapahtuvan henkilötietojen käsittelyn suhteen osapuolet voidaan useimmissa tapauksissa tulkita itsenäisiksi rekisterinpitäjiksi. Riippuen siitä, missä määrin rajapinnan avaaja ja rajapinnan hyödyntäjä yhdessä määrittävät henkilötietojen käsittelyn tarkoitukset ja keinot, ne voidaan käsittää myös käyttäjätilien vertailun osalta joko kahdeksi itsenäiseksi rekisterinpitäjäksi tai GDPR:n 26 artiklan mukaisiksi yhteisrekisterinpitäjiksi. GDPR:n 26 artiklan mukaan, jos vähintään kaksi rekisterinpitäjää määrittää yhdessä käsittelyn tarkoitukset ja keinot, ne ovat yhteisrekisterinpitäjiä. On mahdollista, että yhteisrekisterinpitäjyys toteutuu ainoastaan tietyn henkilötietojen käsittelytoimen, kuten tässä tapauksessa käyttäjätileillä olevien tietojen vertailun osalta, ja muussa puolesta-asioinnissa osapuolet toimivat itsenäisinä rekisterinpitäjinä.[3] GDPR:n 26 artikla määrää, että yhteisrekisterinpitäjien on keskinäisellä läpinäkyvällä järjestelyllä määriteltävä kunkin rekisterinpitäjän vastuualue GDPR:n velvoitteiden noudattamiseksi. Yhteinen vastuu ei kuitenkaan välttämättä merkitse osapuolten samanlaista vastuuta.[4]

Liikennepalvelulain 156 §:n 6 momentti edellyttää, että rajapinnan avaajan ja rajapinnan hyödyntäjän on tehtävä yhteistyötä puolesta-asioinnissa tarvittavien käytännön järjestelyjen mahdollistamiseksi. Solmimalla yhdessä sopimuksen rajapinnan avaamisesta rajapinnan hyödyntäjälle puolesta-asiointia varten sekä tekemällä yhteistyötä puolesta-asioinnin mahdollistamiseksi, osapuolet ovat tilanteessa, jossa määritellään yhdessä käsittelyn tarkoitus ja keinot. Ennen sopimuksen solmimista molemmat osapuolet ovat tietoisia käsittelyn yleisestä tarkoituksesta ja olennaiselta osin myös keinoista. Vertailumallin mukainen tunnistaminen ei myöskään ole mahdollista, elleivät molemmat osapuolet osallistu henkilötietojen käsittelyyn, mikä myös puhuu yhteisrekisterinpitäjyyden puolesta.[5] Voidaan siis katsoa, että puolesta-asioinnin vertailumallissa yhteisrekisterinpitäjyyden edellytykset todennäköisesti täyttyvät. EU-tuomioistuimen viimeaikaisen ratkaisukäytännön valossa voidaan katsoa yhteisrekisterinpitäjyyssuhteen syntyvän varsin helposti myös tilanteissa, joissa toinen rekisterinpitäjä vaikuttaa selkeästi toista enemmän käsittelyn tarkoitusten ja keinojen määrittelemiseen.[6]

**Liikennepalvelulain 156 §:n mukaisessa tilanteessa yhteisrekisterinpitäjyys todennäköisesti toteutuu käyttäjätilien vertailun osalta, ja muun puolesta-asiointiin liittyvän henkilötietojen käsittelyn osalta rajapinnan avaaja ja rajapinnan hyödyntäjä toimivat itsenäisinä rekisterinpitäjinä**. Rajapinnan avaajan ja rajapinnan hyödyntäjän on kuitenkin tarkasteltava tapauskohtaisesti, onko niiden välisessä vertailussa käsillä yhteisrekisterinpitäjyys vai toimivatko osapuolet myös tämän käsittelyn suhteen itsenäisinä rekisterinpitäjinä. Yhteisrekisterinpitäjyys on huomioitava osapuolten välisessä sopimuksessa. Lähtökohtaisesti rajapinnan hyödyntäjien ja rajapinnan

[2] Tilanteessa, jossa rajapinnan avaaja tai rajapinnan hyödyntäjä toimii henkilötietojen käsittelijänä jonkin puolesta-asiointijärjestelyn ulkopuolisen rekisterinpitäjän lukuun, tuon rekisterinpitäjän on erikseen sallittava rajapinnan puolesta-asioinnin yhteydessä tapahtuva henkilötietojen käsittely GDPR 28 artiklan mukaisessa henkilötietojenkäsittelysopimuksessa tai muissa käsittelijälle annetuissa ohjeissa. Tämä muistio käsittelee kuitenkin vain rekisterinpitäjien tietosuojavelvoitteita.

[3] Jokaista henkilötietojen käsittelyn vaihetta on arvioitava erikseen, ks. esimerkiksi asia C-40/17, 29.7.2019 Fashion ID GmbH & Co KG v. Verbraucherzentrale NRW eV, kohdat 70-72.

[4] Asia C-210/16, 5.6.2018, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH, kohta 43.

[5] EDPB: Guidelines 07/2020 on the concepts of controller and processor in the GDPR, sivu 18.

[6] Ks. esimerkiksi asia C-210/16 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH sekä asia C-40/17 Fashion ID GmbH & Co.KG v. Verbraucherzentrale NRW e.V.

avaajien väliset oikeussuhteet ovat osapuolten keskinäisiä sopimussuhteita (inter partes), mistä seuraa, että rajapinnan avaajalla voi olla kunkin rajapinnan hyödyntäjän kanssa erilliset (rinnakkaiset) sopimukset puolesta-asioinnista ja sen teknisestä toteuttamisesta, elleivät useat osapuolet halua erikseen sopia yhteistyöstä. Näin ollen kukin osapuoli on lähtökohtaisesti vastuussa omista sopimusehdoistaan ja vertailumallia koskeva yhteisrekisterinpitäjyyssuhde muodostuu kunkin rajapinnan avaajan ja rajapinnan hyödyntäjän välillä erikseen.

Kun vertailun osalta on kysymyksessä GDPR 26 artiklan mukainen yhteisrekisterinpitäjyys, osapuolten on määriteltävä keskinäisellä järjestelyllä läpinäkyvällä tavalla kunkin vastuualue GDPR:n velvoitteiden noudattamiseksi. Suosittelemme, että rajapinnan avaaja ja rajapinnan hyödyntäjä käsittelevät keskinäisessä sopimuksessaan ainakin seuraavat seikat:

- Osapuolten tietosuojaroolit: todetaan yhteisrekisterinpitäjyys
- Yhteinen käsittely: määritellään yhteisrekisterinpitäjyyssuhteessa tehtävä henkilötietojen käsittely ja käsiteltävät henkilötiedot
- Rekisteröityjen informointi: sovitaan, kuinka osapuolet tahoillaan tiedottavat rekisteröityjä puolesta-asiointiin liittyvän käyttäjätietojen vertailun vaatimasta henkilötietojen käsittelystä. Läpinäkyvyyden takaamiseksi on suositeltavaa, että molemmat osapuolet tiedottavat puolesta-asioinnista ja vertailusta. On erityisen tärkeää kertoa rekisteröidyille käsittelyn eri vaiheista sekä siitä, kumpi osapuoli on vastuussa mistäkin käsittelyn vaiheesta.
- Toiminta henkilötietojen tietoturvaloukkauksen sattuessa: sovitaan osapuolten velvollisuuksista ilmoittaa rekisteröidyille, tietosuojavaltuutetun toimistolle, sekä toisilleen mahdollisesta vertailutietojen käsittelyyn kohdistuvasta tietoturvaloukkauksesta, ja velvollisuuksista auttaa toisiaan tietoturvaloukkauksen selvittämisessä ja lopettamisessa.
- Rekisteröityjen oikeuksien toteuttaminen: sovitaan osapuolten vastuista liittyen rekisteröityjen oikeuksien toteuttamiseen ja keskinäiseen viestintään, esimerkiksi tilanteessa, jossa rekisteröity vaatii vertailussa käytettävien henkilötietojen poistamista. Sopimuksessa varaudutaan siihen, että vastuujärjestelyn sisällöstä riippumatta rekisteröity voi GDPR 26(3) artiklan mukaan käyttää GDPR:n mukaisia oikeuksiaan suhteessa kuhunkin rekisterinpitäjään ja kutakin rekisterinpitäjää vastaan.

## 3. PUOLESTA-ASIOINNIN VERTAILUMALLISSA KÄSITELTÄVÄT HENKILÖTIEDOT

Henkilötiedolla tarkoitetaan GDPR 4(1) artiklan mukaisesti 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”. Määritelmä on laaja, ja suuri osa puolesta-asioinnissa sekä siihen liittyvässä vertailussa käsiteltävistä tiedoista luetaan henkilötiedoiksi. Esimerkiksi osapuolten palveluissaan käsittelemät rekisteröityä koskevat lokitiedot ja tiedot

rekisteröidyn aikaisemmin tekemistä matkoista luetaan todennäköisesti henkilötiedoiksi.

Puolesta-asiointiin liittyvässä käyttäjätilien vertailussa hyödynnetään rekisteröidyn käyttäjätileillä olevia henkilötietoja. Tyypillisesti rajapinnan avaajien ja rajapinnan hyödyntäjien palveluissa olevilla käyttäjätileillä on rekisteröidyistä seuraavia henkilötietoja[7]:

- Puhelinnumero
- Sähköpostiosoite
- Etu- ja sukunimi
- Syntymäaika
- Katuosoite

Osassa käyttäjätilejä tiedot varmennetaan, esimerkiksi käyttäen SMS-varmennuskoodia, julkisen sektorin toimijoiden käyttämää Suomi.fi -tunnistautumista, varmennusta väestörekisterijärjestelmästä tai vahvistusviestillä sähköpostitse. Eri toimijoiden käyttäjätileille keräämien tietojen tyyppi ja määrä eroaa suuresti, kuin myös se, mitkä tiedot varmennetaan ja millä keinoin. Traficomin tekemän kyselyn vastauksissa tuli ilmi yhteensä 50 eri tunnistetietoa, joita käyttäjätileille kerätään. Käyttäjätilikohtaisesti käytössä olevien tunnistetietojen määrä vaihteli yhden ja 40:n välillä.[8]

Käytännössä kaikki käyttäjätilillä olevat tiedot luetaan henkilötiedoksi, jos ne voidaan yhdistää yksittäiseen käyttäjään. Henkilötiedon käsite on laaja ja sisältää myös ns. pseudonymisoidut tiedot, esimerkiksi matkustukseen liittyvät tunnisteet, joita vastaanottava taho ei pysty yhdistämään tiettyyn luonnolliseen henkilöön. Tällaisen tiedon luokitteluun henkilötiedoksi riittää jo se, että joku toinen taho kuin tunnisteen vastaanottanut taho pystyy yhdistämään tunnisteen ja henkilön.[9]

Kuten myöhemmin kappaleissa 7 ja 9 tarkemmin kuvataan, puolesta-asioinnin vertailumallin toteuttamisessa **suurimman haasteen** muodostaa eri toimijoiden käyttäjätileillä olevien henkilötietotyyppien eroavuus yhdistettynä GDPR:n tietojen minimoinnin periaatteeseen ja toisaalta tarpeeseen tunnistaa rekisteröity riittävän luotettavasti, jotta vältetään eheyden ja luottamuksellisuuden periaatteen vaarantuminen virheellisten tunnistusten vuoksi.

On mahdollista, että rajapinnan hyödyntäjä saa puolesta-asioinnin yhteydessä rajapinnan avaajan palvelusta myös tiedon alennettuihin hintoihin oikeuttavista rekisteröidyn ominaisuuksista. Kun rajapinnan hyödyntäjä asioi rekisteröidyn puolesta ja ostaa hänen puolestaan lipun rajapinnan avaajan puolesta, rajapinnan avaaja saattaa veloittaa lipusta alennetun hinnan. Rajapinnan hyödyntäjä saa tiedon alennetusta hinnasta, mistä saattaa tapauskohtaisesti olla pääteltävissä rekisteröidyn

[7] Traficom lähetti toimijoille 12.11.2019 tietopyynnön, jonka tarkoituksena oli selvittää mitä tietoja matkustajasta eri käyttäjätileille kerätään. Tietopyyntöön saatiin 38 vastausta, joiden perusteella Traficom on tehnyt seuraavan yhteenvedon käyttäjätilien tiedoista.

