Viestintäviraston julkaisun 004/2018 J LIITE

Taustaselvitys: Tietosuoja, tietoturva ja sopijapuolen luotettavuudesta varmistuminen

Viestintävirasto

Sisältö

1 Johdanto

Viestintäviraston julkaisun 004/2018 J *Lippu-hankkeen selvitys liikennepalvelulain matkaketjujen sopimuskäytännöistä* kohdissa 8, 9 ja 10 on lyhyet yhteenvedot tietosuojaan, tietoturvaan ja sopijapuolten luotettavuuden varmistamiseen liittyvistä asioista, joita toimijoiden on hyvä ottaa huomioon sopimuksia solmiessaan.

Tässä taustaselvityksessä käsitellään asiakokonaisuudet yksityiskohtaisemmin. Mukana ovat sekä puolesta-asiointiin liittyvät havainnot että Viestintäviraston julkaisussa 004/2017 J *Lippu-hankkeen selvitys liikennepalvelu-lain matkaketjujen sopimuskäytännöistä (Matkaketjujen käytännesäännöt)* käsitellyt kertalipun myyntirajapintaan liittyvät havainnot.

Tämän taustaselvityksen aiheisiin liittyvät Dittmar & Indreniuksen oikeudelliset selvitykset 2017 ja 2018 henkilötietojen käsittelystä ja LIITE LIPPU-API: Security Considerations. ADDITION 2018: informative list of standards, specifications or frameworks.

Liikkumispalveluverkostolla tarkoitetaan tässä liikennepalvelulain mukaisten liikkumispalveluiden tarjoajien keskinäisiä sopimussuhteita ja yhteistyötä, jotka mahdollistavat yhtenäisten matkaketjujen ja puolesta-asioinnin tarjoamisen matkustajille.

1 Henkilötietojen käsittely (tietosuoja)

1.1 Säännökset ja valvonta

Liikennepalvelulain III osan 2 luvun 4 §:ssä säädetään yleisellä tasolla yksityisyyden suojasta ja tietosuojasta huolehtimisesta rajapintojen avaamisessa.

Henkilötietojen suojasta säädetään Euroopan unionin yleisessä tietosuoja-asetuksessa (EU) 2016/679. Henkilötietojen suojaa koskevaa lainsäädäntöä sovelletaan aina silloin, kun käsitellään henkilötietoja.

Toimivaltainen viranomainen tietosuoja-asetuksen valvonnassa on tietosuojavaltuutettu, joten Liikenne- ja viestintävirasto ei voi ratkaista sitä, mikä täyttää tietosuoja-asetuksen vaatimukset.

Toimijoiden tueksi on hankittu oikeudelliset asiantuntijaselvitykset sekä kertalipun myyntirajapinnan avaamisessa että puolesta-asioinnissa. Puolesta-asiointia koskeva selvitys antaa käytännössä ohjeita myös järjestelmien suunnittelulle (esim. käytettävien attribuuttien minimointi, lokitus, säilytysaikojen määrittely, massaluovutusten tarkka harkinta).

> Tässä käytännesääntöjen taustaselvityksen henkilötietojen käsittelyä koskevassa jaksossa **selvityksellä** viitataan Dittmar & Indreniuksen tekemiin oikeudellisiin selvityksiin henkilötietojen käsittelystä matkaketjussa ja puolesta-asioinnissa.

Tämä käytännesääntöjen taustaselvityksen henkilötietojen käsittelyä koskeva osio on laadittu tietosuoja-asetuksen soveltamisen näkökulmasta käyttäen siinä määriteltyjä käsitteitä ja käsittelyperusteita.

1.2 Henkilötiedon käsite ja henkilötiedot liikkumispalveluverkostossa

1.2.1 Henkilötiedon määritelmä

Henkilötiedolla tarkoitetaan tietosuoja-asetuksen 4 artiklan 1 kohdan 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.

Henkilötiedon määritelmä on hyvin laaja. Kun matkustajalle tarjotaan matkaketjupalveluita, syntyy yleensä tilanne, jossa käsitellään henkilötietoja. Tällaisina tietoina pidetään esimerkiksi tilauksen tekemisen yhteydessä käsiteltäviä matkustajan yhteystietoja ja luottokorttitiedot. Henkilötietoja voivat olla myös matkustusoikeuden todentamiseen liittyvät tiedot.

Tietosuojasääntely soveltuu siten laajasti liikkumispalveluverkoston toimintaan.

1.2.2 Pseudonymisointi ja anonymisointi

On huomattava, että vaikka tiedot pseudonymisoitaisiin, niitä pidetään edelleen henkilötietoina. Vaikka yksittäisellä matkaketjun toimijalla ei olisikaan mahdollisuutta selvittää matkustajan identiteettiä, on riittävää, että joku taho voi eri tietoja yhdistelemällä tunnistaa henkilön. Näin ollen esimerkiksi matkatunniste, joka ei sisällä matkustajan nimeä tai muuta selkeää henkilötietoa, mutta on jonkun toimijan yhdistettävissä yksittäiseen matkustajaan, on henkilötieto.

Poikkeuksellisesti voi olla mahdollista, että liikkumispalveluverkoston joku toimija ei käsittelisi henkilötietoja matkaketjussa. Mikäli tieto on anonymisoitu tai sellaista, ettei sitä voida suoraan ja epäsuoraan yhdistää luonnolliseen henkilöön, jää se henkilötietosääntelyn ulkopuolella.

Tieto on anonyymiä, mikäli henkilötiedot muutetaan peruuttamattomasti sellaiseen muotoon, ettei rekisteröity ole niistä suoraan tai epäsuoraan tunnistettavissa kenenkään toimesta. EU:n tietosuojavaltuutettujen muodostama tietosuojatyöryhmä (WP 29) on lausunnossaan (5/2014) anonymisointitekniikoista todennut, että anonymisointi tapahtuu käsittelemällä henkilötietoja siten, että henkilön tunnistaminen estyy peruuttamattomasti. (ks. myös HE 145/2017, 2.1.1.9 Henkilötietojen anonymisointi).

1.3 Rekisterinpitäjän ja käsittelijän asemat

Henkilötietojen käsittelyyn liittyy eri rooleja.

- Rekisterinpitäjänä pidetään toimijaa, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.

- Käsittelijällä tarkoitetaan tahoa, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Käsittely tapahtuu tällöin usein toimeksianto-, alihankinta- tai yhteistyösuhteessa.

- Rekisterinpitäjät voivat olla myös rinnakkaisia, jolloin kullakin rekisterinpitäjällä on itsenäinen oikeus käsitellä henkilötietoja.

Rekisterinpitäjä määrittelee tietojenkäsittelyn tarkoitukset itsenäisesti sekä hyödyntää tietoja omiin käyttötarkoituksiinsa omien tietojenkäsittelymenettelyidensä mukaisesti. Käsittelijä sitä vastoin ei käsittele tietoja omiin käyttötarkoituksiinsa, vaan käsittelee niitä rekisterinpitäjän antamien ohjeiden ja rekisterinpitäjän kanssa tehdyn sopimuksen mukaisesti pelkästään rekisterinpitäjän lukuun. Käsittelijä ei myöskään saa itsenäistä käyttöoikeutta tietojen hyödyntämiseen.

Rekisterinpitäjän on muun muassa informoitava rekisteröityjä suorittamastaan tietojenkäsittelystä. Tiedot on annettava ymmärrettävässä ja selkeässä muodossa. Tietosuoja-asetuksessa on säädetty tarkemmin annettavien tietojen sisällöstä. Näitä ovat esimerkiksi rekisterinpitäjän yhteystiedot, tieto käsittelyn tarkoituksesta ja sen perusteesta sekä tiedot rekisteröidyn oikeuksista. Osapuolet voivat kuitenkin myös sopia keskinäisistä vastuistaan esimerkiksi siten, että sopimuskumppani velvoitetaan huolehtimaan rekisteröityjen informoimisesta.

Kun tietoja luovutetaan rekisterinpitäjältä toiselle rekisterinpitäjälle, tiedot luovuttava taho vastaa luovutuksen lainmukaisuudesta.

