HSL Helsingin seudun liikenne -kuntayhtymä

Tietosuojapolitiikka

17.4.2018

versio 1.1

Sisällys

1 TARKOITUS JA TAUSTAA

Tässä tietosuojapolitiikassa on kuvattu HSL:n määrittelemät tietosuojan tavoitteet, vastuut ja toimintalinjat. HSL tunnistaa tietosuojan ja rekisteröityjen henkilöiden yksityisyyden suojan merkityksen osana toimintaansa ja sitoutuu tietosuojaan tässä tietosuojapolitiikassa kuvatulla tavalla. Tietosuoja on osa toiminnan vaatimustenmukaisuutta, tietoturvallisuutta ja riskienhallintaa.

Tietosuojan tavoitteiden ja merkityksen sekä tietosuojatyön toimintaperiaatteiden määrittely, dokumentointi ja viestintä HSL:n työntekijöille muodostavat keskeisen osan HSL:n tietosuojakulttuuria. Tämän tietosuojapolitiikan ja tähän pohjautuvan tarkemman ohjeistuksen avulla HSL:n henkilöstölle ja yhteistyökumpaneille viestitään HSL:n tietosuojaperiaatteista. Lisäksi laadukkaalla tietoturvatyöllä toteutetaan osaltaan tietosuojan tavoitteiden toteutumista. HSL:n tietoturvapolitiikka määrittelee tietoturvallisuuden ja tietoturvatyön periaatteet.

2 SOVELLETTAVA LAINSÄÄDÄNTÖ JA MÄÄRITELMÄT

2.1 Lainsäädäntö

Tietosuojaan ja henkilötietojen käsittelyyn sovelletaan EU:n yleistä tietosuoja-asetusta (2016/679), kansallista henkilötietolainsäädäntöä, sekä muita soveltuvia erityissäännöksiä. Lisäksi HSL:n tietosuojatyötä ohjaavat HSL:n perussopimus, strategia, hallintosääntö ja sisäiset ohjeistot sekä tietoturvan osalta HSL:n tietoturvapolitiikka, ISO/IEC 27001 & 27002 –standardit sekä alan hyvät käytännöt.

HSL:n toiminnassa toteutetaan perustuslaissa säädettyjä hallinnon julkisuutta ja yksityisyyden suojaa. HSL sovittaa nämä perusoikeudet yhteen lainsäädännössä säädetyllä tavalla.

2.2 Määritelmät

Tässä tietosuojapolitiikassa käytetään EU:n yleisen tietosuoja-asetuksen mukaisia käsitemääritelmiä.

Henkilötieto tarkoittaa kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön, eli rekisteröityyn 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.

Käsittely tarkoittaa 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.

Henkilötietojen käsittelijä tarkoittaa luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka käsittelee henkilötietoja rekisterinpitäjän lukuun.

Rekisteri tarkoittaa mitä tahansa jäsenneltyä henkilötietoja sisältävää tietojoukkoa, josta tiedot ovat saatavilla tietyin perustein, oli tietojoukko sitten keskitetty, hajautettu tai toiminnallisin tai maantieteellisin perustein jaettu.

Rekisterinpitäjä tarkoittaa luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot; jos tällaisen käsittelyn tarkoitukset ja keinot määritellään unionin tai jäsenvaltioiden lainsäädännössä, rekisterinpitäjä tai tämän nimittämistä koskevat erityiset kriteerit voidaan vahvistaa unionin oikeuden tai jäsenvaltion lainsäädännön mukaisesti.

Rekisteröidyn suostumus tarkoittaa mitä tahansa vapaaehtoista, yksilöityä, tietoista ja yksiselitteistä tahdonilmaisua, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn antamalla suostumusta ilmaisevan lausuman tai toteuttamalla selkeästi suostumusta ilmaisevan toimen.

Henkilötietojen tietoturvaloukkaus tarkoittaa tietoturvaloukkausta, jonka seurauksena on siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin.