[8] Traficom lähetti toimijoille 12.11.2019 tietopyynnön, jonka tarkoituksena oli selvittää mitä tietoja matkustajasta eri käyttäjätileille kerätään. Tietopyyntöön saatiin 38 vastausta, joiden perusteella Traficom on tehnyt seuraavan yhteenvedon käyttäjätilien tiedoista

[9] Pseudonymisointi on määritelty GDPR 4(5) artiklassa. GDPR, johdanto-osan kohta 26: "– – Pseudonymisoidut henkilötiedot, jotka voitaisiin yhdistää luonnolliseen henkilöön lisätietoja käyttämällä, olisi katsottava tiedoiksi, jotka koskevat tunnistettavissa olevaa luonnollista henkilöä".

ominaisuuksia, kuten alennukseen oikeuttava vamma.[10] Tällainen tieto katsotaan GDPR 9(1) artiklan mukaiseksi erityisen henkilötietoryhmän tiedoksi, mikä osapuolten on huomioitava esimerkiksi rekisteröidyn tiedottamisessa (ks. kappale 5) sekä käsittelyn oikeusperusteen varmistamisessa (ks. kappale 4). Erityisiin henkilötietoryhmiin liittyviä kysymyksiä ei käsitellä yksityiskohtaisesti tässä muistiossa.

## 4. LAINMUKAISUUDEN PERIAATE – KÄSITTELYN OIKEUSPERUSTE

### 4.1 Johdanto

GDPR artikla 5 sisältää niin kutsutut tietosuojaperiaatteet, jotka rekisterinpitäjien on huomioitava kaikessa tekemässään henkilötietojen käsittelyssä. GDPR 5(1)(a) artiklan mukaan henkilötietoja on "käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi ('lainmukaisuus, kohtuullisuus ja läpinäkyvyys')". Lainmukaisuus tarkoittaa sitä, että käsittelylle on lainmukainen peruste. Käsittely vaatii siis aina GDPR 6 artiklan ja lisäksi erityisten henkilötietoryhmien osalta GDPR 9 artiklan ja tietosuojalain 6 pykälän mukaisen perusteen[11].

Liikennepalvelulain 156 §:n 3 momentin mukaan rekisteröidyn henkilöllisyys on puolesta-asiointisuhdetta perustettaessa tai olennaisesti muuttaessa "voitava varmistaa erityisen luotettavalla tavalla" ja rajapinnan hyödyntäjän hankkiessa henkilökohtaisia matkustusoikeuksia rekisteröidyn käyttäjätiliä hyödyntäen, rekisteröidyn henkilöllisyys on "voitava varmistaa". Puolesta-asioinnin vertailumallissa nämä tunnistamiset tehdään vertailemalla rekisteröidyn perustamilla rajapinnan hyödyntäjän sekä rajapinnan avaajan palveluissa olevilla käyttäjätileillä olevia tietoja. GDPR:n näkökulmasta vertailussa on kyse henkilötietojen käsittelystä luovutuksen muodossa.[12]

Vaikka käyttäjätiliin liitettyjä henkilötietoja ei vertaillessa suoranaisesti siirtyisi käyttäjätililtä toiselle tai rajapinnan avaajan palvelimelta puolesta-asioijan palvelimelle tai toisin päin,[13] GDPR:n mukaiseksi luovutukseksi luetaan jo tilanne, jossa tiedot asetetaan vertailua varten toisen osapuolen saataville rajapinnan kautta tai osapuolelta toiselle siirretään tieto siitä, että samalla rekisteröidyllä on käyttäjätilit molempien palveluissa.

Puolesta-asioinnin vertailumallissa osapuolet voivat perustaa vertailua varten tehtävät henkilötietojen luovutukset joko GDPR 6(1)(b) artiklan mukaisesti rekisteröidyn käyttäjätiliä luodessaan hyväksymäänsä sopimukseen tai GDPR 6(1)(a) artiklan mukaisesti rekisteröidyn suostumukseen. Tässä muistiossa ei käsitellä tarkemmin GDPR 6(1)(c) artiklan mukaista lakisääteistä velvoitetta käsittelyperusteena, koska

[10] GDPR 4(1) artikla sisältää henkilötiedon määritelmän, jonka mukaan henkilötiedolla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja. Tunnistettavissa olevana taas 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.

[11] GDPR 9 artiklan mukaisten erityisten henkilötietoryhmien käsittely on rajattu tämän selvityksen ulkopuolelle. Erityisten henkilötietoryhmien käsittely voisi esimerkiksi tulla kyseeseen käsiteltäessä käyttäjän terveystietoja, kuten liikuntarajoitteesta johtuvaa oikeutta alennuslippuun.

[12] GDPR 4(1)(2) artikla: 'käsittelyllä' [tarkoitetaan] toimintoa tai toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti, kuten tietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakua, kyselyä, käyttöä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista.

[13] Liikennepalvelulakia koskevan hallituksen esityksen HE 145/2017 vp (s. 236) mukaan "henkilötietoja ei ole tarkoitus lähtökohtaisesti lainkaan siirtää käyttäjätililtä toiselle".

näkemyksemme mukaan rekisterinpitäjää ei voida velvoittaa jakamaan henkilötietoja, joiden siirtämiseksi rekisteröity ei ole tehnyt aloitetta. Katsomme, että liikennepalvelulain 156 §:stä johtuvat velvoitteet avata rajapinta ja solmia puolesta-asiointia koskeva sopimus eivät vielä sellaisenaan muodosta oikeutusta henkilötietojen käsittelylle. 156 §:n mukaiseen puolesta-asiointiin liittyvä henkilötietojen jakaminen edellyttää siten yksittäistä sopimusta tai suostumusta.

Rajapinnan hyödyntäjän ja rajapinnan avaajan on tahoillaan varmistuttava siitä, että käyttäjän kanssa tehty sopimus tai käyttäjän antama suostumus kattaa henkilötietojen luovutuksen toiselle osapuolelle käyttäjätilien vertailemista varten. Vaikka liikennepalvelulaki velvoittaa rajapinnan avaajaa avaamaan rajapinnan, katsomme, ettei GDPR 6(1)(c) artiklan mukainen oikeusperuste, ”käsittely on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi” sovellu henkilötietojen käsittelyyn puolesta-asiointitarkoituksessa. Vaikka liikennepalvelulaki velvoittaa rajapinnan avaajaa, katsomme, että suostumus ja sopimus ovat tilanteeseen sopivat oikeusperusteet, koska puolesta-asiointi yksittäisen rekisteröidyn kohdalla alkaa aina rekisteröidyn itse tekemästä aloitteesta.

### 4.2 Sopimus

GDPR 6(1)(b) artiklan mukaan:

> [Käsittely on lainmukaista ainoastaan jos ja vain siltä osin kuin vähintään yksi seuraavista edellytyksistä täyttyy] – ”käsittely on tarpeen sellaisen sopimuksen täytäntöön panemiseksi, jossa rekisteröity on osapuolena, tai sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä;”

Kahden eri palveluissa olevan käyttäjätilin tietojen vertailun osalta sopimus voi toimia käsittelyn perusteena samalla tavoin kuin muunkin palvelun kannalta tarpeellisen henkilötietojen käsittelyn osalta: rekisteröity hyväksyy palvelun käyttäjäsopimuksen, johon osapuolet ovat kirjanneet myös puolesta-asioinnin toteuttamisen vertailumallin avulla.

Kun sopimusta käytetään henkilötietojen käsittelyn perusteena, on tärkeää varmistaa, että puolesta-asioinnin toteuttaminen on kirjattu rekisterinpitäjän palvelun **käyttäjäsopimukseen** eikä ainoastaan tietosuojaselosteeseen. Toisin kuin käyttäjäsopimus, tietosuojaseloste, jota käsitellään tarkemmin kohdassa 5, ei tyypillisesti ole luonteeltaan sopimusdokumentti, vaan sen tarkoituksena on GDPR 12-14 artikloiden mukaisesti rekisteröityjen informointi heidän henkilötietojensa käsittelystä. Tämä tarkoittaa, että osapuolten ei kannata luottaa siihen, että pelkkä puolesta-asioinnin toteuttamiseksi tehtävän vertailun mainitseminen tietosuojaselosteessa riittäisi GDPR 6(1)(b) artiklan mukaisen sopimusperusteen täyttymiseen.


*Kaavion lähde: Traficom (2021): Sopimussuhteet liikennepalvelulain 156 §:n mukaisessa kontekstissa. Lisätty "Sopimus 1" ja "Sopimus 2".*

Yllä oleva kaavio esittää tilanteen, jossa samalla rekisteröidyllä (kaaviossa "asiakas") on sopimussuhde sekä rajapinnan hyödyntäjän ("puolesta-asioija") että rajapinnan avaajan ("liikennepalvelu") kanssa. Koska rekisteröidyn käyttäjätilien tunnistaminen sekä rajapinnan hyödyntäjän että rajapinnan avaajan palveluissa on tarpeen puolesta-asiointisuhteen perustamiseksi ja puolesta-asiointitapahtuman, kuten yksittäisen lippuostoksen, toimeenpanemiseksi, tunnistamiseen liittyvän henkilötietojen käsittelyn oikeusperusteena voidaan käyttää sopimusta. Lähtökohta on se, että molemmat osapuolet perustavat puolesta-asiointia ja vertailua varten tarvittavan henkilötietojen käsittelyn omiin käyttäjäsopimuksiinsa, jotka ne ovat rekisteröidyn kanssa tehneet. Sopimusperuste soveltuu henkilötietojen käsittelyn perusteeksi vain **siltä osin kuin käsittely on tarpeen** sopimuksen täytäntöönpanemiseksi.

Rajapinnan hyödyntäjän ja rekisteröidyn välisen käyttäjäsopimuksen on kuvattava henkilötietojen käsittelyä riittävän yksityiskohtaisesti, jotta rekisteröity voi tehdä informoidun päätöksen sopimuksen hyväksymisestä. Jos käyttäjäsopimus on jo olemassa, mutta siinä ei ole sovittu henkilötietojen käsittelystä puolesta-asiointia ja vertailua varten, rajapinnan hyödyntäjän on tehtävä rekisteröidyn kanssa uusi käyttäjäsopimus, joka huomioi puolesta-asioinnin ja käyttäjätilien vertailun.

## 4.3 Rekisteröidyn suostumus

### 4.3.1 Suostumuksesta yleisesti

Vertailumallia hyödyntävässä puolesta-asioinnissa voidaan käyttää henkilötietojen käsittelyn perusteena sopimuksen sijasta myös rekisteröidyn suostumusta. GDPR 6(1)(a) artiklan mukaan:

> "Käsittely on lainmukaista ainoastaan jos ja vain siltä osin kuin vähintään yksi seuraavista edellytyksistä täyttyy: -- rekisteröity on antanut suostumuksensa henkilötietojensa käsittelyyn yhtä tai useampaa erityistä tarkoitusta varten;"

GDPR 4(11) artiklan mukaan suostumuksen on oltava yksilöity, tietoinen ja aidosti vapaaehtoinen tahdonilmaisu, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn antamalla suostumusta ilmaisevan lausuman tai toteuttamalla selkeästi suostumusta ilmaisevan toimen.[14] Suostumus ei ole pätevä, ellei se täytä näitä vaatimuksia. Suostumuksen pätevyys on arvioitava rekisteröidyn näkökulmasta seuraavasti:

- **Yksilöity:** Suostumus on annettava nimenomaisesti tietojen luovutukseen puolesta-asioinnissa käytettävää käyttäjätilien tietojen vertailua varten. Ei ole riittävää, että rekisteröity antaa suostumuksensa laajaan

[14] Tietosuojavaltuutettu on käsitellyt pätevän suostumuksen kriteeristöä esimerkiksi päätöksessään 8040/163/2019, Ks. myös https://tietosuoja.fi/rekisteroidyn-suostumus.

käsittelykokonaisuuteen, kuten ”puolesta-asiointipalvelun toteuttamiseksi”. Suostumuspyyntö on myös erotettava muusta rekisteröidyille annettavasta materiaalista, kuten sopimusehdoista. Suostumus voidaan pyytä esimerkiksi erillisessä sovelluksen suostumusikkunassa tai bannerissa, kun rekisteröity tekee aloitteen puolesta-asiointiin rajapinnan hyödyntäjän palvelussa.

- **Tietoinen:** Suostumuksen pyytämisen yhteydessä rekisteröidylle on tarjottava riittävät tiedot siitä, mitä suostumus tarkoittaa ja kattaa. Rekisteröidylle on suostumuksen pyytämisen yhteydessä annettava vähintään tiedot rekisterinpitäjästä, käsittelytoimen tarkoituksesta, käsiteltävistä henkilötiedon tyypeistä sekä oikeudesta peruuttaa suostumus.[15] Suostumusta koskevat tiedot on annettava selkeästi ja erillään muista ehdoista, eikä riitä, että ne annetaan esimerkiksi upotettuina yleisiin ehtoihin tai tietosuojaselosteeseen. Edellä mainittujen perustietojen lisäksi on suositeltavaa viitata tietosuojaselosteeseen, josta rekisteröity voi saada tarkempaa informaatiota henkilötietojensa käsittelystä.