1.3.1 Roolit matkaketjuissa

Liikkumispalveluverkostossa MaaS-operaattori kokonaispalvelun tarjoajana toimii rekisterinpitäjänä suhteessa matkustajista kerättyihin henkilötietoihin.

MaaS-operaattori välittäjänä sekä kuljetuspalvelun tarjoajat voivat toimia rekisterinpitäjänä ja/tai käsittelijänä riippuen siitä, miten tietoja kulloinkin käsitellään ja mitä kunkin toimijan tehtävistä ja roolista on sovittu. Rooleja arvioidaan kuitenkin aina tosiasiallisen tietojenkäsittelytoiminnan perusteella ja tapauskohtaisesti. Lainsäädännön perusteella määräytyvästä roolista ei voida sopimuksella poiketa.

1.3.2 Roolit puolesta-asioinnissa

Oikeudellisen selvityksen perusteella toimijoiden roolit henkilötietojen käsittelyssä vaikuttavat selviltä. Selvityksen perusteella toimijat ovat luonnollisen henkilön käyttäjätilin puolesta-asioinnissa oletusarvoisesti itsenäisiä rekisterinpitäjiä. Tällöin toimijat vastaavat oletusarvoisesti kukin henkilötietojen käsittelystä.

Tietosuoja-asetuksessa ei nimenomaisesti puhuta rinnakkaisista rekisterinpitäjistä, mutta käytännön soveltamisessa vastuut voi arvioida rinnakkaisten rekisterinpitäjien suhteena. Rinnakkaisten rekisterinpitäjien välillä sovittavia asioita käsitellään jäljempänä.

Arvio rooleista **luonnollisen henkilön** käyttäjätilin tietojen käsittelyssä:

- Käyttäjä: rekisteröity
- Puolesta-asioija (yhdistämis- tai liikkumispalvelu): itsenäinen rekisterinpitäjä

- Pääsyn avaaja (liikkumis- tai yhdistämispalvelu): itsenäinen rekisterinpitäjä
- Pääsyn avaaja (liikkumis- tai yhdistämispalvelun puolesta lippu- ja maksujärjestelmästä vastaava toimija: riippuu liikkumis- tai yhdistämispalvelun ja lippu- ja maksujärjestelmästä vastaavan välisestä sopimuksesta, onko lippu- ja maksujärjestelmästä vastaava toimija itsenäinen rekisterinpitäjä vai käsittelijä. Käsittelijä toimii henkilötietojen käsittelyssä rekisterinpitäjän kanssa tehdyn sopimuksen (tietosuoja-asetuksen 28 art.) mukaisesti ja luovutuksesta toiselle rekisterinpitäjälle päättää ja vastaa rekisterinpitäjä, ei käsittelijä.
- Kolmas alennuksen, korvauksen tai erityisehdon määräytymisperusteisiin liittyviä tietoja hallinnoiva taho: itsenäinen rekisterinpitäjä

Arvio rooleista **oikeushenkilön** käyttäjätiliin liittyvien henkilötietojen käsittelyssä:

- Roolit ovat tietosuoja-asetuksen valossa erilaiset kuin luonnollisen henkilön käyttäjätilin kohdalla.
- Oikeushenkilön eli käyttäjäyrityksen työntekijä, konsultti tms.: rekisteröity
- Oikeushenkilö eli käyttäjäyritys: rekisterinpitäjä
- Puolesta-asioija: voi olla käsittelijä käyttäjäyrityksen lukuun, mutta voi olla myös rekisterinpitäjä
- Pätevä käsittelyperuste on arvioitava roolin perusteella.

1.4 Henkilötietojen käsittelyperusteet ja käyttötarkoitukset

Henkilötietojen käsitteleminen edellyttää aina lainmukaisen käsittelyperusteen olemassaoloa. Henkilötietojen käyttötarkoitukset vaikuttavat käsittelyperusteen valintaan ja määräytymiseen.

Tietosuoja-asetuksen mukaan henkilötietoja saa käsitellä:

(a) rekisteröidyn suostumuksella;

(b) rekisteröidyn ja rekisterinpitäjän välisen sopimuksen täytäntöön panemiseksi;

(c) rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi;

(d) rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaamiseksi;

(e) yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi; tai

(f) rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi.

Henkilötietojen käyttötarkoitukset vaikuttavat käsittelyperusteen valintaan ja määräytymiseen. Käyttötarkoitukset on suunniteltava ja määriteltävä ennen tietojen keräämistä. Liikkumispalveluverkostossa tietoja kerätään pääasiassa palveluiden tarjoamiseksi ja asiakkuudenhoitoa varten. Rekisterinpitäjän on informoitava rekisteröityjä käyttötarkoituksista ennen tietojenkäsittelyn aloittamista. On myös huomioitava, että tietoja saa lähtökohtaisesti käyttää vain etukäteen määriteltyihin käyttötarkoituksiin.

1.4.1 Käsittelyperusteet matkaketjussa

Liikkumispalveluverkostossa henkilötietojen käsittelyperusteena voi pääasiassa tulla kysymykseen sopimuksen täytäntöön paneminen (b) tai oikeutettujen etujen toteuttaminen (f). Myös julkinen matkaketjun toteuttamiseen osallistuva viranomaisena pidettävä taho (kuten kuntayhtymä) voi perustaa henkilötietojen käsittelyn oikeutettuun etuun silloin kun kyse ei ole julkisen vallan käyttämisestä tai muusta julkisten hallintotehtävien hoitamisesta. On mahdollista, että rekisterinpitäjällä on eri tarkoituksissa tapahtuvaan henkilötietojen käsittelyyn useita rinnakkaisia käsittelyperusteita.

Mikäli rekisterinpitäjä haluaa käsitellä palveluiden tarjoamiseksi tarvittavien tietojen lisäksi muita henkilötietoja, saattaa tämä edellyttää rekisteröidyn suostumusta (a). Suostumuksen osalta on olennaista, että se on selkeästi muotoiltu, jotta rekisteröity ymmärtää, mihin hän antaa suostumuksensa. Rekisteröidyn on annettava suostumuksensa vapaaehtoisesti jollakin aktiivisella toimenpiteellä.

1.4.2 Käsittelyperusteet puolesta-asioinnissa

Selvityksen perusteella henkilötietojen käsittelyperusteet puolesta-asioinnissa ovat selkeästi määriteltävissä. Pääsääntöisesti käsittelyperusteena voivat olla sopimuksen täytäntöönpano ja avaamisvelvollisen lakisääteisen velvoitteen noudattaminen. Arkaluonteisten henkilötietojen käsittelyyn tarvitaan kuitenkin rekisteröidyn suostumus.

Pätevä käsittelyperuste on arvioitava jokaisen rekisterinpitäjän oman aseman ja käyttötarkoituksen perusteella. Käsittelyperuste on arvioitava tietosuoja-asetuksen valossa, mikä rajoittaa sopimusvapautta

Henkilötiedon voi luovuttaa rekisterinpitäjälle, jolla on itsellään käsittelyperuste. Pelkkä katseluoikeuskin katsotaan luovutukseksi, vaikka tiedon katsoja ei tallentaisikaan tietoa itse.

Arvio tietosuoja-asetuksen mukaisista käsittelyperusteista:

- Puolesta-asioija: käyttäjän kanssa tehdyn sopimuksen täytäntöönpano
- Avaamisvelvollinen: lakisääteinen velvoite, vaihtoehtoisesti rekisteröidyn kanssa tehdyn sopimuksen täytäntöönpanon valmistelu
- Kolmas taho: lakisääteinen velvoite on säädetty liikennepalvelulaissa vain yleistasoisena yhteistyövelvoitteena. Käsittelyn voi kuitenkin perustaa ainakin avaamisvelvollisen oikeutettuun etuun. (Erityissääntelyn vaikutusta suhteessa liikennepalvelulakiin ei ole arvioitu esim. Kelan osalta).

- Arkaluonteiset tiedot: tarvitaan rekisteröidyn nimenomainen suostumus, koska liikennepalvelulaissa ei ole nimenomaisesti säädetty muuta. Nimenomaisen suostumuksen vaatimukset voi täyttää tekniseltä kannalta esimerkiksi sähköinen allekirjoitus tai kaksivaiheinen varmennus. Voidaan katsoa, että suostumuksen pyytäminen kerran riittää, kunhan se muotoillaan huolellisesti niin että kattaa jatkuvamman puolesta-asioinnin.