Profilointi tarkoittaa mitä tahansa henkilötietojen automaattista käsittelyä, jossa henkilötietoja käyttämällä arvioidaan luonnollisen henkilön tiettyjä henkilökohtaisia ominaisuuksia, erityisesti analysoidaan tai ennakoidaan piirteitä, jotka liittyvät kyseisen luonnollisen henkilön työsuoritukseen, taloudelliseen tilanteeseen, terveyteen, henkilökohtaisiin mieltymyksiin, kiinnostuksen kohteisiin, luotettavuuteen, käyttäytymiseen, sijaintiin tai liikkeisiin.

3 TIETOSUOJAPERIAATTEET

EU:n yleisen tietosuoja-asetuksen mukaisilla periaatteilla ohjataan henkilötietojen käsittelyä niin, että asetuksen vaatimukset toteutuvat ja rekisteröidyn oikeuksia kunnioitetaan. Henkilötietojen käsittelyssä tulee huomioida kaikki alla esitellyt periaatteet. Tietosuojaperiaatteet tulee huomioida koko henkilötietojen käsittelyn elinkaaren ajan.

3.1 Lainmukaisuus, kohtuullisuus ja läpinäkyvyys

Henkilötietoja on käsiteltävä lainmukaisesti, kohtuullisesti sekä rekisteröidyn kannalta läpinäkyvästi. Rekisteröityjen tulee tietää, miten heitä koskevia tietoja kerätään ja käsitellään. Käsittelyyn liittyvien tietojen ja viestinnän on oltava helposti saatavilla ja ymmärrettävissä. Rekisteröityjen tulee tietää rekisterinpitäjän henkilöllisyys ja käsittelyn tarkoitukset. Rekisterinpitäjän pitää pystyä antamaan rekisteröidyille tieto heitä koskevien henkilötietojen käsittelystä sekä siitä, miten rekisterinpitäjä varmistaa henkilötietojen käsittelyn asianmukaisuuden ja läpinäkyvyyden.

3.2 Käyttötarkoitussidonnaisuus

Henkilötietojen keräämisen tulee olla sidonnainen käyttötarkoitukseen, eli tietojen keräämisen tulee tapahtua tiettyä, nimenomaista ja laillista tarkoitusta varten. Kerättyä tietoa ei saa käyttää myöhemmin muuhun käyttötarkoitukseen.

Henkilötietojen myöhempää käsittelyä ei katsota yhteensopimattomaksi alkuperäisten tarkoitusten kanssa, jos käsittely tapahtuu EU:n yleisen tietosuoja-asetuksen tarkoittamia yleisen edun mukaisia arkistointitarkoituksia, tieteellisiä tai historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten (artikla 89 1 kohta).

3.3 Tietojen minimointi

Henkilötietojen on oltava asianmukaisia, olennaisia, riittäviä ja rajoituttava siihen, mikä on tarpeellista niiden käsittelyn tarkoitusten kannalta. Henkilötietojen säilytysajan on oltava mahdollisimman lyhyt. Henkilötietoja olisi käsiteltävä vain jos käsittelyn tarkoitusta ei voida kohtuullisesti toteuttaa muilla keinoin. Rekisterinpitäjän täytyy asettaa määräajat henkilötietojen poistolle. Jos tarkkoja määräaikoja ei voida asettaa, rekisterinpitäjän tulee antaa kriteerit henkilötietojen poiston määräajoille.

3.4 Tietojen täsmällisyys

Henkilötietojen on oltava täsmällisiä ja tarvittaessa päivitettyjä sekä rekisterinpitäjän on kohtuullisin toimenpitein varmistettava, että käsittelyn tarkoituksiin nähden epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä, esimerkiksi muutoksenhakuajan päätyttyä. Rekisteröidyllä on oikeus saada puutteelliset henkilötiedot täydennettyä, muun muassa toimittamalla lisäselvitys.

3.5 Tietojen säilytyksen rajoittaminen

Henkilötiedot on säilytettävä sellaisessa muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin se on tarpeellista tietojen käsittelyä varten. Tietoja voi kuitenkin säilyttää kauemmin, mikäli tietoja käsitellään ainoastaan yleisen edun mukaisia arkistointitarkoituksia varten tai tietoja käytetään historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten.