- **Vapaaehtoinen:** Suostumusta ei saa pyytää osana yleisiä ehtoja, joista rekisteröity ei voi neuvotella. Rekisteröidyn on voitava kieltäytyä antamasta suostumusta, eikä tämä saa aiheuttaa hänelle haitallisia vaikutuksia, kuten poistaa käytöstä muita palvelun toimintoja, joiden tarjoamista varten tämä suostumus ei ole tarpeen.

- **Tietoinen tahdonilmaisu:** Suostumus on annettava aktiivisella toimella, kuten rastittamalla suostumusta kuvaava ruutu tai antama kirjallinen tai suullinen (nauhoitettu) lausuma. Rekisteröidyn on itse tehtävä aktiivinen suostumusta tarkoittava toimi. Valmiiksi rastitetut suostumusta kuvaavat ruudut tai muut valmiiksi käyttöliittymässä tehdyt valinnat eivät ole sallittuja. Suostumusta ei voi olettaa rekisteröidyn aikaisemman toiminnan perusteella.

GDPR 7(3) artiklan mukaan rekisteröidyllä on oikeus peruuttaa suostumus milloin tahansa ja suostumuksen peruuttamisen on oltava yhtä helppoa kuin sen antaminen. Suostumusta pyytävän rekisterinpitäjän, eli rajapinnan hyödyntäjän tai rajapinnan avaajan, on siis luotava palveluunsa mahdollisuus suostumuksen peruuttamiseen. GDPR 7(1) artiklan mukaan rekisterinpitäjän on myös pystyttävä osoittamaan, että rekisteröity on antanut suostumuksen henkilötietojensa käsittelyyn. Tämä edellyttää, että suostumusta hyödyntävä rekisterinpitäjä ylläpitää järjestelmää, joka tallentaa annetut ja peruutetut suostumukset.

### 4.3.2 Lapsen suostumus

GDPR 8(1) artiklan mukaan tietoyhteiskunnan palvelujen tarjoaminen lapselle suostumuksen perusteella on lainmukaista vain siinä tapauksessa ja siltä osin kuin lapsen vanhempainvastuunkantaja on antanut siihen suostumuksen tai valtuutuksen. Tietosuojalain 5 § täsmentää, että käsittelyn voi perustaa lapsen omaan suostumukseen, jos lapsi on vähintään 13-vuotias.

[15] EDPB Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1, s. 15. Silloin kun käsittelyn luonne vaatii, rekisteröidylle on annettava myös tiedot GDPR 22(2)(c) artiklan mukaisen automaattisen päätöksenteon olemassaolosta sekä mahdollisista riskeistä, jotka liittyvät GDPR 46 artiklassa kuvattuihin henkilötietojen siirtoihin ilman tietosuojan vastaavuuspäätöstä tai asianmukaisia suojatoimia.

Tietoyhteiskunnan palveluksi luetaan kaikki etäpalveluina sähköisessä muodossa palvelun vastaanottajan henkilökohtaisesta pyynnöstä toimitettavat palveluita, joista tavallisesti maksetaan korvaus.[16] Erilaiset puolesta-asioinnin mahdollistavat sovellukset luetaan siis tietoyhteiskunnan palveluiksi, ja jos rekisterinpitäjä käsittelee henkilötietoja näiden palveluiden yhteydessä perustuen rekisteröidyn suostumukseen, sen on GDPR 8(2) artiklan mukaan kohtuullisin toimenpitein tarkistettava, että lapsen vanhempi on antanut käsittelyyn oman suostumuksensa tai valtuutuksensa.

Tilanteen mukaan kohtuulliseksi toimenpiteeksi voidaan lukea esimerkiksi tunnistautumismenetelmät, joilla varmistetaan palvelun tilaajan tai ostajan ikä sekä alle 13-vuotiaiden lasten kohdalla lapsen vanhemman tai edustajan henkilöllisyys.

### 4.4 Yhteenveto oikeusperusteen valinnasta

Vertailumallia hyödyntävässä puolesta-asioinnissa voidaan käyttää henkilötietojen käsittelyn oikeusperusteena joko sopimusta tai suostumusta. Näkemyksemme on, että rajapinnan hyödyntäjän ja rekisteröidyn välistä sopimusta voidaan pitää suositeltavana oikeusperusteena, koska tämä sopimus käytännössä aloittaa puolesta-asioinnin. Etenkin rajapinnan hyödyntäjän kannalta puolesta-asiointi muodostaa merkittävän osan palvelua, jonka rekisteröity tahtoo rajapinnan hyödyntäjältä hankkia. Rajapinnan avaajan palvelussa toisen osapuolen toteuttama puolesta-asiointi ja sen toteuttamiseksi tehtävä henkilötietojen vertailu taas ei välttämättä ole osa tämän palvelun ydintä. Sopimus myös mahdollistaa henkilötietojen käsittelyn selittämisen rekisteröidylle suostumuslomaketta yksityiskohtaisemmin. Myös suostumusta voidaan käyttää puolesta-asioinnin ja vertailun oikeusperusteena, mutta huomioiden kaikki GDPR:n suostumukselle asettamat vaatimukset, pätevän suostumuksen hankkiminen saattaa olla hankalampaa kuin käsittelyn perustaminen sopimukseen.

## 5. LÄPINÄKYVYYS JA ASIANMUKAISUUS

### 5.1 Johdanto

GDPR 5(1)(a) artikla vaatii, että henkilötietoja on käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi. Lainmukaisuuden osuus, eli käsittelyn oikeusperuste, on käyty läpi edellä kappaleessa 4, ja tämä kappale koskee asianmukaisuuden ja läpinäkyvyyden osuutta. Asianmukaisuuden periaatteen ydin on se, että henkilötietoja ei saa käsitellä tavalla, joka on ennalta arvaamatonta ja odottamatonta rekisteröidyn kannalta. Läpinäkyvyys taas edellyttää, että rekisteröidyn on saatava selkeästi ja ymmärrettävästi tietoa hänen henkilötietojensa käsittelystä.

GDPR 12 artikla asettaa vaatimuksia tietojen toimittamisen tavalle. Henkilötietojen käsittelystä on kerrottava selkeästi ja ymmärrettävästi. Tiedot on annettava rekisteröidylle silloin kun henkilötietoja kerätään rekisteröidyltä, tai jos tiedot saadaan muualta kuin rekisteröidyltä itseltään, kohtuullisen ajan kuluttua siitä, kun rekisterinpitäjä on saanut henkilötiedot. Jos henkilötietoja on tarkoitus luovuttaa

[16] GDPR 4(25) artiklan mukaan tietoyhteiskunnan palveluilla tarkoitetaan palveluja, jotka määritellään Euroopan parlamentin ja neuvoston direktiivin (EU) 2015/1535 1 artiklan 1 kohdan b alakohdassa. Direktiivin 2015/1535 määritelmän mukaan tietoyhteiskunnan palvelulla tarkoitetaan kaikkia etäpalveluina sähköisessä muodossa palvelun vastaanottajan henkilökohtaisesta pyynnöstä toimitettavia palveluita, joista tavallisesti maksetaan korvaus. Etäpalvelu tarkoittaa palvelua, joka toimitetaan siten että osapuolet eivät ole samanaikaisesti läsnä. Sähköisellä muodolla tarkoitetaan palvelua, joka lähetetään lähetyspaikasta ja vastaanotetaan määränpäässä tietoja elektronisesti käsittelevien laitteiden tai tietojen säilytyksen avulla ja joka lähetetään, siirretään ja vastaanotetaan kokonaan linjoja, radioyhteyttä, optisia tai muita elektromagneettisia välineitä käyttäen. Palvelun vastaanottajan henkilökohtaisesta pyynnöstä toimitettavalla palvelulla tarkoitetaan palvelua, joka toimitetaan henkilökohtaisen pyynnön perusteella tapahtuvana tiedonsiirtona.

toiselle vastaanottajalle, tiedot on annettava viimeistään silloin kun näitä tietoja luovutetaan ensimmäisen kerran.

Puolesta-asioinnin vertailumallissa käsiteltävät henkilötiedot on tyypillisesti saatu rekisteröidyltä itseltään, eli rekisteröidylle on annettava seuraavat, GDPR 13 artiklan vaatimat tiedot:

- Rekisterinpitäjän ja tapauksen mukaan tämän mahdollisen edustajan identiteetti ja yhteystiedot;
- Tietosuojavastaavan yhteystiedot, jos rekisterinpitäjä on sellaisen nimittänyt;
- Henkilötietojen käsittelyn tarkoitukset sekä käsittelyn oikeusperuste;
- Jos käsittely perustuu rekisterinpitäjän tai kolmannen osapuolen oikeutettuun etuun, tieto siitä, mikä tämä etu on;
- Henkilötietojen vastaanottajat tai vastaanottajaryhmä;
- Tieto mahdollisista henkilötietojen siirroista EU:n/ETA:n ulkopuolelle sekä tieto siirrossa sovellettavista asianmukaisista suojatoimista (kuten EU-komission vakiosopimuslausekkeista), tai EU-komission antamasta vastaanottajamaan tietosuojan riittävyyttä koskevasta päätöksestä
- Henkilötietojen säilytysaika tai jos se ei ole mahdollista, tämän ajan määrittämiskriteerit;
- Tieto GDPR III luvussa mainituista rekisteröidyn oikeuksista: oikeus saada tietoa henkilötietojensa käsittelystä, oikeus saada pääsy tietoihin, oikeus oikaista tietoja, oikeus poistaa tiedot ja tulla unohdetuksi, oikeus rajoittaa tietojen käsittelyä, oikeus siirtää tiedot järjestelmästä toiseen, oikeus vastustaa tietojen käsittelyä sekä oikeus olla joutumatta automaattisen päätöksenteon kohteeksi;
- Rekisteröidyn oikeus peruuttaa suostumus, jos käsittely perustuu suostumukseen;
- Oikeus tehdä valitus valvontaviranomaiselle;
- Onko henkilötietojen antaminen lakisääteinen tai sopimukseen perustuva vaatimus taikka sopimuksen tekemisen edellyttämä vaatimus sekä onko rekisteröidyn pakko toimittaa henkilötiedot ja tällaisten tietojen antamatta jättämisen mahdolliset seuraukset;
- automaattisen päätöksenteon, ja profiloinnin olemassaolo, sekä ainakin näissä tapauksissa merkitykselliset tiedot käsittelyyn liittyvästä logiikasta samoin kuin kyseisen käsittelyn merkittävyys ja mahdolliset seuraukset rekisteröidylle;

Jos henkilötiedot on saatu muualta kuin rekisteröidyltä itseltään, esimerkiksi väestörekisteristä, rekisteröidylle on annettava myös seuraavat GDPR 14 artiklan vaatimat tiedot:

- Käsiteltävät henkilötietoryhmät;

- Mistä henkilötiedot on saatu sekä tarvittaessa se, onko tiedot saatu yleisesti saatavilla olevista lähteistä;

### 5.2 Läpinäkyvyyden periaatteen toteuttaminen puolesta-asioinnissa

Tyypillisesti GDPR 13 ja 14 artikloiden vaatimat tiedot annetaan rekisterinpitäjän tietosuojaselosteessa. Molempien osapuolien onkin läpinäkyvyysperiaatetta noudattaakseen varmistuttava siitä, että niiden rekisteröidyille suuntaamassaan tietosuojaselosteessa yllä kuvatut tiedot on annettu myös puolesta-asioinnin ja vertailun osalta. Esimerkiksi puolesta-asiointiin liittyvän, käyttäjätilien vertailun avulla tehtävän tunnistamisen oikeusperuste, sekä käsittelyn tarkoitus on kerrottava. Käsittelytarkoituksen yhteydessä on kerrottava ymmärrettävästi, mitä puolesta-asiointi ja käyttäjätilien vertailu henkilötietojen käsittelyn kannalta tarkoittavat. Jos rajapinnan avaaja tai rajapinnan hyödyntäjä ovat määrittäneet tietyt henkilötiedot välttämättömiksi vertailua hyödyntävän puolesta-asioinnin toteuttamiseksi, rekisteröidylle on annettava tieto siitä, ettei puolesta-asiointia voida suorittaa, ellei rekisterinpitäjällä ole näitä tietoja. Tietosuojaselosteessa on myös tärkeää kertoa, mitä henkilötietoja osapuolten välillä luovutetaan käyttäjätilien vertailun ja tunnistamisen toteuttamiseksi ja minkä henkilötietojen suhteen osapuolet toimivat yhteisrekisterinpitäjinä (yhteisrekisterinpitäjyydestä tarkemmin kappaleessa 2).