1.4.3 Tarpeelliset henkilötiedot puolesta-asioinnissa

Yleinen vaatimus siitä, että käsitellään vain tarpeellisia henkilötietoja, tarkoittaa sitä, että kunkin rekisterinpitäjän on arvioitava, mitä henkilötietoja sillä on tarve käsitellä. Täytyy muistaa, että henkilötietoja voi käyttää tällä tarpeellisuusperusteella vain puolesta-asiointitarkoitukseen, ei esim. markkinointiin.

Tarpeellisuusarviointi edellyttää seuraavia asioita:

- Minimointi: rekisterinpitäjä voi käsitellä vain puolesta-asiointitapahtuman toteuttamiseksi välttämättömiä tietoja. Rekisterinpitäjän on arvioitava, ovatko tiedot tarpeen ja voiko palvelun toteuttaa kohtuudella ilman jotain henkilötietoa. Rekisterinpitäjän on myös varmistettava luovuttaessaan, onko tieto tarpeen saajalle. Mahdolliset massaluovutukset on arvioitava erityisen tarkasti.

- Käyttötarkoitussidonnaisuus: Henkilötietoja voi käyttää vain siihen tarkoitukseen, jos ne on saatu. Puolesta-asioinnin toteuttamiseksi käsiteltäviä henkilötietoja ei voi siten käyttää esimerkiksi markkinointiin.

- Säilytysaika: tiedon säilytysaika on määriteltävä ja tietoa tulee säilyttää vain sen aikaa, kun säilytys on tarpeen oikeutettujen etujen kannalta esim. reklamaatioiden käsittelemiseksi. Tämän jälkeen tieto on poistettava tai anonymisoitava. Henkilötietojen poisto asianmukaisesti on huomioitava myös, jos sopimus päättyy.

1.5 Rekisteröidyn oikeudet

Rekisteröidyllä eli palveluiden käyttäjällä on useita henkilötietojensa käsittelyyn liittyviä oikeuksia. Lähtökohtaisesti jokainen rekisterinpitäjä on itse vastuussa oikeuksien toteuttamisesta keräämiensä tietojen osalta.

Liikkumispalveluverkostossa toimivien tahojen on otettava rekisteröityjen oikeuksien toteuttaminen huomioon sekä omassa toiminnassaan että keskinäisissä sopimuksissaan.

- Rekisterinpitäjän on tietojenkäsittelyn läpinäkyvyyden varmistamiseksi informoitava rekisteröityjä ennen tietojenkäsittelyn aloittamista.

- Mikäli rekisteröidyllä on kysyttävää tietojensa käsittelystä, rekisterinpitäjän on vastattava rekisteröidyn pyyntöihin ilman aiheetonta viivytystä. (Tietosuoja-asetuksessa säädetään määräajoista.)

- Rekisteröidyllä on oikeus tarkastaa, mitä tietoja rekisterinpitäjä hänestä käsittelee sekä oikeus pyytää tietojen poistamista ja oikaisua tai tietojenkäsittelyn rajoittamista.

- Tietyissä tapauksissa rekisteröidyllä on myös oikeus vastustaa tietojen käsittelyä.

- Mikäli tietoja käsitellään sopimuksen toimeenpanemiseksi tai rekisteröidyn suostumuksella, rekisteröidyllä on oikeus siirtää tietonsa järjestelmästä toiseen toiselle rekisterinpitäjälle. Rekisteröidyllä on myös aina oikeus peruuttaa antamansa suostumus tietojenkäsittelyyn.

1.6 Tietosuojasta huolehtimisen vaiheet ja sopiminen puolesta-asioinnissa

1.6.1 Tietosuojasta huolehtimisessa voidaan tunnistaa seuraavat vaiheet:

- Osapuolet arvioivat roolinsa henkilötietojen käsittelyssä
- Kukin rekisterinpitäjä arvioi ja dokumentoi, mitkä ovat tarpeelliset tiedot ja niiden käyttötarkoitus puolesta-asioinnissa
- Kukin rekisterinpitäjä arvioi ja dokumentoi tietojen käsittelyperusteensa
- Kukin rekisterinpitäjä arvioi ja dokumentoi henkilötietojen käsittelynsä tietoturvallisuuden
- Jos henkilötietoja käsittelee toimija (yleensä alihankkija), joka on katsottava käsittelijäksi, rekisterinpitäjä huolehtii käsittelystä sopimisesta tietosuoja-asetuksen 28 artiklaa mukaisesti
- Rinnakkaisten rekisterinpitäjien eli pääsyyn oikeutetun puolesta-asioijan ja avaamisvelvollisen sopimuksessa sovitaan tarpeelliset asiat
- Tuotantovaiheessa henkilötietojen tietoturvaloukkaustilanteessa kukin rekisterinpitäjä selvittää tilanteita ja informoi sopimuskumppania ja rekisteröityä

1.6.2 Rinnakkaisten rekisterinpitäjien sopimus

Rinnakkaisten rekisterinpitäjien on hyvä huomioida sopimuksessaan seuraavat:

- Käsiteltävät henkilötiedot
- Listataan, mitä henkilötietoja ja mihin tarkoitukseen sopimusosapuoli voi puolesta-asioinnissa esim. katsella ja tallentaa
- Rajapinnan avaamisvelvolliselle syntyy tietosuojavelvoitteiden näkökulmasta velvollisuus varmistaa, että luovuttaa tietoja vain sellaiselle, jolla on oikeus käsitellä niitä, huomioidaan siten erityisesti, mikä on henkilötietoja näkevän/saavan käsittelyperuste ja käyttötarkoitus. Sopimuksella luovuttaja voi osoittaa huolehtineensa siitä, että luovuttaa henkilötiedot vain taholle, jolla on oikeus käsitellä niitä.
- Toisen rekisterinpitäjän tietojen eheyden ja luottamuksellisuuden turvaaminen, esimerkiksi mahdollinen lokituksesta sopiminen.
- Käyttäjän/rekisteröidyn oikeuksista huolehtiminen
- Tiedon vaihtaminen rekisterinpitäjien kesken, jos rekisteröity oikaisee tai poistaa tietojaan
- Tiedon vaihtaminen tarvittaessa henkilötietojen tietoturvaloukkaustilanteessa
- Käyttäjän informointi
- Tarvittaessa tietojen säilytysajat

2 Tietoturva

2.1 Säännökset ja valvonta

Liikennepalvelulain III osan 2 luvun 4 §:ssä säädetään tietoturvasta huolehtimisesta rajapintoja avattaessa.

EU:n yleisen tietosuoja-asetuksen 32 artiklassa säädetään henkilötietojen käsittelyn tietoturvallisuudesta.

Liikennepalvelulakia valvoo Liikenne- ja viestintävirasto (ennen vuotta 2019 Liikenteen turvallisuusvirasto Trafi).

Henkilötietojen käsittelyn tietoturvavaatimuksia valvoo tietosuojavaltuutettu.

2.2 Tietoturvan tasosta huolehtiminen eli tietoturvavaatimukset

Rajapinnan ja palvelun tietoturvasta huolehtimiseksi on noudatettava hyviä tietoturvakäytäntöjä.

Tietoturvallisuuden ylläpidolla tarkoitetaan niitä teknisiä ja organisatorisia toimenpiteitä, joita toimija toteuttaa verkko- ja tietojärjestelmien eheydestä, käytettävyydestä ja tiedon luottamuksellisuudesta huolehtimiseksi.

Tietoturvallisuudesta huolehtiminen tarkoittaa jatkuvaa tietoturvallisuuden kokonaisuuden hallintaa ja sitä, että toteutetaan riittävät tietoturvatoimenpiteet tietoliikenne-, tietojärjestelmä- ja käyttöturvallisuudesta sekä fyysisen turvallisuudesta huolehtimiseksi.

Toimenpiteissä on huomioitava tekninen kehitys ja toimenpiteiden kustannukset ja ne on suhteutettava uhkiin ja riskeihin.