3.6 Tietojen eheys ja luottamuksellisuus

Henkilötietoja käsittelyssä on varmistettava asianmukainen tietoturvallisuus eli tietojen eheys, luottamuksellisuus ja saatavuus. Tietoja tulee suojata luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta.

3.7 Rekisterinpitäjän osoitusvelvollisuus

Osoitusvelvollisuus tarkoittaa, että rekisterinpitäjän on pystyttävä osoittamaan rekisteröidyille ja tietosuojaviranomaisille, miten tietosuojaperiaatteita noudatetaan. Osoittaminen tapahtuu muun muassa tietosuojaselosteiden laatimisen, rekisteröityjen informoimisen, huolellisesti dokumentoitujen henkilötietojen käsittelyprosessien ja organisaation sisäisen ohjeistuksen keinoin. Rekisterinpitäjän tulee säännöllisesti arvioida, miten periaatteet toteutuvat omassa toiminnassa.

4 TIETOSUOJAN HALLINTAMALLI

HSL:n hallintosäännön mukaan hallitus vastaa tietosuojasta ja nimeää tietosuojavastaavan. Tietosuojavastaava vastaa tietosuoja-asetuksessa ja tietosuojan hallintamallissa määritellyistä tehtävistä.

Tietosuojan hallintamalli määrittelee HSL:n tietosuojatehtävät ja –vastuut hallintosäännön ja tietosuojapolitiikan mukaisesti. Toimitusjohtaja hyväksyy HSL:n tietosuojan hallintamallin.

Osaston johtajat vastaavat oman osastonsa toiminnan osalta tietosuojan toteuttamisesta tietosuojapolitiikan mukaisesti, mukaan lukien henkilötietojen käsittelyn ulkoistetut palvelut. Henkilötietojen käsittelyn ulkoistamisesta laaditaan aina kirjallinen sopimus, missä osapuolet sopivat henkilötietojen käsittelyyn liittyvistä vastuista ja velvollisuuksista EU:n yleisessä tietosuoja-asetuksessa määritellyn mukaisesti. Osastonjohtajat vastaavat henkilötietojen käsittelyn vaikutustenarviointien tekemisestä. Vaikutustenarviointi on tehtävä, jos käsittely todennäköisesti aiheuttaa korkean riskin rekisteröityjen oikeuksien ja vapauksien kannalta. Vaikutustenarvioinnin tekemiseen tulee pyytää neuvoja tietosuojavastaavalta.

Toimitusjohtaja ja osaston johtajat huolehtivat tarpeellisista ja riittävistä resursseista tietosuojatyöhön.

Tietosuojavelvoitteet koskevat HSL:n henkilökuntaa ja HSL:n yhteistyökumppaneita.

HSL:n tietosuojaa arvioidaan säännöllisesti hallintamallin mukaisesti. Tietosuojavastaava raportoi osaston johtajille tietosuojapoikkeamatilanteissa sekä säännöllisesti osaston johtajille ja hallitukselle tietosuojan hallintamallin periaatteiden mukaisesti.

HSL:n henkilökunta ja sen yhteistyökumppanit ovat velvollisia ilmoittamaan havaitsemistaan tietosuojan puutteista, menettelyvirheistä tai muista uhkista lähiesimiehelleen ja HSL:n tietosuojavastaavalle.

5 TIETOSUOJAPOLITIKAN HYVÄKSYMINEN JA PÄIVITTÄMINEN

HSL:n hallitus on hyväksynyt tämän tietosuojapolitiikan sisällön. Tietosuojapolitiikan sisältöä tarkistetaan ja päivitetään tarvittaessa. HSL:n tietosuojavastaavan tehtävänä on arvioida tietosuojapolitiikan päivitystarvetta ja päivitysehdotukset viedään HSL:n hallitukseen hyväksyttäviksi.

Hallituksen hyväksymä 17.4.2018