Tietosuojaseloste on pidettävä jatkuvasti rekisteröityjen saatavilla, minkä lisäksi selosteeseen on suositeltavaa erikseen viitata ainakin puolesta-asiointisuhteen perustamisvaiheessa. Puolesta-asiointisuhdetta perustettaessa osapuolet voivat esimerkiksi antaa tiiviissä muodossa perustiedot puolesta-asioinnin vaatimasta henkilötietojen käsittelystä sekä tarjota rekisteröidylle linkin tietosuojaselosteeseen, jossa on tarjolla yksityiskohtaisempaa tietoa[17].

Kun rekisterinpitäjät päivittävät tietosuojaselosteitaan puolesta-asioinnin ja vertailun vaatiman henkilötietojen käsittelyn osalta, päivityksestä on tiedotettava rekisteröidyille siten, että se tosiasiassa myös tulee rekisteröidyn tietoon. Tässä voidaan hyödyntää esimerkiksi palvelun yhteydessä käytettäviä viestintäkanavia, tai kanavia, joiden kautta palvelun muutoksista tyypillisesti viestitään käyttäjille, kuten sähköpostia.

## 6. KÄYTTÖTARKOITUSSIDONNAISUUS

GDPR 5(1)(b) artikla määrää käyttötarkoitussidonnaisuuden periaatteesta, joka tarkoittaa sitä, että rekisterinpitäjä voi kerätä henkilötietoja ainoastaan tiettyä, nimenomaista ja laillista tarkoitusta varten, eikä niitä saa käsitellä myöhemmin näiden tarkoitusten kanssa yhteensopimattomalla tavalla. Käyttötarkoitussidonnaisuuden periaatetta noudattaakseen rajapinnan hyödyntäjän ja rajapinnan avaajan on määritettävä käsittelemiensä henkilötietojen käsittelytarkoitus ja kerrottava alusta asti rekisteröidylle selkeästi, mihin tarkoitukseen hänen henkilötietojaan kerätään ja muuten käsitellään (ks. asianmukaisuudesta ja läpinäkyvyydestä kappale 5).

Rajapinnan avaajille ja rajapinnan hyödyntäjille käyttötarkoitussidonnaisuus tarkoittaa sitä, että esimerkiksi käyttäjätilin perustamisen yhteydessä kerättyjä henkilötietoja ei lähtökohtaisesti suoraan saa käyttää puolesta-asiointiin, ellei niitä ole kerätty tätä tarkoitusta varten. Jos rajapinnan hyödyntäjä tai rajapinnan avaaja ovat keränneet rekisteröidyn henkilötietoja muihin tarkoituksiin ja päättävät sittemmin

[17] EDPB:n edeltäjä WP 29 on suositellut tällaista ”kerroksittaista” lähestymistapaa digitaalisessa ympäristössä. Ks. Article 29 Working Party Guidelines on transparency under Regulation 2016/679 (WP 260), sivu 19.

hyödyntää tietoja puolesta-asiointiin ja siihen vaadittavaan käyttäjätilien vertailuun, niiden on huomioitava seuraavat seikat:

1) Jos näiden henkilötietojen käsittely perustuu suostumukseen, pyydettävä käsittelyyn uusi suostumus. Tämä voidaan tehdä, kun rekisteröity pyytää puolesta-asiointia ensimmäisen kerran.

2) Jos näiden henkilötietojen käsittely perustuu vanhaan käyttäjäsopimukseen, tehtävä rekisteröidyn kanssa uusi käyttäjäsopimus, joka huomioi puolesta-asioinnin ja käyttäjätilien vertailun; taikka

3) Arvioitava, että alkuperäinen käyttötarkoitus sekä uusi käyttötarkoitus (vertailuun perustuva puolesta-asiointi) ovat yhteensopivia huomioiden;

    - henkilötietojen keruun tarkoitusten ja aiotun myöhemmän käsittelyn tarkoitusten väliset yhteydet;
    - henkilötietojen keruun asiayhteys erityisesti rekisteröityjen ja rekisterinpitäjän välisen suhteen osalta;
    - henkilötietojen luonne, erityisesti se, käsitelläänkö erityisiä henkilötietojen ryhmiä GDPR 9 artiklan mukaisesti;
    - aiotun myöhemmän käsittelyn mahdolliset seuraukset rekisteröidyille;
    - asianmukaisten suojatoimien, kuten salaamisen tai pseudonymisoinnin, olemassaolo.

## 7. TIETOJEN MINIMOINTI

Puolesta-asioinnin toteuttamisessa sekä siihen liittyvässä rekisteröidyn käyttäjätileillä olevien henkilötietojen vertailussa on aina huomioitava GDPR 5(1)(c) artiklan tietojen minimoinnin periaate. Tietojen minimoinnin periaate vaatii, että henkilötietojen on oltava asianmukaisia ja olennaisia ja rajoitettuja siihen, mikä on tarpeellista suhteessa niihin tarkoituksiin, joita varten niitä käsitellään. Puolesta-asiointiin liittyvässä vertailussa rajapinnan hyödyntäjän ja rajapinnan avaajan on siis käsiteltävä niin vähän henkilötietoja kuin vain mahdollista, jotta rekisteröidyn henkilöllisyys voidaan varmistaa liikennepalvelulain vaatimalla tasolla.

Liikennepalvelulain 156 §:n 3 momentissa todetaan, että puolesta-asiointitapahtuman yhteydessä saa henkilötietoja käsitellä ainoastaan siinä määrin kuin on tarpeen henkilöllisyyden varmistamiseksi ja puolesta-asiointitapahtuman toteuttamiseksi. Samassa momentissa todetaan myös:

> ”Sen lisäksi, mitä muualla laissa säädetään, henkilöllisyys on voitava varmistaa erityisen luotettavalla tavalla, kun puolesta-asiointisuhde perustetaan tai sitä muutetaan olennaisesti. Myös puolesta-asiointitapahtuman yhteydessä henkilöllisyys on voitava varmistaa.”

Tämä tarkoittaa, että tietojen minimoinnin periaatteesta huolimatta rajapinnan avaaja ja rajapinnan hyödyntäjä voivat käsitellä rekisteröidyn henkilötietoja siinä määrin, kun se on tarpeellista:

1) Rekisteröidyn henkilöllisyyden varmistamiseksi erityisen luotettavalla tavalla, kun puolesta-asiointisuhde perustetaan tai sitä muutetaan olennaisesti; ja

2) Rekisteröidyn henkilöllisyyden varmistamiseksi puolesta-asioinnin yhteydessä.

Liikennepalvelulaki ei määrittele sitä, mitä ”erityisen luotettavalla tavalla” tarkoitetaan. On kuitenkin selvää, että henkilöllisyyden varmistamisen vaatimus on voimakkaampi puolesta-asiointisuhteen perustamisen yhteydessä kuin yksittäisen puolesta-asiointitapahtuman yhteydessä. Tietojen minimoinnin periaate on tasapainotettava liikennepalvelulain vaatiman henkilöllisyyden varmistamisen sekä eheyden ja luottamuksellisuuden periaatteen (ks. kappale 9) kanssa. On myös huomioitava, että täsmällisyyden periaate vaatii käsiteltävien henkilötietojen paikkansapitävyyttä, mikä voi vaarantua liian heikkotasoisen tunnistamisen tapauksessa. Eheyden ja luottamuksellisuuden periaate puolestaan vaatii rajapinnan avaajaa ja rajapinnan hyödyntäjää varmistamaan henkilötietojen asianmukaisen turvallisuuden sekä suojaamaan niitä esimerkiksi luvattomalta käsittelyltä, joka olisi suora seuraus väärien käyttäjätilien yhdistämisestä.

Tietojen minimoinnin periaate johtaa siihen, että osapuolten tulee lähtökohtaisesti suhtautua pidättyväisesti uusien henkilötietojen keräämiseen toteuttaessaan tunnistamisjärjestelyä. Tästä huolimatta vertailumallin toteuttaminen riittävän luotettavasti saattaa kuitenkin tosiasiassa vaatia ”ylimääräisiä” käsittelytoimia, kuten vahvan tunnistautumisen käyttöä. Tietojen minimoinnin periaate ei voi estää henkilötietojen käsittelyä, joka on tarpeellista käyttäjän henkilöllisyyden varmistamiseksi liikennepalvelulain vaatimalla tavalla. Viime kädessä käyttäjän riittävän tarkka tunnistaminen on määriteltävä erikseen kussakin yksittäistapauksessa. Rajapinnan avaajan ja rajapinnan hyödyntäjän tekniset ratkaisut määrittävät keinot käyttäjän riittävän tarkkaan tunnistamiseen, joka kuitenkin perustuu mahdollisimman vähäiseen henkilötietojen käsittelyyn.

Jos rajapinnan hyödyntäjä ja rajapinnan avaaja päätyvät siihen, että puolesta-asioinnin toteuttaminen vertailumallin avulla vaatii tietyn uuden henkilötietotyypin, vaikkapa uuden tunnisteen käsittelyä, osapuolten on varmistettava, että heidän valitsemansa oikeusperuste (ks. kappale 4 lainmukaisuudesta) kattaa kyseisen henkilötietotyypin käsittelyn ja että rekisteröityä on informoitu tämän henkilötietotyypin käsittelystä (ks. kappale 5 läpinäkyvyydestä).

Tietojen minimoinnin periaatetta toteuttavassa vertailun toteuttamisessa voidaan esimerkiksi hyödyntää hajauttamista (”hashing”). Hajauttamisessa osapuolet käyttävät algoritmia, joka muuntaa vertailua varten tarvittavat tiedot uudeksi merkkijonoksi, eli niin kutsutuksi tiivisteeksi (”hash”). Tyypillisesti tämä prosessi on yksisuuntainen, eli tiivistettä ei enää voida muuntaa takaisin alkuperäiseen muotoonsa. Vertailumallin tapauksessa rajapinnan avaaja ei pystyisi muuntamaan rajapinnan hyödyntäjältä saamaansa tunnistetta takaisin muotoon, joka näyttäisi esimerkiksi puhelinnumeron tai sähköpostiosoitteen. Sen sijaan rajapinnan avaaja käyttäisi samaa algoritmia kaikkien rekisteröityjensä vastaaviin tietoihin ja vertaisi rajapinnan hyödyntäjältä saamaansa tiivistettä näistä tiedoista luotuihin tiivisteisiin. Tämän vertailun lopputulos olisi joko

1) samaa tiivistettä ei löydy ja rajapinnan avaaja palauttaa rajapinnan hyödyntäjälle viestin, ettei rekisteröidyn käyttäjätiliä löydy eikä henkilötietoja siten luovuteta, tai

2) vastaava tiiviste löytyy, mikä tarkoittaa, että myös tiivisteen luomiseen käytetyt henkilötiedot ovat rajapinnan avaajan ja rajapinnan hyödyntäjän käyttäjätileillä samat. Tämän jälkeen rajapinnan avaaja luovuttaa rajapinnan hyödyntäjälle minimimäärän henkilötietoja, eli tiedon siitä, että molemmilla toimijoilla on palvelussaan saman rekisteröidyn käyttäjätili. Myös hajautusalgoritmia hyödyntävässä tunnistamisessa luovutetaan siten henkilötietoja.

Osapuolten tulisi esimerkiksi hyödyntää yllä kuvattua hajauttamista tai vastaavia teknisiä ratkaisuja, joiden avulla vertailussa käsitellään niin vähän henkilötietoja kuin mahdollista, ja rajapinnan avaajan tulisi palauttaa rajapinnan hyödyntäjälle ainoastaan tieto siitä, onko tiivisteen tai muun tunnisteen kuvaama käyttäjätili löytynyt.

Tietojen minimoinnin periaate edellyttää, että silloinkin, kun tietojen vertailu tuottaa tiedon vastaavuudesta, vertailun loppuun saattamisessa tulee käyttää vain ja ainoastaan tarpeellisia tietoja, ei siis muita mahdollisesti saatavilla olevia tietoja. Jos vastaavuuksia ei ole, myöskään tietoja ei pitäisi jakaa.

## 8. TÄSMÄLLISYYS

GDPR 5(1)(d):n täsmällisyyden periaate vaatii, että käsiteltävien henkilötietojen on oltava täsmällisiä ja tarvittaessa päivitettyjä. Lisäksi on toteutettava kaikki mahdolliset kohtuulliset toimenpiteet sen varmistamiseksi, että käsittelyn tarkoituksiin nähden epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä. Käsiteltävien henkilötietojen täsmällisyys on olennaista myös liikennepalvelulain vaatimusten täyttämiseksi. Liikennepalvelulain 156 §:n 3 momentti vaatii rekisteröidyn henkilöllisyyden varmistamista erityisen luotettavalla tavalla, kun puolesta-asiointisuhde perustetaan tai sitä muutetaan olennaisesti. Sama lainkohta vaatii rekisteröidyn tunnistamista myös yksittäisen puolesta-asiointitapahtuman yhteydessä.