2.2.1 Luottamuksellisuus, eheys ja käytettävyys

Tietoturvallisuuden ylläpidolla tarkoitetaan niitä teknisiä ja organisatorisia toimenpiteitä, joita toimija toteuttaa verkko- ja tietojärjestelmien eheyden, käytettävyyden ja tiedon luottamuksellisuuden turvaamiseksi.

- Luottamuksellisuus (*confidentiality*) tarkoittaa sitä, että tietoon pääsevät käsiksi vain siihen oikeutetut. Tämä edellyttää käytännössä sekä tietojen että tietoon oikeutettujen määrittelyä riittävällä tasolla.
    - Esimerkkinä määrittelymallista voidaan mainita *Bell – LaPadula* malli.
- Eheys (*integrity*) tarkoittaa sitä, että tietoa tai järjestelmää ei päästä muuttamaan tai hävittämään oikeudettomasti koko sen elinkaaren aikana ja että muutokset havaitaan.
- Käytettävyys (*availability*) tarkoittaa sitä, että tieto tai järjestelmä on käytettävissä silloin, kun sitä tarvitaan. Käytettävyys tarkoittaa myös käyttötarpeeseen nähden riittävää kapasiteettia.

- Käytännesäännöissä ei eritellä tarkemmin käytettävyysasioita. Toimijat sopivat niistä keskenään huomioiden lain oikeudenmukaisuus, kohtuullisuus- ja syrjimättömyysvaatimukset.

2.2.2 Tietoliikenne-, tietojärjestelmä- ja käyttöturvallisuus ja fyysinen turvallisuus

Hyvät tietoturvakäytännöt kattavat yleisen tietoturvallisuuden hallinnan ja tietoliikenne-, tietojärjestelmä- ja käyttöturvallisuuden sekä fyysisen turvallisuuden.

Kun määritellään riittäviä tietoturvatoimenpiteitä, on hyvä ottaa huomioon soveltuvin osin seuraavan listan osa-alueet.

1) tietoliikenneturvallisuus

   a) verkon rakenteellinen turvallisuus

   b) tietoliikenneverkon vyöhykkeistäminen

   c) suodatussäännöt vähimpien oikeuksien periaatteilla

   d) suodatuksen ja valvontajärjestelmien hallinnointi koko elinkaaren ajan

   e) hallintayhteydet

2) tietojärjestelmäturvallisuus

   a) pääsyoikeuksien hallinta

   b) järjestelmien käyttäjien tunnistaminen

   c) järjestelmien koventaminen

   d) haittaohjelmasuojaus

   e) turvallisuuteen liittyvien tapahtumien jäljitys

   f) poikkeamien havainnointikyky ja toipuminen

   g) kansainvälisesti tai kansallisesti suositellut salausratkaisut

3) käyttöturvallisuus

   a) muutosten hallinta

   b) salassa pidettävän aineiston käsittely-ympäristö

   c) etäkäyttö ja -hallinta

   d) ohjelmistohaavoittuvuuksien hallinta

   e) varmuuskopiointi

4) fyysinen turvallisuus

   a) toimijan omien tilojen fyysiset suojaukset ja kulunvalvonta

b) käytettyjen palveluntarjoajien fyysiset suojaukset ja kulunvalvonta

Sopijapuolten tunnistaminen

Tietoliikenne- ja tietojärjestelmäturvallisuuteen kuuluu se, että sopijapuolet sopivat keskenään osapuolten tunnistamisessa käytettävien varmenteiden tai niiden tunnistetietojen luotettavasta vaihtamisesta ja hallinnasta. Viranomaiset eivät toteuta liikkumispalveluverkostolle keskitettyä varmenteiden hallintaa. Sopijapuolten on noudatettava hallinnassa yleisiä hyviä tietoturvakäytäntöjä ja varmenteet on suositeltavaa myöntää enintään 3 vuodeksi kerrallaan.

2.2.3 Riskiin suhteutetut toimenpiteet

Molemminpuolisesti vaadittavien tietoturvakäytäntöjen lähtökohtana on syytä käyttää uhkamallinnusta ja riskilähtöisyyttä. Lähtötietoina näissä ovat esimerkiksi suojattavien henkilötietojen, maksuvälinetietojen ja taloudellisen riskin määrä - ja toisaalta taloudelliset tappiot tai maineriski, jos palvelu ei ole saatavilla vaikkapa palvelunestotilan vuoksi.

Sopijapuoli voi edellyttää, että toinen sopijapuoli suhteuttaa tekniset ja organisatoriset toimenpiteet tietoturvan ylläpitämiseksi uhan vakavuuteen ja todennäköisyyteen, toimenpiteistä aiheutuviin kustannuksiin sekä käytettävissä oleviin teknisiin mahdollisuuksiin torjua uhka.

Uhan vakavuuden arvioinnissa on otettava huomioon ainakin

- suojattavan tiedon luonne (esimerkiksi henkilötietojen käsittelyn tai sertifikaattien avaintenhallinnan vaatimukset),
- suojattavan toiminnon kriittisyys järjestelmän eheyden kannalta ja
- mahdollisten henkilötietovahinkojen sekä taloudellisten vahinkojen suuruus uhan toteutuessa.

Uhan todennäköisyyden arvioinnissa on otettava huomioon ainakin

- vallitseva ajantasainen tietämys online-verkkopalveluihin,
- sekä niiden taustalla olevaan alustainfrastruktuuriin kohdistuvista tietoturvauhkista.

Uhka-analyysissä suositellaan käytettäväksi jonkin yleisen standardin mukaista viitekehystä.

2.2.4 Standardit ja suositukset

Liikennepalvelulaissa säädettyyn rajapintojen avaamiseen ei liity säädettyjä standardiviittauksia. Standardit eivät siten ole pakollisia tai mikään tietty standardi ei sellaisenaan määrittele tietoturvatasoa, joka täyttää lain vaatimukset.

Standardit kuvaavat kuitenkin yleisesti arvioiden hyviä tietoturvakäytäntöjä. Toimijat voivat hyödyntää niitä omassa toiminnassaan ja sopimuksis-

saan sekä puolesta-asioinnin avaamisessa tarvittavien ennakkokriteeriensä määrittelyssä.

Kertalipun myyntirajapinnan avaamista koskevassa käytännesääntöjen ensimmäisessä versiossa on liitteenä Lippu-projektissa laadittu suositus rajapinnan tietoturvallisesta toteutuksesta (julkaisun 004/207 J LIITE 2 *LIPPU-API: Security Considerations).* Suositus perustuu yleisiin hyvin käytäntöihin ja lähteisiin sekä uhka-analyysinäkökulmaan.

Suositus pätee myös puolesta-asioinnin rajapinnan avaamiseen. Puolesta-asiointi laajentaa tietoturvallisuustarpeita mm. henkilötietojen käsittelyn takia ja tietoturvallisuussuositusta on siksi täydennetty informatiivisilla standardiviittauksilla hyödyllisiin standardeihin. (LIITE *LIPPU-API: Security Considerations. ADDITION 2018: informative list of standards, specifications or frameworks.)*

2.3 Tunnistamisen luotettavuus

2.3.1 Säännökset

Liikennepalvelulain III osan 2 luvun 2 a §:ssä säädetään henkilöllisyyden varmistamisesta puolesta-asioinnissa.

Lain mukaan *henkilöllisyys on voitava varmistaa erityisen luotettavalla tavalla, kun puolesta-asiointisuhde perustetaan tai sitä muutetaan olennaisesti. Myös puolesta-asiointitapahtuman yhteydessä henkilöllisyys on voitava varmistaa.*

2.3.2 Tunnistamistarve matkaketjuissa ja puolesta-asioinnissa

Sopijapuolten on arvioitava, onko matkustaja tarpeen tunnistaa siten, että hänen henkilöllisyytensä varmistetaan ja sidotaan matkaketjuun jossain matkaketjun vaiheessa.

Puolesta-asioinnissa sopijapuolten on arvioitava käsiteltävien henkilötietojen suojaamistarpeen ja käyttäjätilin luotettavuuden ylläpitämistarpeen perusteella, onko käyttäjätilien yksilöinti ja yhdistäminen toisiinsa riittävää vai onko tarpeen varmistaa käyttäjän oikea henkilöllisyys.

Sopijapuolten täytyy sopia siitä, millä menettelyillä ne tunnistavat osaltaan käyttäjän, varmistavat tarvittaessa tämän oikean henkilöllisyyden ja yhdistävät käyttäjän antaman valtuutuksen käyttäjätiliin.

Pääperiaate on, että henkilötietoja ei pidä käsitellä tarpeettomasti, mikä koskee myös matkustajan tunnistamista.

Matkustaja voidaan tunnistaa sähköisesti tai paikan päällä asioinnissa/kuljetuksessa, jos siihen on palvelun toteuttamisen kannalta tarve (ja henkilötietosääntelyn mukainen peruste).

Sitä, missä määrin matkustajan on mahdollista hankkia matkaketju henkilötietojen käsittelyn näkökulmasta täysin anonyymisti, voidaan arvioida henkilötietojen käsittelyä koskevan selvityksen perusteella. Täysin anonyymi matkaketjun hankkiminen ja käyttäminen lienee kuitenkin mahdollista lähinnä käteismaksulla.

Yleisesti ottaen kuljetuspalveluissa henkilön tunnistustarve voi syntyä seuraavissa tilanteissa:

- Jos alennus saadaan henkilöllisyyden perusteella
- Kun kyseessä on henkilökohtaiset lipputuotteet/kausiliput
- Eräissä liikennemuodoissa on säädettyjä vaatimuksia matkustajan tunnistamisesta (henkilöllisyyden varmistamisesta)

Liikennepalvelulain **myyntirajapinnan avaamisvelvoitteen mukaiseen vähimmäistuotteeseen ei liity edellä mainittuja syitä tunnistaa matkustajaa.** Matkustaja saatetaan kuitenkin tunnistaa nimenomaisesti tai välillisesti matkaketjun hankkimiseen tai käyttämiseen liittyvistä käytännön syistä tai tarpeista:

- Tunnistus ei välttämättä liity matkustajan henkilöllisyyteen sinänsä, vaan se voi liittyä esimerkiksi sähköiseen maksuvälineeseen, jolla matkustaja tai muu henkilö maksaa matkan.

- Tunnistus voi myös liittyä siihen tunnisteeseen, jolla matkustusoikeus todennetaan kuljetusvälineessä. Tunnistetta ei välttämättä ole sidottu tiettyyn henkilöön vaan tunnisteen haltijaan.

- Jos henkilöllisyys sidotaan matkaketjuun, merkitystä on myös sillä, missä vaiheessa henkilön sitominen matkaketjuun tehdään. Esim. henkilöllisyys voidaan varmistaa henkilötodistuksella matkustamisen yhteydessä.

- Reklamaatio- ja korvaustilanteissa on pystyttävä yhdistämään korvausta vaativa matkustaja riittävän luotettavasti siihen matkaketjuun, josta hän vaatii korvausta.

Puolesta-asioinnissa tunnistamisen tarve voi syntyä seuraavista syistä:

- Puolesta-asioija ja avaamisvelvollinen sopivat siitä, että puolesta-asioija voi asioida valtuutettuna käyttäjän puolesta tämän käyttäjätilillä, jota avaamisvelvollinen ylläpitää. Valtuutus täytyy yhdistää molemmilla osapuolilla oikeaan käyttäjätiliin ja samaan henkilöön.

- Puolesta-asioija asioi käyttäjän puolesta käyttäjätilillä, joka on liitetty tiettyyn henkilöön. Henkilötiedot eivät saa tulla muiden kuin käsittelyyn oikeutettujen tietoon.

- Puolesta-asioija hankkii henkilön puolesta tuotteen, johon liittyy henkilöön sidottu alennusperuste tai erityisehto. Henkilötiedot eivät saa tulla muiden kuin käsittelyyn oikeutettujen tietoon ja tuotteita saa käyttää vain niihin oikeutettu.

Tunnistamisen ja henkilöllisyyden varmistamisen tarpeellisuutta voi arvioida seuraavissa käyttäjätilin hallinnan ja puolesta-asioinnin vaiheissa.

vaihe	**tarve varmistaa käyttäjätilin haltijan oikea henki-**	**tarve varmistaa, että asioija on käyttäjätilin haltija**	**lain vaatimus**

	löllisyys		
Avaamisvelvollinen liittää valtuutuksen käyttäjätiliin tai valtuutus muutetaan tai perutaan	riippuu palvelusta ja käyttäjätilin sisällöstä	kyllä	erityisen huolellinen
Puolesta-asioija liittää valtuutuksen käyttäjätiliin tai valtuutus muutetaan tai perutaan	riippuu palvelusta ja käyttäjätilin sisällöstä	kyllä	erityisen huolellinen
Valtuutuksen perustaminen, muutos tai peruminen tiedotetaan avaamisvelvollisen ja puolesta-asioijan välillä	riippuu palveluista ja käyttäjätilien sisällöistä	pystyttävä yhdistämään molemmilla toimijoilla saman käyttäjän käyttäjätiliin	erityisen huolellinen
puolesta-asiointitapahtuma	kuten yllä, ei lisävaatimuksia	pystyttävä yhdistämään molemmilla toimijoilla saman käyttäjän käyttäjätiliin	huolellinen
Ulkoinen rekisterinpitäjä luovuttaa henkilötiedon avaamisvelvolliselle ja/tai puolesta-asioijalle (myös katseluoikeus katsotaan luovutukseksi)	riippuu henkilötiedosta ja henkilötiedon sääntelystä, mutta todennäköisesti on varmistettava riittävästi, että henkilötieto liitetään vain oikean henkilön käyttäjätiliin ja että se tulee vain oikean henkilön tai tätä edustamaan oikeutetun (holhooja, edunvalvoja, työnantaja jne.)	pystyttävä yhdistämään molemmilla toimijoilla saman käyttäjän käyttäjätiliin	ei erityissääntelyä liikennepalvelulaissa

2.3.3 Tunnistamisen luotettavuus sähköisessä asioinnissa yleisesti

Käyttäjä voidaan tunnistaa sähköisessä asioinnissa erilaisilla menetelmillä, joiden varmuus vaihtelee.

Heikko tunnistus

Palvelussa voidaan esimerkiksi luoda käyttäjälle käyttäjätunnus-salasana -pari käyttäjän itse antamien henkilötietojen perusteella. Tällöin on kysymys

heikosta tunnistamisesta, jossa tiedetään lähtökohtaisesti vain se, että asioija on taho, jolla on tiedossaan kyseinen käyttäjätunnus ja salasana (tai jolla on vaikkapa pääsy päätelaitteeseen, jolla käyttäjätunnus ja salasana ovat tallennettuna). Henkilöön liittyviä tietoja voidaan varmistaa tai vahventaa eri lähteistä.

Vahva tunnistus

Vahva sähköinen tunnistus perustuu siihen, että tunnistustapahtumassa käytetään aina vähintään kahta erityyppistä todentamistekijää: jotain mitä henkilö tietää (esim. PIN-koodi tai muu salasana, käyttäjätunnus), mitä hänellä on hallussaan (tunnuslukulaite, tunnuslukulista, mobiililaite) tai henkilön ominaisuus (sormenjälki tai muu biometrinen tekijä). Lisäksi vahva tunnistus edellyttää sitä, että todentamistekijät on tunnistusvälinettä luotaessa sidottu luotettavasti oikeaan henkilöön eli henkilöllisyys on varmistettu luotettavasta lähteestä ja välinen on liitetty luotettavasti juuri tähän henkilöön ja toimitettu vain tämän haltuun. Tunnistusmenetelmän täytyy olla myös kokonaisuutena tietoturvallinen.

Suomessa yleisesti tunnustetuksi vahvaksi sähköiseksi tunnistukseksi katsotaan menetelmät, jotka on ilmoitettu ja hyväksytty vahvasta sähköisestä tunnistamisesta ja luottamuspalveluista annetun lain (617/2009) mukaisesti Viestintäviraston rekisteriin. Maksupalveluissa käytettävän tunnistuksen vaatimuksista säädetään maksupalvelusääntelyssä.