Epätäsmälliset ja virheelliset henkilötiedot voivat vaarantaa rekisteröidyn oikeuksia. Kun rajapinnan hyödyntäjä ja rajapinnan avaaja vertaavat käyttäjätileillä olevia tietoja toisiinsa, pienikin virhe verrattavassa henkilötiedossa voi johtaa siihen, että väärän rekisteröidyn käyttäjätiliä käytetään puolesta-asioinnissa. Tämä taas johtaa kappaleessa 9 käsitellyn eheyden ja luottamuksellisuuden periaatteen vaarantumiseen.

Kun tietojen minimoinnin periaate edellyttää sitä, että puolesta-asiointia ja käyttäjätilien yhdistämisessä käytettävää vertailua varten käsitellään niin vähän henkilötietoja kuin mahdollista, täsmällisyyden periaate sekä liikennepalvelulain 156 §:n 3 momentti vaativat varmistumaan, että rekisteröity on tunnistettu riittävällä tarkkuudella. Eri toimijoiden käyttäjätileillä olevien henkilötietotyyppien eroavuuden vuoksi osapuolten tulee keskenään harkita, mitkä henkilötiedot mahdollistavat riittävän tarkan tunnistamisen vertailumallissa. Lähtökohtana on kuitenkin pidettävä sitä, ettei rajapinnan avaaja voi vaatia rajapinnan hyödyntäjältä erityisen luotettavaan tunnistamiseen enempää kuin mitä rajapinnan avaaja vaatii omilta käyttäjiltään. Esimerkiksi jos rajapinnan avaajan palvelussa käyttäjätilin avaamiseksi vaaditaan vain vahvistettu sähköpostiosoite, ei myöskään puolesta-asioinnissa voida rajapinnan hyödyntäjältä vaatia useampien henkilötietotyyppien keräämistä tunnistamistarkoitukseen. Siten erityisen luotettavan henkilöllisyyden varmistamisen

taso määrittyy niiden tietojen perusteella, joita rajapinnan avaajan palvelussa olevalla käyttäjätilillä on.[18]

Osapuolten on huomioitava, että vertailemalla tapahtuva puolesta-asiointi on turvallisesti mahdollista vain jossain tapauksissa: silloin, kun molempien osapuolten käyttäjätilien tietokannat sisältävät riittävät tiedot ja ovat yhteensopivia, määrämuotoisia ja asianmukaisen luotettavalla tavalla tunnistettuja tietojen oikeellisuuden varmistamiseksi. Vaikka tietojen minimoinnin periaate edellyttää pidättyväistä suhtautumista uusien henkilötietojen keräämiseen, osapuolet voivat todeta, että rekisteröidyn riittävän tarkka tunnistaminen liikennepalvelulain ja GDPR:n täsmällisyyden periaatteen edellyttämällä tavalla vaatii uusien henkilötietojen käsittelemistä. Tämä päätös on syytä perustella sekä dokumentoida mahdollisimman tarkasti esimerkiksi tietosuojan vaikutustenarvioinnin yhteydessä (ks. kappale 12 vaikutustenarvioinnista).

Mikäli käyttäjätilien tietojen vertailun perusteella tullaan lopputulokseen, jossa puolesta-asiointiin tarvittavaa käyttäjän käyttäjätiliä ei voida yksilöidä (ei ole olemassa, tai vertailuun käytettävät tiedot eivät täsmää) ei puolesta-asiointisuhdetta voida näillä tiedoilla perustaa.[19] Käyttäjätilien yksilöinnin ja yhdistämisen riittävyyttä on myös yksittäisen puolesta-asiointitapahtuman kohdalla arvioitava käsiteltävien henkilötietojen suojaamistarpeen perusteella: rekisteröidyn asuinkunnan ja alennusstatuksen (esim. liikuntavamma) huomioivan kausilipun myynnissä tunnistamistarpeen voivan arvioida olevan vahvempi kuin tavallisen kertalipun myynnissä.

On rekisterinpitäjän vastuulla varmistua käsittelemänsä tiedon täsmällisyydestä. Puolesta-asioinnin yhteydessä voidaan pitää erityisen tärkeänä, että käyttäjätilien vertailussa käytettävien tunnisteiden täsmällisyydestä on varmistuttu. Täsmällisyyden periaatteen noudattaminen voi siten edellyttää esimerkiksi vertailussa käytettävän puhelinnumeron ja sähköpostiosoitteen kaksivaiheista vahvistamista. Tämän vahvistuksen uusiminen esimerkiksi vuosittain edesauttaa myös mahdollisia vääriä yhdistämisiä tilanteessa, jossa rekisteröity on vaihtanut puhelinnumeroaan ja jättänyt uuden numeron päivittämättä käyttäjätililleen.

## 9. EHEYS JA LUOTTAMUKSELLISUUS

GDPR 5(1)(f) artiklan mukaan henkilötietoja on käsiteltävä tavalla, jolla varmistetaan niiden asianmukainen turvallisuus, mukaan lukien suojaaminen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta käyttäen asianmukaisia teknisiä tai organisatorisia toimia. Tämä eheyden ja luottamuksellisuuden periaate vaatii rajapinnan avaajaa ja rajapinnan hyödyntäjää ehkäisemään riskejä, joita esimerkiksi käyttäjätilien virheellinen yhdistäminen sekä tietovuodot voisivat aiheuttaa. Lisäksi rajapinnan avaajan ja rajapinnan hyödyntäjän on pyrittävä estämään puolesta-asioinnin hyväksikäyttö siten, että toinen henkilö pystyisi ostamaan lippuja rekisteröidyn nimiin saatuaan haltuunsa hänen henkilötietojaan. GDPR 32 artikla velvoittaa rekisterinpitäjää ottamaan käyttöön riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet. Käsittelyyn liittyvän riskin arvioimisessa rekisterinpitäjä voi hyödyntää esimerkiksi tietosuojan vaikutustenarviointia (ks. kappale 12).

[18] Traficomin kanta. Annettu 17.3.2021 vastauksena Bird & Birdin tiedusteluun.
[19] Traficom: Puolesta-asioinnin vertailumallin kuvaus, s. 7.

Myös liikennepalvelulain 158 §:n 2 momentti sisältää molempia osapuolia koskevan tietoturva- ja tietosuojavelvoitteen:

> ”Edellä 154–156 §:ssä tarkoitettujen rajapintojen avaamiseen velvoitettujen palveluntarjoajien on huolehdittava siitä, että avaaminen voi tapahtua palvelun tietoturvan ja yksityisyyden suojan vaarantumatta. Edellä 156 §:ssä tarkoitetun pääsyyn oikeutetun liikkumis- tai yhdistämispalvelun tarjoajan on huolehdittava oman palvelunsa tietoturvan ja tietosuojan tasosta niin, että puolesta-asiointi voi tapahtua näitä vaarantamatta.”

Liikennepalvelulain 156 §:n 4 momentin mukaan rajapinnan avaajalla, jonka liikkeelle laskemaan lippuun liittyy alennus, korvaus tai erityisehto, on oikeus arvioida pääsyyn oikeutetun rajapinnan luotettavuus ennalta asetettujen arviointikriteerien ja ehtojen mukaan. Traficomin muistioluonnos puolesta-asioijan luotettavuuden arviointikriteereistä listaa joukon kriteereitä, joita rajapinnan avaaja saa käyttää pohjana rajapinnan hyödyntäjien luotettavuuden arvioinnissa[20]:

- Puolesta-asioijan asiakkaiden tunnistamisen luotettavuus
- Puolesta-asioijan käyttäjätilien luotettavuus vertailussa:
  - Tietosisältöjen soveltuvuus vertailuun
  - Tietosisältöjen oikeellisuus/tietojen varmentaminen
- Puolesta-asioijan tietoturva
- Puolesta-asioijan taloudellinen tilanne
- Puolesta-asioijan maine

Näiden kriteerien huomioiminen, sekä kriteerit täyttämättömien rajapinnan hyödyntäjien karsiminen, edesauttaa myös GDPR 5(1)(f) artiklan mukaisen eheyden ja luottamuksellisuuden periaatteen toteuttamista. Osapuolet voivat lisäksi hyödyntää eheyden ja luottamuksellisuuden periaatteen toteuttamisessa esimerkiksi:

- Osapuolten välillä välitettävien henkilötietojen salausta viimeisimmän salausteknologian mahdollistamalla tavalla.

- Vertailuun perustuvassa käyttäjätilien yhdistämisessä erilaisia tunnuksia, jotka ainoastaan rajapinnan avaaja ja rajapinnan hyödyntäjä voivat yhdistää tiettyyn rekisteröityyn, esimerkiksi erilaiset laskennallisesti luodut tiivisteet (”hashit”) tai muut tunnisteet (esim. ”tokenit”).

- Kaksivaiheista tunnistamista rajapinnan hyödyntäjän palvelussa esimerkiksi puhelinnumeroon tai sähköpostiin perustuen, jos näitä henkilötietoja käytetään vertailussa.

- Vahvaa sähköistä tunnistamista, kuten suomi.fi- tai pankkitunnuksilla tehtävää tunnistamista kummankin osapuolen käyttäjätilejä perustettaessa.[21]

[20] Traficomin muistioluonnos puolesta-asioijan luotettavuuden arviointikriteereistä, 6.11.2020: https://www.liikkumisenrajapinnat.fi/sites/default/files/media/file/Arviointikriteeritmuistioluonnos.dotx__0.pdf

[21] Vahvaa sähköistä tunnistamista ei kuitenkaan voida edellyttää puolesta-asiointivaltuutusta perustettaessa. 12.12.2020 antamassaan ratkaisussa 07091/19/7599 Helsingin hallinto-oikeus totesi, että Traficom on voinut pitää valtuutukseen liittyvää vahvaa tunnistamista kohtuuttomana käyttöehtona ja siten velvoittaa rajapinnan avaajan muuttamaan puolesta-asiointiratkaisuaan tältä osin ja hylätä rajapinnan avaajan asiaa koskevan oikaisuvaatimuksen.

- Puolesta-asiointivaltuuden voimassaolon rajoittamista.

## 10. OSOITUSVELVOLLISUUS

GDPR 5(2) artikla määrää osoitusvelvollisuuden periaatteesta. Osoitusvelvollisuus tarkoittaa, että rekisterinpitäjän on pystyttävä osoittamaan noudattavansa tietosuojalainsäädäntöä**.** Käytännössä tämä tarkoittaa kaikkien tässä muistiossa käsiteltyjen toimenpiteiden tekemistä ja dokumentoimista.

Puolesta-asioinnissa sekä siihen liittyvässä käyttäjätilien tietojen vertailussa osapuolten on huomioitava, erityisesti seuraavan dokumentaation säilyttäminen:

- **Seloste käsittelytoimista (GDPR artikla 30)**. Jos rekisterinpitäjä on velvollinen ylläpitämään selostetta käsittelytoimista, selosteeseen on päivitettävä tiedot puolesta-asioinnin yhteydessä tehtävästä henkilötietojen käsittelystä. Koska puolesta-asiointiin ja käyttäjätilien vertailuun liittyvä henkilötietojen käsittely on teknisesti monimutkaista, se tulisi dokumentoida riittävän yksityiskohtaisesti.
- **Rekisteröidyn informointi (GDPR artiklat 12-14).** Rekisterinpitäjän on päivitettävä tietosuojaselosteensa kattamaan puolesta-asiointia koskevan käsittelyn.
- **Käsittelyn oikeusperuste (GDPR artiklat 6-10).** Jos henkilötietoja käsitellään suostumuksen perusteella, dokumentaatio annetuista ja peruutetuista suostumuksista sekä siitä, kuinka suostumuksen antajaa on informoitu. Jos käsittely perustuu sopimukseen, dokumentaatio sopimuksista.
- **Muut sisäiset ja ulkoiset ohjeistukset (GDPR artiklat 12, 13, 14, 24, 25, 28, 29, 32)**
  - Mahdollisia riskiarvioita koskeva dokumentaatio sekä toteutetut tekniset ja organisatoriset suojatoimenpiteet – esimerkiksi osapuolten tekemät toimet väärien vertailutulosten minimoimiseksi
  - Tietoturvaloukkauksiin liittyvät ohjeistukset
  - Sisäiset ja ulkoiset ohjeet rekisteröidyn oikeuksien toteuttamiseksi
  - Ohjeet henkilötietoja käsitteleville työntekijöille ja henkilötietojen käsittelijöille
  - Raportit sisäisistä tarkastuksista ja auditoinneista
- **Yhteisrekisterinpitäjyyttä koskevat sopimukset (GDPR artikla 26).** Jos rajapinnan avaaja ja rajapinnan hyödyntäjä arvioivat olevansa käyttäjätilien vertailun suhteen yhteisrekisterinpitäjyyssuhteessa, yhteisrekisterinpitäjien vastuualueita koskevat sopimukset on säilytettävä.
- **Tietosuojan vaikutustenarviointeja ja tietosuojavaltuutetun ennakkokuulemista koskeva dokumentaatio (GDPR artiklat 35 ja 36).** Jos osapuolet päättävät toteuttaa puolesta-asiointia koskevan tietosuojan vaikutustenarvioinnin, johon viitataan usein lyhenteellä DPIA**,** ja sen tulosten perusteella pyytää tietosuojavaltuutetun ennakkokuulemista, näitä koskeva dokumentaatio on säilytettävä.