Vahvoja sähköisiä tunnistusmenetelmiä ovat pankkitunnistus, mobiilivarmenteet ja poliisin myöntämällä henkilökortilla oleva väestörekisterikeskuksen myöntämä tunnistusvarmenne. Vahvaa sähköistä tunnistusta asiointipalveluille tarjoavat pankkien ja mobiilioperaattorien lisäksi tunnistusvälityspalvelut, jotka löytyvät Viestintäviraston ylläpitämästä rekisteristä.

2.3.4 Tunnistaminen puolesta-asioinnissa

Puolesta-asioinnissa käyttäjän tunnistamisen varmuutta voi hahmottaa kolmelle eri tasolle:

1) Käyttäjätilin yksilöinti. Käyttäjätili erotetaan uniikisti muista käyttäjätileistä ja varmistetaan, että asioija/henkilö on oikea käyttäjätili, mutta henkilöllisyyttä tai tiliä käyttävää henkilöä ei ole varmistettu.

2) Käyttäjätilillä asioijan yksilöinti. Varmistetaan, että asioinnissa on osapuolena oikea käyttäjä ja sama taho, joka antoi valtuutuksen, mutta käyttäjän henkilöllisyyttä ei ole varmistettu.

3) Käyttäjän yksilöinti henkilönä. Varmistetaan edellisten lisäksi käyttäjän henkilöllisyys esimerkiksi vahvalla sähköisellä tunnistamisella tai muulla riittäväksi arvioidulla menettelyllä.

Liikennepalvelulain mukaan henkilöllisyyden varmistamisen täytyy olla huolellista tai erityisen huolellista.

Lain perusteluissa todetaan, että laissa ei vaadita vahvan sähköisen tunnistamisen käyttämistä puolesta-asioinnissa. Muusta sääntelystä voi kuitenkin tulla säädettyjäkin vaatimuksia tunnistukselle. Esimerkkinä perusteluissa on mainittu maksupalvelusääntely.

Liikkumis- tai yhdistämispalvelun **omassa asiointipalvelussa** ja käyttäjätilin perustamisessa liikkumis- tai yhdistämispalvelun tarjoaja arvioi omista lähtökohdistaan asiakkaansa henkilöllisyyden varmistamisen tarpeellisuuden ja asioinnissa käytettävän tunnistamisen luotettavuustarpeet. **Toisin sanoen liikkumis- tai yhdistämispalvelun tarjoaja arvioi oman palvelunsa ja omien velvoitteidensa kannalta, kuinka tärkeää on varmistua siitä, että käyttäjä on ilmoittanut/ilmoittaa todella oikeat/omat henkilötietonsa.** Jos ei käytetä vahvaa sähköistä tunnistusta, menettelyyn voi sen lisäksi, että käyttäjä ilmoittaa itse henkilötiedot, liittyä esimerkiksi kertaluonteinen tai toistuva tekstiviesti- tai sähköpostivahvistus.

Kun **kahden toimijan** käyttäjätilit täytyy puolesta-asioinnissa pystyä riittävän luotettavasti linkittämään toisiinsa, avaamisvelvollisen ja puolesta-asioijan täytyy sopia, millainen menetelmä ja mitkä henkilötiedot ovat riittäviä puolesta-asiointiin. **Toisin sanoen avaamisvelvollisen ja puolesta-asioijan täytyy yhdessä arvioida, miten ne voivat riittävästi varmistua siitä, että ne todella käsittelevät saman henkilön käyttäjätilejä ja henkilötietoja.** Puolesta-asioinnissa on tätäkin osin hyvä ottaa huomioon liikennepalvelulain tavoite tarjota käyttäjäystävällisiä palveluita sekä tietosuoja-asetuksen henkilötietojen käsittelyn minimointiperiaate.

Jos sopijapuolet tai toinen niistä ei käytä vahvaa sähköistä tunnistusta, ne voivat esimerkiksi sopia, minkä henkilötietokokonaisuuden vertailun perusteella valtuutus voidaan liittää käyttäjätiliin (nimi, osoite, sähköpostiosoite, puhelinnumero, syntymäaika jne.) **eli millä tiedoilla ne varmistuvat puolin ja toisin siitä, että käsittelevät saman henkilön tietoja.**

Jos valtuutus koskee useampaa kuin yhtä kertaluontoista puolesta-asiointitapahtumaa, käyttäjätilin ja käyttäjän yksilöinnin lisäksi sopijapuolten täytyy sopia teknisemmällä tasolla, mitä tietoja käytetään puolesta-asiointitapahtumissa (esimerkiksi käyttäjätilin numero tai muu pseudonyymi), kun puolesta-asioija asioi avaamisvelvollisen palvelussa käyttäjän puolesta.

2.4 Yhteenveto myyntirajapinnan avaamisen tietoturva- ja tietosuojavaatimuksista

Avaamisvelvollisella tarkoitetaan sitä liikkumis- tai yhdistämispalvelua tai näiden puolesta lippu- ja maksujärjestelmästä tarjoavaa, jonka on lain mukaan avattava pääsy kertalipun myyntirajapintaan.

Sopijapuolilla tarkoitetaan myyntirajapinnan avaamisvelvollista ja liikkumispalvelua, joka hankkii tuotteita myyntirajapinnan kautta.

- Avaamisvelvollisen on huolehdittava siitä, että avaaminen voi tapahtua palvelun tietoturvan ja yksityisyyden suojan vaarantumatta.

- Sopijapuoli voi edellyttää, että toinen sopijapuoli noudattaa riskiin suhteutettuja hyviä tietoturvakäytäntöjä lippu- ja maksujärjestelmän myyntirajapinnan tietoliikenteessä ja omissa järjestelmissään, jotka vaikuttavat myyntirajapinnan tietoliikenteeseen tai sen kautta saatujen tietojen käsittelyn tietoturvallisuuteen.

2.5 Yhteenveto puolesta-asioinnin tietoturva- ja tietosuojavaatimuksista

Seuraavaan listaan on koottu yleisen tason kuvaus tietoturvavaatimusten ja henkilötietojen suojan vaatimusten toteuttamisesta puolesta-asioinnissa.

Puolesta-asioijalla tarkoitetaan sitä yhdistämis- tai liikkumispalvelua, joka asioi käyttäjän valtuuttamana toisen liikkumis- tai yhdistämispalvelun tarjoamalla käyttäjätilillä.

Avaamisvelvollisella tarkoitetaan sitä liikkumis- tai yhdistämispalvelua tai näiden puolesta lippu- ja maksujärjestelmästä tarjoavaa, jonka on lain mukaan avattava pääsy käyttäjän käyttäjätilille tai muuhun sähköiseen asiointitapaan.

- Puolesta-asioija voi käyttää pääsyä käyttäjätilille sillä rajapinnalla tai niillä käyttäjän tai puolesta-asioijan tunnisteilla, jotka avaamisvelvollinen käyttäjätilin ylläpitäjä tarjoaa ja joista sovitaan avaamisen yhteydessä.

- Puolesta-asiointitapahtuma käynnistyy käyttäjän aloitteesta

- Puolesta-asioijan ja avaamisvelvollisen käyttäjätilin ylläpitäjän on kummankin osaltaan:
  - noudatettava tietojen käsittelyssä omissa tietojärjestelmissään hyviä riskiin suhteutettuja tietoturvakäytäntöjä
  - noudatettava tietojen siirtämisessä tietoliikenteessä hyviä riskiin suhteutettuja tietoturvakäytäntöjä
  - huolehdittava siitä, että käyttäjän henkilötietoja käsitellään turvallisesti
  - huolehdittava siitä, että puolesta-asioinnissa käsitellään vain puolesta-asioinnin kannalta tarpeellisia henkilötietoja
  - huolehdittava siitä, että sopimusosapuolen liikesalaisuuksia, kryptografisia salaisuuksia tai muita käyttäjätilin avaamisessa puolesta-asiointiin tarvittavia tietoja käsitellään turvallisesti ja vain sovittuun tarkoitukseen
  - tallennettava puolesta-asiointitapahtuman todentamiseen tarvittavat tiedot mahdolliseen häiriöselvitykseen tai vastaavaan tarpeeseen tarvittavan ajan

- Puolesta-asioijan on:
  - tunnistauduttava avaamisvelvolliselle käyttäjätilin ylläpitäjälle tavalla, josta on sovittu avaamisen yhteydessä
  - huolehdittava siitä, että käyttäjän tunnisteet ja muut henkilötiedot eivät ole muiden kuin käyttäjän ja avaamisvelvollisen saatavilla

2.6 Tietoturvallisuudesta sovittavat asiat

Tähän kohtaan on koottu muistilista tietoturva-asioista, joista on hyvä sopia. Näitä ovat
- ✓ Tiedon säilyttämisen tietoturvallisuus
- ✓ Tiedon siirtämisen tietoturvallisuus
- ✓ Menettely järjestelmä-, rajapinta- ja vaatimusmuutoksissa
- ✓ Rajapinnan tai järjestelmän häiriötilanteiden tai uhkien käsittely
- ✓ Häiriö-, muutos- ja tapahtumatietojen luottamuksellisuus

✓ Menettely sopijapuolen tietoturvallisuudesta/luotettavuudesta varmistumiseksi

Sopijapuolten on hyvä vaatia molemminpuolisesti vähintään seuraavia asioita:

- Tiedon säilyttämisen tietoturvallisuus
  - Tieto ja käyttöoikeudet luokitellaan
  - Tietoa salataan ja suojataan yhteisen sopimuksen mukaisesti
  - Tiedon käsittely lokitetaan soveltuvin osin
  - Tiedon käsittely ja siirtäminen järjestelmästä kyetään jäljittämään toimenpiteen tehneeseen henkilöön
- Tiedon siirtämisen tietoturvallisuus
  - Järjestelmän vyöhykkeistys – rajapinnan ja taustajärjestelmien riittävä eriyttäminen
  - Osapuolten tunnistaminen
    - sertifikaatit, pääsy rajapintaan sallittu vain ennalta määritellyille IP-osoitteille
    - Verkkorajapinnan TLS-tason autentikointi tai muu vastaava menettely. Mikäli mahdollista, verkkoliikenteessä molemmat osapuolet olisi hyvä tunnistaa varmentein (asiakasvarmenne ja palvelinvarmenne), jotka on vaihdettu ennen toiminnan aloittamista
    - Varmenteiden vaihtomenettely ja hallinta
  - Tiedonsiirto: protokollan vaatimukset, salaus
- Menettely järjestelmä-, rajapinta- ja vaatimusmuutoksissa
  - Sopijapuolen informointi riittävän ajoissa
- Rajapinnan tai järjestelmän häiriötilanteiden tai uhkien käsittely
  - Havainnointikyky
    - esimerkiksi lokien seuranta ja poikkeamien havaintokyky, kyky havaita ja tuottaa heräte vähintään tyypillisten transaktiomäärien tai vastaavien oletettujen raja-arvojen poikkeamista
  - Sopijapuolen informointi ja menettely tietoturvallisuuspoikkeamatapauksissa
    - Poikkeamakontaktin nimeäminen. Molemmilla toimijoilla on syytä olla kontakti, johon toinen sopijapuoli voi tarvittaessa olla yhteydessä havaitessaan mahdollisen tietoturvaongelman.

- Tiedottamisen viestintäkanavat ja ilmoitusajat. Viestintäkanavien tulee olla riittävän tietoturvallisia välitettävään tietoon suhteutettuna.
- Sopijapuolten on hyvä sopia tietoturvauhkien ja -häiriöiden tiedottamisesta, jotta sopijapuolet ja muut liikkumispalveluverkoston toimijat voivat ennakoida tilanteita ja tehdä osaltaan tarvittavat varautumis- tai korjaustoimenpiteet. Esimerkiksi tietoturvauhka, kuten ohjelmiston haavoittuvuus, käynnissä oleva phishing-kampanja tai palvelunestohyökkäys on hyvä ilmoittaa matalalla kynnyksellä, jotta sopijapuolet/muut liikkumispalveluverkoston toimijat voivat ennakoida tilannetta.
- Yhteistyö häiriön selvittämisessä
- Rajapinnan tai sen osan sulkeminen tilapäisenä tietoturvatoimenpiteenä, jos se on välttämätöntä

- Sopijapuolen informointi ja menettely ennakoiduista tai odottamattomista huoltokatkoista tai toimivuushäiriöistä rajapinnassa/siihen liittyvässä palvelussa.
  - Näistä on syytä ilmoittaa ainakin, jos ne vaikuttavat sopijapuolten palveluihin.

- Häiriö-, muutos- ja tapahtumatietojen luottamuksellisuus
  - Sopijapuolilla ei ole oikeutta luovuttaa kolmansille osapuolille luottamuksellista tietoa, jonka ne ovat saaneet sopimuksen perusteella.
  - Sopijapuolet *voivat* sopia siitä, että ne tiedottavat toistensa puolesta häiriötilanteista kolmansille osapuolille tai yleisölle.

Sopijapuolten keskinäisellä salassapidolla ei saa olla haitallista vaikutusta kuluttajan oikeuteen saada tietoa siitä, kenen toimijan puoleen kuluttaja voi kääntyä vedotakseen laillisiin oikeuksiinsa.

- Menettely sopijapuolen tietoturvallisuudesta/luotettavuudesta varmistumiseksi
  - Puolesta-asioinnissa menettely ja luotettavuuden osoittaminen määritellään avaamisvelvollisen ennalta laatimissa arviointikriteereissä ja ehdoissa, ks. jäljempänä kohta 3.3
  - Kertalipun myyntirajapinnan avaamisessa suositeltavia menettelyjä käsitellään jäljempänä kohdassa 3.2.
  - Molemmissa tilanteissa ja rajapintojen avaamisessa muutoinkin voivat tulla kysymykseen seuraavat hyvät käytännöt:

- Näyttö siitä, että palvelun toteuttamisessa käytetyn sovelluksen ja sovelluksen alustan tietoturvallisuudesta on varmistuttu riskiin nähden riittävin toimenpitein. Tämä voi sisältää esimerkiksi:
  - Sovelluksen penetraatiotestausraportin tai vastaavan dokumentin, josta käy ilmi, että sopijapuoli on testannut tai testauttanut sovelluksensa tietoturvallisuuden
  - Sovelluksen palvelinalustan palveluntarjoajan (esim. pilvipalveluntarjoaja) hyväksynnät tai tietoturvallisuussertifikaatit
  - Edellä mainittujen on syytä olla aina helposti saatavilla, jotta velvoitteiden täyttymisestä voidaan varmistua mahdollisimman helpoin menettelyin.

3 Sopijapuolen luotettavuudesta varmistuminen

3.1 Säännökset ja valvonta

Liikennepalvelulain III osan 2 luvun 4 §:ssä säädetään rajapintojen avaamisen tietoturva- ja tietosuojavaatimuksista sekä pääsyn ehdoista.

Saman luvun 2 a §:ssä säädetään puolesta-asioinnissa avaamisvelvollisen oikeudesta *arvioida pääsyyn oikeutetun liikkumis- tai yhdistämispalvelun tarjoajan luotettavuus ennalta asetettujen arviointikriteerien ja ehtojen mukaan.*

Liikennepalvelulain noudattamista ja siten myös arviointikriteerien ja ehtojen lainmukaisuutta valvoo Liikenne- ja viestintävirasto.

3.2 Kertalipun myyntirajapinta

Sopijapuoli voi edellyttää toiselta sopijapuolelta sopimista siitä, millä menettelyllä osapuolet voivat varmistua toistensa tietoturvallisuuden ylläpidon riittävyydestä.

Suositeltava ja kohtuullinen menettely on sopia vaatimukset huolellisesti sopimuksessa ja tehdä internetiin auki oleville rajapinnoille tekninen testaus.

Mahdollisia menettelytapoja ovat seuraavat

- Tietoturvavaatimukset määritellään ja vaatimuksien täyttyminen dokumentoidaan kirjallisessa sopimuksessa.
- Sopijapuolen järjestelmän kaikille internetiin auki oleville verkkorajapinnoille suoritetaan tekninen testaus riippumattoman arvioijan tai toimijan itsensä toimesta, mikäli toimijan on mahdollista näyttää toteen testauksen tekijän ammattitaito. Testauksessa huomioidaan myös alihankkijoiden kautta avatut rajapinnat. Testaustulokset informoidaan toiselle sopijapuolelle.