Osapuolten on myös tahoillaan säilytettävä esimerkiksi tietoturvaloukkauksia koskeva dokumentaatio ja henkilötietojen käsittelijöiden kanssa tehdyt sopimukset sekä sopimukset ja dokumentaatio henkilötietojen siirrosta EU:n ja Euroopan talousalueen (ETA) ulkopuolelle.

## 11. REKISTERÖITYJEN OIKEUDET

Rekisteröidyillä on joukko henkilötietojensa käsittelyyn liittyviä oikeuksia, jotka on listattu GDPR III luvussa. Tämä kappale käsittelee vertailumallia hyödyntävän puolesta-asioinnin kannalta olennaisimpia rekisteröityjen oikeuksia. Rekisteröidyn informointia GDPR 13 ja 14 artiklojen mukaisesti on käsitelty edellä kappaleessa 5. Rekisteröityjen oikeuksien tehokas toteuttaminen on eräs GDPR:n tärkeimmistä päämääristä. Kuten esimerkiksi edellä kappaleessa 4.3 on todettu, rekisteröidyt voivat koska tahansa peruuttaa suostumuksensa. Tämä pätee kaikkiin tilanteisiin, joissa henkilötietojen käsittelyn oikeusperusteena on suostumus.

Rekisteröidyn oikeuksien käyttäminen on mahdollistettava silloinkin, kun se voi haitata puolesta-asioinnin ja käyttäjien tunnistamisen toteuttamista. Tätä saatetaan joutua arvioimaan erityisesti GDPR 17 artiklan mukaisen rekisteröidyn poisto-oikeuden kannalta. 17 artiklan mukaan rekisteröidyllä on tietyin edellytyksin oikeus saada rekisterinpitäjä poistamaan rekisteröityä koskevat henkilötiedot ja rekisterinpitäjällä on velvollisuus poistaa tiedot ilman aiheetonta viivytystä.[22] Jos rekisteröity on määrännyt rekisterinpitäjän poistamaan vertailuun perustuvaa tunnistamista varten välttämättömiä tietojaan rajapinnan avaajan palvelusta, eikä vertailua enää ole mahdollista tehdä väärien tunnistusten riskin vuoksi, rajapinnan avaajan on estettävä puolesta-asiointi noudattaakseen eheyden ja luottamuksellisuuden periaatetta. Sama tilanne voi syntyä myös silloin, kun rekisteröity käyttää oikeuttaan poistaa vastaavia tunnisteita rajapinnan hyödyntäjän palvelusta.

Vertailuun perustuva tunnistaminen voi estyä myös silloin, kun rekisteröity käyttää GDPR 16 artiklan mukaista oikeuttaan tietojen oikaisemiseen. Jos rekisteröity oikaisee vertailua varten tarpeellisia henkilötietojaan toisessa vertailuun osallistuvassa palvelussa, mutta ei tee vastaavaa oikaisua toisessa, on mahdollista, että vertailu tosiasiallisesti estyy. Riittävän luotettavan vertailun estyessä osapuolten on estettävä puolesta-asiointi.

GDPR 12(3) artiklan asettama lähtökohta on, että rekisterinpitäjän täytyy vastata poisto- tai oikaisupyynnön tehneelle rekisteröidylle ilman aiheetonta viivytystä, joka tapauksessa kuukauden kuluessa pyynnön vastaanottamisesta. Vastauksessa rekisterinpitäjä kertoo toimenpiteistä, joihin se on pyynnön vuoksi ryhtynyt. Vastauksessa rajapinnan hyödyntäjä tai rajapinnan avaaja voi myös informoida rekisteröityä, että tunnistamista varten tarvittavien tietojen muokkaaminen tai poistaminen voi estää palvelun käytön. Pyynnön toteuttamisen määräaikaa voidaan tarvittaessa jatkaa enintään kahdella kuukaudella ottaen huomioon pyyntöjen monimutkaisuus ja määrä. Mahdollisesta määräajan jatkamisesta, sekä jatkamisen syistä, on kuitenkin ilmoitettava rekisteröidylle kuukauden kuluessa pyynnön vastaanottamisesta.

[22] GDPR 17 artiklassa listataan seuraavat tilanteet, joissa tiedot on pyynnöstä poistettava: 1) henkilötietoja ei enää tarvita niihin tarkoituksiin, joita varten ne kerättiin tai joita varten niitä muutoin käsiteltiin, 2) rekisteröity peruuttaa suostumuksen, johon käsittely on perustunut, eikä käsittelyyn ole muuta laillista perustetta, 3) rekisteröity vastustaa henkilötietojensa käsittelyä suoramarkkinoinnin tarkoituksiin tai käyttää vastustamisoikeuttaan muutoin, eikä käsittelyyn ole olemassa perusteltua syytä, 4) henkilötietoja on käsitelty lainvastaisesti, 5) henkilötiedot on poistettava unionin oikeuteen tai jäsenvaltion lainsäädäntöön perustuvan rekisterinpitäjään sovellettavan lakisääteisen velvoitteen noudattamiseksi, 6) henkilötiedot on kerätty tietoyhteiskunnan palvelujen tarjoamisen yhteydessä lapselle. Tilanteessa, jossa käsittelyn artiklan 6 mukaisena oikeusperusteena toimii rekisterinpitäjän ja rekisteröidyn välinen sopimus, poistovelvollisuutta ei ole, ellei joku edellä luetelluista kriteereistä toteudu. Tässä tilanteessa rekisterinpitäjän on kuitenkin syytä tarjota mahdollisuutta käyttäjäsopimuksen irtisanomiseen ja käyttäjätilin poistamiseen, jos käyttäjä tätä tahtoo.

Rajapinnan avaajan ja rajapinnan hyödyntäjän on GDPR 19 artiklan mukaisesti ilmoitettava rekisteröidyn pyynnöstä tehdyistä henkilötietojen oikaisusta ja poistosta jokaiselle vastaanottajalle, jolle henkilötietoja on luovutettu, paitsi jos tämä osoittautuu mahdottomaksi tai vaatii kohtuutonta vaivaa. Koska käyttäjätileillä olevien henkilötietojen vertaileminen lähtökohtaisesti sisältää tietojen luovutusta osapuolten välillä, osapuolten on tiedotettava toisiaan vertailussa käytettäviin tietoihin kohdistuneista toteutetuista poisto- ja oikaisupyynnöistä. Näkemyksemme mukaan osapuolilla ei kuitenkaan ole automaattisesti oikeutta luovuttaa toisilleen uusia, rekisteröidyn GDPR 18 artiklan nojalla oikaisemia henkilötietoja, koska on mahdollista, ettei rekisteröity tahdo näitä tietoja luovutettavan edelleen. Osapuolet voivat kuitenkin kysyä rekisteröidyn lupaa korjattujen tietojen luovuttamisesta puolesta-asioinnin toiselle osapuolelle esimerkiksi samalla lomakkeella, jolla rekisteröidyt voivat tehdä oikaisupyyntöjä. Rekisterinpitäjän on ilmoitettava rekisteröidylle näistä vastaanottajista, jos rekisteröity sitä pyytää.

## 12. TIETOSUOJAN VAIKUTUSTENARVIOINTI

Jos henkilötietojen käsittelyyn liittyy korkea riski rekisteröityjen oikeuksille, rekisterinpitäjän on laadittava GDPR 35 artiklan mukainen kirjallinen vaikutustenarviointi ennen käsittelyn aloittamista. Rekisterinpitäjä voi myös hyödyntää vaikutustenarviointia vapaaehtoisesti milloin tahansa, kun se suunnittelee toimintoja, joissa on tarkoitus käsitellä henkilötietoja. Tietosuojavaltuutetun toimisto on julkaissut luonnoksen ohjeeksi tietosuojan vaikutustenarvioinneista.[23]

Korkean riskin käsittelyä on GDPR:n mukaan muun muassa käsittely, johon liittyy:

- luonnollisten henkilöiden henkilökohtaisten ominaisuuksien järjestelmällistä ja kattavaa arviointia, joka perustuu automaattiseen käsittelyyn, kuten profilointiin, ja johtaa päätöksiin, joilla on luonnollista henkilöä koskevia merkittäviä vaikutuksia,
- laajamittaista erityisten henkilötietoryhmien (9(1) artikla) tai rikoksia ja rikkomuksia koskevien tietojen (10 artikla) käsittelyä, tai
- yleisölle avoimen alueen järjestelmällistä valvontaa laajamittaisesti.

GDPR ei kuitenkaan tarjoa tyhjentävää listaa vaan myös muihin käsittelytoimiin voi liittyä korkea riski rekisteröidyille ja ne voivat siten edellyttää vaikutustenarvioinnin laatimista. Tietosuojavaltuutettu on listannut GDPR:a täydentävästi henkilötietojen käsittelyn piirteitä, jotka vaativat vaikutustenarvioinnin laatimista.[24] Vaikutustenarviointi on esimerkiksi tehtävä, jos käsittely sisältää kaksi seuraavista ominaispiirteistä:

- henkilötietojen arviointi tai pisteytys,
- automaattinen päätöksenteko, jolla on oikeusvaikutuksia,
- rekisteröityjen järjestelmällinen valvonta,
- erityisiin henkilötietoryhmiin kuuluvien (9(1) artikla) tai muuten hyvin henkilökohtaisten tietojen käsittely,
- tietojen laajamittainen käsittely,
- tietokokonaisuuksien yhdistäminen,
- heikossa asemassa olevien henkilötietojen käsittely,
- uusien teknisten tai organisatoristen ratkaisujen soveltaminen tai innovatiivinen käyttö.

[23] Tietosuojavaltuutetun toimiston luonnos tietosuojan vaikutustenarviointia koskevaksi ohjeeksi: https://tietosuoja.fi/-/tietosuojavaltuutetun-toimisto-pyytaa-kommentteja-uudesta-tietosuojan-vaikutustenarviointia-koskevasta-ohjeesta

[24] Tietosuojavaltuutetun verkkosivuilla julkaistu listaus korkean riskin käsittelystä: https://tietosuoja.fi/vaikutustenarviointi.

Rajapinnan avaajan ja rajapinnan hyödyntäjän valitsemasta puolesta-asioinnin ja käyttäjätilien vertailun tavasta riippuen yllä listatuista voivat toteutua esimerkiksi tietojen laajamittainen käsittely, tietokokonaisuuksien yhdistäminen, erityisiin henkilötietoryhmiin kuuluvien tai muuten hyvin henkilökohtaisten tietojen käsittely sekä uusien teknisten tai organisatoristen ratkaisujen soveltaminen tai innovatiivinen käyttö. Voidaan siis katsoa, että GDPR 35 artiklan mukainen vaikutustenarviointi tulee laadittavaksi varsin monissa puolesta-asiointimalleissa. Rajapinnan avaaja ja rajapinnan hyödyntäjä voivat joko arvioida velvollisuutensa toteuttaa vaikutustenarviointi ja laatia arvioinnin tahoillaan, tai sopia arvioinnin toteuttamisesta yhdessä siten, että se käsittää koko vertailumalliin perustuvan puolesta-asioinnin kokonaisuuden.

Vaikutustenarvioinnissa on käytävä läpi seuraavat kartoitettua henkilötietojen käsittelyä koskevat asiat:

- kuvaus suunnitelluista käsittelytoimista ja käsittelyn tarkoituksista,
- arvio käsittelytoimien tarpeellisuudesta ja oikeasuhteisuudesta tarkoituksiin nähden,
- arvio rekisteröityjen oikeuksia ja vapauksia koskevista riskeistä,
- suunnitellut toimenpiteet riskeihin puuttumiseksi sekä sen osoittamiseksi, että GDPR:a on noudatettu.

Bird & Bird

**LIITE 1: KOOSTE SUOSITUKSISTA**

| Tietosuojavelvoite | Velvoitteen merkitys puolesta-asioinnin vertailumallissa | Suositus rajapinnan hyödyntäjälle | Suositus rajapinnan avaajalle | Puolesta-asioinnin vaihe |
|---|---|---|---|---|
| GDPR 24 ja 26 artiklat: Tietosuojaroolien määritys ja yhteisrekisterinpitäjyyteen liittyvät velvoitteet<br><br>Kappale 2 | Rajapinnan avaajan ja rajapinnan hyödyntäjän on tunnistettava tietosuojaroolinsa ja rooleihin liittyvät vastuunsa vertailumallia hyödyntävään puolesta-asiointiin liittyvässä henkilötietojen käsittelyssä.<br><br>Jos osapuolet toteavat olevansa yhteisrekisterinpitäjiä vertailuun liittyvän henkilötietojen käsittelyn suhteen, niiden on sovittava yhteiseen käsittelyyn liittyvistä vastuistaan sopimuksessa. | Viesti tietosuojarooli rekisteröidyille tietosuojaselosteessa. Lähtökohtaisesti rajapinnan hyödyntäjä toimii puolesta-asioinnissa itsenäisenä rekisterinpitäjänä.<br><br>Totea käyttäjätilien vertailuun liittyvä yhteisrekisterinpitäjyys rajapinnan avaajan kanssa ja laadi sopimus yhteisrekisterinpitäjyydestä. | Viesti tietosuojarooli rekisteröidyille tietosuojaselosteessa. Lähtökohtaisesti rajapinnan avaaja toimii puolesta-asioinnissa itsenäisenä rekisterinpitäjänä.<br><br>Totea käyttäjätilien vertailuun liittyvä yhteisrekisterinpitäjyys rajapinnan hyödyntäjän kanssa ja laadi sopimus yhteisrekisterinpitäjyydestä. | Vaihe 1. Rajapinnan avaaja ja rajapinnan hyödyntäjä solmivat sopimuksen puolesta-asiointirajapinnan hyödyntämisestä |
| GDPR 5(1)(a) artikla: Lainmukaisuus<br><br>Kappale 4 | Henkilötietojen käsittelyn on perustuttava GDPR 6 artiklan mukaiseen oikeusperusteeseen. Puolesta-asioinnin ja siihen liittyvän käyttäjätilien vertailun oikeusperusteena voi toimia sopimus tai suostumus. | Jos käsittelyn oikeusperusteeksi on valittu sopimus, varmista, että rekisteröidyn kanssa tehty käyttäjäsopimus mainitsee ja mahdollistaa puolesta-asiointiin sekä käyttäjätilien vertailuun vaadittavan henkilötietojen käsittelyn. Jos näin ei ole tee uusi käyttäjäsopimus rekisteröidyn kanssa ja informoi selkeästi sopimukseen tehdyistä muutoksista.<br><br>Jos käsittelyn oikeusperusteeksi on valittu rekisteröidyn suostumus, varmista, että suostumus täyttää GDPR:n vaatimukset, esimerkiksi rekisteröidyn informoinnista suostumuksen yhteydessä (ks. kappale | Jos käsittelyn oikeusperusteeksi on valittu sopimus, varmista, että rekisteröidyn kanssa tehty käyttäjäsopimus mainitsee ja mahdollistaa puolesta-asiointiin sekä käyttäjätilien vertailuun vaadittavan henkilötietojen käsittelyn. Jos näin ei ole tee uusi käyttäjäsopimus rekisteröidyn kanssa ja informoi selkeästi sopimukseen tehdyistä muutoksista.<br><br>Jos käsittelyn oikeusperusteeksi on valittu rekisteröidyn suostumus, varmista, että suostumus täyttää GDPR:n vaatimukset, esimerkiksi rekisteröidyn informoinnista suostumuksen yhteydessä (ks. kappale | Vaihe 2. Rekisteröidyllä on käyttäjätili/luo käyttäjätilin rajapinnan avaajan palveluun<br><br>Vaihe 3. Rekisteröidyllä on käyttäjätili/luo käyttäjätilin rajapinnan hyödyntäjän palveluun<br><br>Vaihe 4. Rekisteröity tekee pyynnön puolesta-asiointipalvelun käyttöönotosta rajapinnan hyödyntäjälle |

Bird & Bird

**LIITE 1: KOOSTE SUOSITUKSISTA**

| Tietosuojavelvoite | Velvoitteen merkitys puolesta-asioinnin vertailumallissa | Suositus rajapinnan hyödyntäjälle | Suositus rajapinnan avaajalle | Puolesta-asioinnin vaihe |
|---|---|---|---|---|
| | | 4.3). Varmista, että rekisteröity voi aina peruuttaa suostumuksensa yhtä helposti kuin on sen antanutkin. Varmista, että suostumuksia hallinnoidaan järjestelmässä, josta on mahdollista todentaa yksittäisen rekisteröidyn antama tai peruuttama suostumus. | 4.3). Varmista, että rekisteröity voi aina peruuttaa suostumuksensa yhtä helposti kuin on sen antanutkin. Varmista, että suostumuksia hallinnoidaan järjestelmässä, josta on mahdollista todentaa yksittäisen rekisteröidyn antama tai peruuttama suostumus. | |
| GDPR 5(1)(a) artikla: Läpinäkyvyys ja asianmukaisuus<br><br>Kappale 5 | Rekisteröidyn on tiedettävä, miten hänen henkilötietojaan käsitellään puolesta-asioinnin toteuttamisessa ja mitkä toimijat käsittelyyn osallistuvat. Käsittelytoimet eivät saa tulla rekisteröidylle yllätyksenä hänen oikeutettuihin odotuksiinsa nähden.<br><br>Rajapinnan hyödyntäjän ja rajapinnan avaajan on annettava rekisteröidyille GDPR 13 ja 14 artikloissa määritetyt tiedot. | Päivitä tietosuojaselosteeseen kuvaus vertailumallissa vaadittavasta henkilötietojen käsittelystä ja saata selosteen muutos rekisteröityjen tietoon. Pidä seloste rekisteröityjen saatavilla. | Päivitä tietosuojaselosteeseen kuvaus vertailumallissa vaadittavasta henkilötietojen käsittelystä ja saata selosteen muutos rekisteröityjen tietoon. Pidä seloste rekisteröityjen saatavilla. | Vaihe 2. Rekisteröidyllä on käyttäjätili/luo käyttäjätilin rajapinnan avaajan palveluun<br><br>Vaihe 3. Rekisteröidyllä on käyttäjätili/luo käyttäjätilin rajapinnan hyödyntäjän palveluun<br><br>Läpi palvelun elinkaaren. |

Bird & Bird

**LIITE 1: KOOSTE SUOSITUKSISTA**

| Tietosuojavelvoite | Velvoitteen merkitys puolesta-asioinnin vertailumallissa | Suositus rajapinnan hyödyntäjälle | Suositus rajapinnan avaajalle | Puolesta-asioinnin vaihe |
|---|---|---|---|---|
| GDPR 5(1)(b) artikla: Käyttötarkoitussidonnaisuus<br><br>Kappale 6 | Rajapinnan avaajan ja rajapinnan hyödyntäjän on määritettävä puolesta-asiointia ja vertailua varten käsittelemiensä henkilötietojen käsittelytarkoitus ja kerrottava alusta asti rekisteröidylle selkeästi, mihin tarkoitukseen hänen henkilötietojaan kerätään ja muuten käsitellään. Jos muita tarkoituksia varten kerättyjä henkilötietoja ryhdytään käsittelemään puolesta-asiointia ja vertailua varten, käsittelylle on varmistettava uusi oikeusperuste tai varmistettava uuden käyttötarkoituksen yhteensopivuus vanhan tarkoituksen kanssa. | Jos henkilötietojen käsittely perustuu suostumukseen, pyydä uuteen käsittelytarkoitukseen, kuten käyttäjätilien vertailuun, uusi suostumus.<br><br>Jos henkilötietojen käsittely perustuu vanhaan käyttäjäsopimukseen, tee rekisteröidyn kanssa uusi käyttäjäsopimus, joka huomioi puolesta-asioinnin ja käyttäjätilien vertailun, tai erillinen suostumus.<br><br>Rekisterinpitäjä voi myös arvioida, että alkuperäinen käyttötarkoitus sekä uusi käyttötarkoitus (vertailuun perustuva puolesta-asiointi) ovat yhteensopivia. Ks. arviointikriteerit kappaleesta 6. | Jos henkilötietojen käsittely perustuu suostumukseen, pyydä uuteen käsittelytarkoitukseen, kuten käyttäjätilien vertailuun, uusi suostumus.<br><br>Jos henkilötietojen käsittely perustuu vanhaan käyttäjäsopimukseen, tee rekisteröidyn kanssa uusi käyttäjäsopimus, joka huomioi puolesta-asioinnin ja käyttäjätilien vertailun, tai erillinen suostumus.<br><br>Rekisterinpitäjä voi myös arvioida, että alkuperäinen käyttötarkoitus sekä uusi käyttötarkoitus (vertailuun perustuva puolesta-asiointi) ovat yhteensopivia. Ks. arviointikriteerit kappaleesta 6. | Molempien osapuolten on huomioitava mahdolliset uudet käyttötarkoitukset jo puolesta-asiointipalvelua suunniteltaessa.<br><br>Käyttötarkoitussidonnaisuus on oltava taattuna viimeistään seuraavien vaiheiden alkaessa:<br><br>Vaihe 4. Rekisteröity tekee pyynnön puolesta-asiointipalvelun käyttöönotosta rajapinnan hyödyntäjälle<br><br>Vaihe 5. Rajapinnan hyödyntäjä ja rajapinnan avaaja perustavat puolesta-asiointisuhteen ko. rekisteröidyn osalta |
| GDPR 5(1)(c) artikla: Tietojen minimointi<br><br>Kappale 7 | Puolesta-asiointiin liittyvässä vertailussa rajapinnan hyödyntäjän ja rajapinnan avaajan on käsiteltävä niin vähän henkilötietoja kuin mahdollista, jotta rekisteröidyn henkilöllisyys voidaan varmistaa | Suunnittele puolesta-asioinnin ja käyttäjätilien vertailun toteuttaminen siten, että siinä käsitellään mahdollisimman vähän henkilötietoja.<br><br>Vertailussa tulisi esimerkiksi suosia hajauttamista (”hashing”) tai muita menetelmiä, joiden avulla minimoidaan | Suunnittele puolesta-asioinnin ja käyttäjätilien vertailun toteuttaminen siten, että siinä käsitellään mahdollisimman vähän henkilötietoja.<br><br>Vertailussa tulisi esimerkiksi suosia hajauttamista (”hashing”) tai muita menetelmiä, joiden avulla minimoidaan | Molempien osapuolten on huomioitava tietojen minimointi jo puolesta-asiointipalvelua suunniteltaessa. Käyttäjätilien vertailun osalta tietojen minimointi |

Bird & Bird

**LIITE 1: KOOSTE SUOSITUKSISTA**

| Tietosuojavelvoite | Velvoitteen merkitys puolesta-asioinnin vertailumallissa | Suositus rajapinnan hyödyntäjälle | Suositus rajapinnan avaajalle | Puolesta-asioinnin vaihe |
|---|---|---|---|---|
| | liikennepalvelulain vaatimalla tasolla. | henkilötietojen luovutus osapuolten välillä. | henkilötietojen luovutus osapuolten välillä. | on huomioitava erityisesti seuraavissa vaiheissa:<br><br>5. Rajapinnan hyödyntäjä ja rajapinnan avaaja perustavat puolesta-asiointisuhteen ko. rekisteröidyn osalta<br><br>6. Rajapinnan hyödyntäjä hankkii rekisteröidyn pyynnöstä rajapinnan avaajan liikkumispalvelun käyttäjätiliä hyödyntäen rekisteröidyn henkilökohtaisia matkustusoikeuksia itselleen, ja veloittaa itse rekisteröityä |
| GDPR 5(1)(d) artikla: Täsmällisyys<br><br>Kappale 8 | Käyttäjätilien vertailu on toteutettava siten, ettei vääriä tunnistuksia synny, eikä vääriä henkilötietoja siten käsitellä. Käsiteltävien henkilötietojen on oltava täsmällisiä ja tarvittaessa päivitettyjä. | Varmistu siitä, että molempien osapuolten käyttäjätilien tietokannat sisältävät riittävät tiedot ja ovat yhteensopivia, määrämuotoisia ja mielellään vahvasti tunnistettuja riittävän luotettavan tunnistamisen varmistamiseksi.<br><br>Puolesta-asioinnin yhteydessä voidaan pitää erityisen tärkeänä, että käyttäjätilien vertailussa käytettävien tunnisteiden täsmällisyydestä on | Varmistu siitä, että molempien osapuolten käyttäjätilien tietokannat sisältävät riittävät tiedot ja ovat yhteensopivia, määrämuotoisia ja mielellään vahvasti tunnistettuja riittävän luotettavan tunnistamisen varmistamiseksi.<br><br>Puolesta-asioinnin yhteydessä voidaan pitää erityisen tärkeänä, että käyttäjätilien vertailussa käytettävien tunnisteiden täsmällisyydestä on | Molempien osapuolten on huomioitava täsmällisyyden periaate jo puolesta-asiointipalvelua suunniteltaessa. Käyttäjätilien vertailun osalta täsmällisyys on huomioitava erityisesti seuraavissa vaiheissa:<br><br>5. Rajapinnan hyödyntäjä ja rajapinnan avaaja |