    - Ks. LIITE *LIPPU-API: Security Considerations* sopivien itsetestaustyökalujen ja -menetelmien valitsemiksi.

- Sopijapuolen koko järjestelmään teetetään riippumaton tietoturvallisuuden auditointi (mukaan lukien verkkorajapintojen testaus). Uhkatason ollessa korkea, edellytetään tietoturvallisuuden standardinmukaista (esim. ISO 27001) sertifiointia.

- Sopijapuoli saa oikeuden tehdä toisen sopijapuolen järjestelmään tietoturvallisuuden auditoinnin.

Suositeltava ja kohtuullinen menettely on vähintään sopia vaatimukset huolellisesti sopimuksessa ja tehdä internetiin auki oleville rajapinnoille tekninen testaus.

Yksinomaan myyntirajapinnan avaamisen takia ei ole katsottava kohtuulliseksi vaatia koko järjestelmän riippumatonta auditointia tai sertifiointia. Sopijapuolen tekemässä auditoinnissa on syytä huomioida liike- ja ammattisalaisuuksien, sekä henkilötietojen suoja. Näitä raskaampia menettelyjä voidaan toki hyödyntää, jos ne ovat muutoinkin liiketaloudellisista syistä toimijalla käytössä.

3.3 Sopijapuolten tehtävät puolesta-asioinnin pääsyn avaamisen eri vaiheissa

1) Ennen pääsyn avaamista

Avaamisvelvollinen

- tunnistaa tarjoamaansa käyttäjätiliin tai muuhun sähköiseen asiointitapaan liittyvät henkilötiedot ja muut tietosisällöt, tietoturvaominaisuudet ja omat sertifikaattinsa tms. turvallisuusnäytöt.

- Laatii kuvauksen tarjoamansa käyttäjätiliin tai muun sähköiseen asiointitavan rajapinnasta tai muusta pääsytekniikasta

- Laatii arviointikriteerit ja ehdot puolesta-asioijalle eli rajapinnan tai muun pääsytavan käyttäjälle

Puolesta-asioija

- Laatii kuvauksen tietoturvallisuudesta ja henkilötietojen käsittelystä huolehtimisestaan

2) Pääsyä pyydettäessä

Avaamisvelvollinen

- julkaisee tai toimittaa rajapinnan tai muun pääsytavan kuvauksen ja ennalta laaditun arviointikriteeristön ja ehdot pääsyn avaamista pyytävälle

- Tarkistaa pääsyn avaamista pyytävän selvityksen tietoturvallisuudesta ja henkilötietojen käsittelystä

- Neuvottelee tarvittaessa pääsyä pyytävän kanssa tämän turvallisuusnäytöistä ja yhteen toimivuuden toteuttamisesta järjestelmien välillä
- Sopii menettelyistä muutos- tai häiriötilanteessa

Puolesta-asioija

- Toimittaa avaamisvelvolliselle selvityksen tietoturvallisuudesta ja henkilötietojen käsittelystä huolehtimisestaan
- Neuvottelee tarvittaessa avaamisvelvollisen kanssa turvallisuusnäytöistä ja yhteen toimivuuden toteuttamisesta järjestelmien välillä
- Sopii menettelyistä muutos- tai häiriötilanteessa

3) Tuotantovaiheessa

Avaamisvelvollinen ja puolesta-asioija

- Informoivat toisiaan häiriötilanteesta.
- Informoivat toisiaan muutoksista.
- Selvittävät häiriötilanteet tarvittaessa yhdessä.
- Keskeyttävät rajapinnan tai muun pääsytavan käytön tarvittaessa sopimuksen mukaisesti.

3.4 Puolesta-asioinnin avaamisvelvollisen ennalta laatimat kriteerit ja ehdot

Avaamisvelvollisen on laadittava ennalta arviointikriteerit ja ehdot puolesta-asioijalle. Avaamisvelvollisen suositellaan julkaisevan arviointikriteerit ja ehdot esimerkiksi verkkosivuillaan. Jos avaamisvelvollinen ei julkaise niitä, sen tulee toimittaa ne viivytyksettä, kun puolesta-asioija pyytää pääsyn avaamista. Arviointikriteerien ja ehtojen täytyy lain mukaan olla oikeudenmukaisia, kohtuullisia ja syrjimättömiä eivätkä ne saa sisältää käyttöä rajoittavia ehtoja.

Lain oikeudenmukaisuus-, kohtuullisuus- ja syrjimättömyysvaatimuksen valossa avaamisvelvollisen täytyy huomioida kriteereissä vastaavat luotettavuusnäytöt, joita sillä itsellään on. Nämä eivät kuitenkaan voi olla vähimmäisvaatimuksia. Samoin pääsyä pyytävältä edellytettävässä käyttäjien tunnistamisessa vaatimukset on suhteutettava oikeudenmukaisesti avaamisvelvollisen omaan kyvykkyyteen ja käytäntöihin käyttäjän tunnistamisessa sekä henkilöllisyyden varmentamisen tarpeellisuuteen.

Arviointikriteerien ja ehtojen täytyy sisältää vähintään seuraavat tiedot:

1) Kuvaus vaadituista kohtuullisista tietoturvakäytännöistä, joita sopimuskumppanilta edellytetään järjestelmän eri osa-alueilla.

- Tarkennettuna esimerkiksi tämän taustaselvityksen osa-aluejaottelun mukaan (ks. kohta 2.2.2), vaatimusten perusteet ja mahdolliset ohjeelliset standardiviittaukset

- Kuvaus tavoista, joilla pääsyä pyytävä voi täyttää tai osoittaa käyttäjätilin tai käyttäjätilin haltijan tunnistamisen luotettavuuden. Erityisesti on huomioitava, tarvitaanko henkilöllisyyden varmentamista vai pelkästään käyttäjätilin yksilöintiä.

2) Kuvaus niistä tavoista, joilla pääsyä pyytävä voi osoittaa täyttävänsä 1 kohdan kohtuulliset tietoturvavaatimukset ja henkilötietojen käsittelyn säädetyt vaatimukset

   - Kuvaus niistä viranomaisen tai viranomaisen valtuuttaman kolmannen osapuolen vastaavaa tarkoitusta myöntämistä luvista, hyväksynnöistä, auditoinneista tai sertifioinneista, joiden perusteella puolesta-asioija voi oletusarvoisesti osoittaa luotettavuutensa

   - Kuvaus muista menettelyistä, joilla puolesta-asioija voi osoittaa toimintansa vastaavan yleisesti käytettyä standardia tai alan yleisesti hyväksyttyjä ehtoja ja joilla puolesta-asioija voi oletusarvoisesti osoittaa luotettavuutensa. Erityisesti on syytä kuvata, missä määrin EU:n yleisen tietosuoja-asetuksen noudattamisen osoittaminen riittää.

   - Kuvaus siitä, miten puolesta-asioija voi osoittaa vaatimusten täyttämisen, jos sillä ei ole 2 tai 3 kohdissa määriteltyjä näyttöjä.

3) Kuvaus tavoista, joilla pääsyä pyytävä voi osoittaa täyttävänsä muut luotettavuusvaatimukset, jotka voivat liittyä esimerkiksi seuraaviin

   - liikennepalvelulaissa säädetyn ilmoituksen tekeminen, jos puolesta-asioija on välitys- tai yhdistämispalvelu (III:5 luku:1 §)

   - oikeustoimi- ja liiketoimintakelpoisuutta koskevat rekisteröinnit tai julkiset tietolähteet

   - mahdollisten kansainvälisten pakotteiden muodostamat esteet.

4) Muut rajapinnan tai pääsyn avaamisen kannalta tarpeelliset ehdot, jotka liittyvät tukipalveluihin, käyttöehtoihin, ohjelmistoihin, lisensseihin ja muihin tarvittaviin palveluihin.

5) Kuvaus siitä, millaisia puolesta-asioinnin valtuutusjärjestelyjä avaamisvelvollinen tukee.

   - Esim. hankkiiko avaamisvelvollinen valtuutukset itse käyttäjältä vai hyväksyykö avaamisvelvollinen puolesta-asioijan ilmoituksen siitä, että tämä on hankkinut valtuutuksen.

Viestintävirasto
www.viestintävirasto.fi