Bird & Bird

**LIITE 1: KOOSTE SUOSITUKSISTA**

| Tietosuojavelvoite | Velvoitteen merkitys puolesta-asioinnin vertailumallissa | Suositus rajapinnan hyödyntäjälle | Suositus rajapinnan avaajalle | Puolesta-asioinnin vaihe |
|---|---|---|---|---|
| | | varmistuttu. Täsmällisyyden periaatteen noudattaminen voi siten edellyttää esimerkiksi vertailussa käytettävän puhelinnumeron ja sähköpostiosoitteen kaksivaiheista vahvistamista.<br><br>Vaikka tietojen minimoinnin periaate edellyttää pidättyväistä suhtautumista uusien henkilötietojen keräämiseen, osapuolet voivat todeta, että rekisteröidyn riittävän tarkka tunnistaminen liikennepalvelulain ja täsmällisyyden periaatteen edellyttämällä tavalla vaatii uusien henkilötietojen käsittelemistä. | varmistuttu. Täsmällisyyden periaatteen noudattaminen voi siten edellyttää esimerkiksi vertailussa käytettävän puhelinnumeron ja sähköpostiosoitteen kaksivaiheista vahvistamista.<br><br>Vaikka tietojen minimoinnin periaate edellyttää pidättyväistä suhtautumista uusien henkilötietojen keräämiseen, osapuolet voivat todeta, että rekisteröidyn riittävän tarkka tunnistaminen liikennepalvelulain ja täsmällisyyden periaatteen edellyttämällä tavalla vaatii uusien henkilötietojen käsittelemistä. | perustavat puolesta-asiointisuhteen ko. rekisteröidyn osalta<br><br>6. Rajapinnan hyödyntäjä hankkii rekisteröidyn pyynnöstä rajapinnan avaajan liikkumispalvelun käyttäjätiliä hyödyntäen rekisteröidyn henkilökohtaisia matkustusoikeuksia itselleen, ja veloittaa itse rekisteröityä |
| GDPR 5(1)(f) artikla: Eheys ja luottamuksellisuus<br><br>Kappale 9 | Eheyden ja luottamuksellisuuden periaate vaatii rajapinnan avaajaa ja rajapinnan hyödyntäjää ehkäisemään asianmukaisilla turvatoimilla riskejä, joita esimerkiksi käyttäjätilien virheellinen yhdistäminen sekä tietovuodot voisivat aiheuttaa. Lisäksi rajapinnan avaajan ja rajapinnan hyödyntäjän on pyrittävä estämään puolesta-asioinnin hyväksikäyttö siten, että toinen henkilö pystyisi ostamaan lippuja rekisteröidyn nimiin | Suunnittele ja toteuta puolesta-asiointi ja vertailu mahdollisimman tietoturvallisesti. Ota käyttöön asianmukaiset tekniset ja organisatoriset toimet turvallisuuden takaamiseksi. Esimerkkeinä: salaus, tiivisteet (”hashit”) tai muut tunnisteet (esim. ”tokenit”). Vahva sähköinen tunnistaminen käyttäjätilejä perustettaessa. | Suunnittele ja toteuta puolesta-asiointi ja vertailu mahdollisimman tietoturvallisesti. Ota käyttöön asianmukaiset tekniset ja organisatoriset toimet turvallisuuden takaamiseksi. Esimerkkeinä: salaus, tiivisteet (”hashit”) tai muut tunnisteet (esim. ”tokenit”). Vahva sähköinen tunnistaminen käyttäjätilejä perustettaessa.<br><br>Hyödynnä liikennepalvelulain mahdollistama tietoturvaan ja luotettavuuteen liittyvän kriteeristö täysimääräisesti rajapinnan hyödyntäjien arvioimisessa ja kriteerit | Molempien osapuolten on huomioitava eheyden ja luottamuksellisuuden periaate jo puolesta-asiointipalvelua suunniteltaessa.<br><br>Rajapinnan avaajan on hyödynnettävä liikennepalvelulain mahdollistamaa tietoturva- ja luotettavuuskriteeristöä rajapinnan hyödyntäjiä arvioidessaan. |

Bird & Bird

**LIITE 1: KOOSTE SUOSITUKSISTA**

| Tietosuojavelvoite | Velvoitteen merkitys puolesta-asioinnin vertailumallissa | Suositus rajapinnan hyödyntäjälle | Suositus rajapinnan avaajalle | Puolesta-asioinnin vaihe |
|---|---|---|---|---|
| | saatuaan haltuunsa hänen henkilötietojaan. | | täyttämättömien toimijoiden pois karsimisessa. | |
| GDPR 5(2) artikla: Osoitusvelvollisuus<br><br>Kappale 10 | Rekisterinpitäjän on pystyttävä osoittamaan noudattavansa tietosuojalainsäädäntöä**.** Käytännössä tämä tarkoittaa kaikkien tässä muistiossa käsiteltyjen toimenpiteiden tekemistä ja dokumentoimista. | Päivitä seuraava dokumentaatio kattamaan puolesta-asiointi ja vertailu ja säilytä se kokonaisuudessaan:<br><br>• Seloste käsittelytoimista (GDPR artikla 30)<br>• Rekisteröidyn informointi, tietosuojaseloste (GDPR artiklat 12-14)<br>• Käsittelyn oikeusperusteeseen liittyvä dokumentaatio, kuten suostumuslomakkeet- ja rekisterit tai käyttäjäsopimus (GDPR artiklat 6-10)<br>• Muut sisäiset ja ulkoiset ohjeistukset (GDPR artiklat 12, 13, 14, 24, 25, 28, 29, 32)<br><br>Tarvittaessa laadi ja säilytä seuraava dokumentaatio:<br><br>• Yhteisrekisterinpitäjyyttä koskevat sopimukset (GDPR artikla 26)<br>• Tietosuojan vaikutustenarviointeja ja tietosuojavaltuutetun ennakkokuulemista koskeva | Päivitä seuraava dokumentaatio kattamaan puolesta-asiointi ja vertailu ja säilytä se kokonaisuudessaan:<br><br>• Seloste käsittelytoimista (GDPR artikla 30)<br>• Rekisteröidyn informointi, tietosuojaseloste (GDPR artiklat 12-14)<br>• Käsittelyn oikeusperusteeseen liittyvä dokumentaatio, kuten suostumuslomakkeet- ja rekisterit tai käyttäjäsopimus (GDPR artiklat 6-10)<br>• Muut sisäiset ja ulkoiset ohjeistukset (GDPR artiklat 12, 13, 14, 24, 25, 28, 29, 32)<br><br>Tarvittaessa laadi ja säilytä seuraava dokumentaatio:<br><br>• Yhteisrekisterinpitäjyyttä koskevat sopimukset (GDPR artikla 26)<br>• Tietosuojan vaikutustenarviointeja ja tietosuojavaltuutetun ennakkokuulemista koskeva | Molempien osapuolten on huomioitava osoitusvelvollisuus jo puolesta-asiointipalvelua suunniteltaessa sekä läpi palvelun elinkaaren. |

Bird & Bird

**LIITE 1: KOOSTE SUOSITUKSISTA**

| Tietosuojavelvoite | Velvoitteen merkitys puolesta-asioinnin vertailumallissa | Suositus rajapinnan hyödyntäjälle | Suositus rajapinnan avaajalle | Puolesta-asioinnin vaihe |
|---|---|---|---|---|
| | | dokumentaatio (GDPR artiklat 35 ja 36) | dokumentaatio (GDPR artiklat 35 ja 36) | |
| Rekisteröityjen oikeudet, erityisesti GDPR 17 artiklan rekisteröidyn poisto-oikeus sekä GDPR 16 artiklan mukainen oikeus tietojen oikaisemiseen.<br><br>Kappale 11 | Rekisteröidyn oikeuksien käyttäminen on mahdollistettava silloinkin, kun se voi haitata puolesta-asioinnin ja käyttäjien tunnistamisen toteuttamista. | Tiedota rajapinnan avaajaa vertailussa käytettäviin tietoihin kohdistuneista toteutetuista poisto- ja oikaisupyynnöistä. | Tiedota rajapinnan hyödyntäjää vertailussa käytettäviin tietoihin kohdistuneista toteutetuista poisto- ja oikaisupyynnöistä.<br><br>Jos rekisteröity määrää poistamaan vertailun kannalta välttämättömät tietonsa rajapinnan avaajan palvelussa tai oikaisee tietojaan, puolesta-asiointi on estettävä riittävän luotettavan vertailun estyessä. | Rekisteröity voi käyttää poisto- tai oikaisuoikeuttaan missä tahansa puolesta-asioinnin vaiheessa. |
| GDPR 35 artikla: Tietosuojan vaikutustenarviointi<br><br>Kappale 12 | Jos henkilötietojen käsittelyyn liittyy korkea riski rekisteröityjen oikeuksille, rekisterinpitäjän on laadittava tietosuojan vaikutustenarviointi ennen käsittelyn aloittamista. Rekisterinpitäjä voi myös hyödyntää vaikutustenarviointia vapaaehtoisesti milloin tahansa, kun se suunnittelee toimintoja, joissa on tarkoitus käsitellä henkilötietoja. Ks. kappale 12 riskin arvioinnista. | Jos henkilötietojen käsittely aiheuttaa korkean riskin (ks. kappale 12 riskin arvioinnista), laadi kirjallinen tietosuojan vaikutustenarviointi, joko itsenäisesti tai yhteistyössä rajapinnan avaajan kanssa. | Jos henkilötietojen käsittely aiheuttaa korkean riskin (ks. kappale 12 riskin arvioinnista), laadi kirjallinen tietosuojan vaikutustenarviointi, joko itsenäisesti tai yhteistyössä rajapinnan hyödyntäjän kanssa.<br><br>Erityisesti rajapinnan avaajalle voi olla suositeltavaa laatia vaikutustenarviointi myös vapaaehtoisesti rajapinnan avaamisen suunnitteluvaiheessa. Tämä helpottaa tietosuojariskien arviointia ja edesauttaa osoitusvelvollisuuden toteuttamista. | Vaikutustenarvioinnin tarve on arvioitava ja arviointi tarvittaessa toteutettava ennen käyttäjätilien vertailun ja puolesta-asioinnin aloittamista. |

Bird & Bird

**LIITE 2: SELVITYKSEN RAJAUKSET**

Selvityksen kohteena ovat ainoastaan tietosuojalainsäädännön vaatimukset puolesta-asioinnin eri vaiheissa puolesta-asioijan ja rajapinnan avaajan näkökulmista. Tietosuojalainsäädännöllä tarkoitetaan GDPR:a ja tietosuojalakia. Esimerkiksi pelkästään viranomaistahoihin sovellettavat sekä sektorikohtaiset tietosuojavelvoitteet on rajattu selvityksen ulkopuolelle. Selvitys perustuu tämänhetkiseen käsitykseemme tietosuoja-asetuksen ja tietosuojalain tulkinnasta sekä Euroopan tietosuojaviranomaisista koostuvan Euroopan tietosuojaneuvoston (EDPB) antamiin suosituksiin, jotka on annettu tämän selvityksen päiväykseen mennessä.

Selvityksen ulkopuolelle on rajattu muiden kuin vertailumalliin perustuvien puolesta-asiointimallien tietosuojaa koskeva arviointi. Selvityksen ulkopuolelle on rajattu myös yleinen sopimusoikeudellinen neuvonta, kuten vastuunrajoitukset osapuolten välisissä sopimuksissa, sekä sopimusmallien laatiminen. Selvitys ei ota kantaa toimijoiden välittömän puolesta-asiointisuhteen ulkopuolisiin sopimusjärjestelyihin, kuten kolmansien osapuolten kanssa tehtyihin sopimuksiin ja alihankintajärjestelyihin. Selvityksessä ei myöskään käsitellä yksityiskohtaisesti erityisiin henkilötietoryhmiin liittyviä kysymyksiä.

Olemme käyttäneet harkintaamme niiden seikkojen korostamisessa, jotka ovat meidän näkemyksemme mukaan olennaisia. Selvityksen havainnot ja suositellut toimenpiteet perustuvat riskin arviointiin yleisellä tasolla. Jokainen puolesta-asiointisuhde on kuitenkin olosuhteiltaan yksilöllinen. Viimesijainen arviointi riskeistä kussakin yksittäistapauksessa kuuluu rekisterinpitäjälle.