Helsingin kaupungin tietosuojalinjaukset

Postiosoite: PL1, 00099 HELSINGIN KAUPUNKI
Käyntiosoite: Pohjoisesplanadi 11-13, 00170 Helsinki
kaupunginkanslia@hel.fi
+358 9 310 1641
www.hel.fi
y-tunnus: 0201256-6

Johdanto

Henkilötietojen suojasta säädetään EU:n yleisessä tietosuoja-asetuksessa (EU 2016/679), jäljempänä ”tietosuoja-asetus”. Tietosuojalaki (1050/2018) tarkentaa tietosuoja-asetuksen säädöksiä. Lisäksi monet lait, esimerkiksi salassapitolainsäädäntö, ohjaavat sitä, miten henkilötietoja on käsiteltävä.

Tietosuoja-asetus sisältää rekisteröidyn oikeuksia ja vastaavasti rekisterinpitäjän ja henkilötietojen käsittelijän velvollisuuksia.

Kaupunki sovittaa yhteen toiminnassaan yksityishenkilöiden yksityisyyden suojan ja hallinnon toiminnan avoimuuden ja julkisuuden lainsäädännössä säädetyllä tavalla. Hallinnon julkisuutta koskeva ohjeistus annetaan erikseen.

Nämä linjaukset sisältävät ohjeita siitä, miten tietosuojalainsäädännön mukaiset velvoitteet täytetään kaupungin toiminnassa. Ohjeita täydennetään, kun lainsäädännön soveltamisesta saadaan tarkempia ohjeita valvontaviranomaisilta.

Helsingin kaupunki käsittelee henkilötietoja vain, kun se on kaupungin toimintojen toteuttamiseksi välttämätöntä ja sille on lain mukainen peruste. Henkilötietojen käsittelystä tiedotetaan avoimesti. Henkilötietoja voidaan kerätä vain tiettyä, nimenomaista ja laillista tarkoitusta varten. Henkilötietoja on käsiteltävä siten, että varmistetaan tietojen asianmukainen turvallisuus ja luottamuksellisuus.

Henkilötiedot säilytetään vain niin kauan kuin se on tarpeen käsittelytarkoituksen toteuttamiseksi. Henkilötietoja voidaan säilyttää pidempiä aikoja, jos henkilötietoja käsitellään yleisen edun mukaisia arkistointitarkoituksia tai historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten.

Tiedonohjaussuunnitelmassa määritellään arkistoitavat tiedot ja niiden säilytysajat. Arkistoitavien tietojen säilyttämisessä on huomioitava, että on toteutettu asianmukaiset tekniset ja organisatoriset toimenpiteet rekisteröityjen yksityisyyden suojaamiseksi.

Keskeiset määritelmät

Henkilötieto

Henkilötiedolla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan henkilöön liittyviä tietoja.

Tunnistettavana pidetään 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.

Henkilötietoja ovat nimen ja henkilötunnuksen lisäksi esimerkiksi osoite, puhelinnumero, sähköpostiosoite, auton rekisterinumero, kiinteistötunnus ja IP-osoite sekä kaikki henkilöön liittyvät tiedot kuten kyseistä henkilöä koskevat terveystiedot, hänelle annettuja kaupungin palveluja koskevat tiedot, henkilön tulotiedot ja hänen yksityiselämäänsä koskevat tiedot.

Henkilötietoja ovat sellaisetkin tiedot, joista ei suoraan käy ilmi ketä ne koskevat, mutta jotka ovat yhdistettävissä luonnolliseen henkilöön yhdistämällä tiedot muualta saatavaan tietoon.

Henkilötietojen käsittely

Henkilötiedolla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan henkilöön liittyviä tietoja. Henkilötietojen käsittely tarkoittaa muun muassa 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 ja tuhoamista. Henkilötietojen katsominenkin on henkilötietojen käsittelyä.

Henkilötietojen käsittelyllä tarkoitetaan siis toimintoa tai toimintoja, joita kohdistetaan henkilötietoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti.

Henkilörekisteri

Helsingin kaupunki kerää henkilötietoja eri rekistereihin tietojen käyttötarkoitusten mukaan. Rekisterissä olevat tiedot on kerätty samaa käyttötarkoitusta varten. Rekisterillä tarkoitetaan mitä tahansa jäsenneltyä henkilötietoja sisältävää tietojoukkoa, josta tiedot ovat saatavilla tietyin perustein. Rekisteri voi syntyä niin sähköisesti kuin paperillekin tallennetuista tiedoista.

Rekisterinpitäjä

Rekisterinpitäjällä tarkoitetaan ihmistä tai organisaatiota, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.

Helsingin kaupungin rekistereiden osalta rekisterinpitäjinä ovat yleensä toimielimet: kaupunginhallitus, lautakunnat ja johtokunnat. Helsingin kaupungilla rekisterinpitäjän tehtävät on delegoitu toimielimiltä viranhaltijoille. Rekisterinpitäjänä voi olla myös viranhaltija, jos rekisteri

liittyy viranhaltijalla lainsäädännön, hallintosäännön tai delegointipäätöksen nojalla olevan erityistoimivallan käyttöön.

Rekisteröity

Rekisteröity tarkoittaa henkilöä, jonka tietoja on kerätty rekistereihin ja jonka tietoja käsitellään. Rekisteröity voi olla esimerkiksi kuntalainen, asiakas tai kaupungin työntekijä.

Tietosuoja-asioiden vastuunjako Helsingin kaupunginorganisaatiossa

Hallintosäännön 8 luvun 1 § 1 momentin 5 kohdan mukaan kaupunginhallitus vastaa, että kaupunki täyttää tietosuojalainsäädännön velvoitteet ja valvoo niitä.

Tietosuojavastaava

Tietosuojavastaavan asema ja tehtävät määräytyvät tietosuoja-asetuksen 38 ja 39 artiklan nojalla. Tietosuojavastaava mm. neuvoo ja ohjeistaa tietosuojalainsäädännön mukaisista velvollisuuksista, seuraa, että tietosuojalainsäädöksiä kaupungin toiminnassa noudatetaan ja tekee tähän liittyviä tarkastuksia. Lisäksi hän tekee yhteistyötä valvontaviranomaisen eli tietosuojavaltuutetun toimiston kanssa ja toimii sen yhteyspisteenä henkilötietojen käsittelyyn liittyvissä kysymyksissä.

Tietosuoja-asetuksen 37 artiklan mukaan rekisterinpitäjän ja henkilötietojen käsittelijän on nimitettävä tietosuojavastaava aina, kun tietojen käsittelyä suorittaa jokin muu viranomainen tai julkishallinnon elin kuin tuomioistuin. Tietosuojavastaava raportoi suoraan kaupungin ylimmälle johdolle eikä hänelle saa antaa ohjeita siitä, kuinka hän suorittaa tehtävänsä.

Rekisterinpitäjän on tuettava tietosuojavastaavaa antamalle tälle resurssit, jotka ovat tarpeen tämän tehtävien täyttämisessä, samoin kuin pääsyn henkilötietoihin ja käsittelytoimiin.

Linjaus 1: Tietosuojan vastuunjako

Tietosuojavastaava
Helsingin kaupungin tietosuojavastaavan virkaan ottamisesta päättää hallintosäännön 8 luvun 1 §:n 5 kohdan mukaan kaupunginhallitus. Hallinnollisesti tietosuojavastaava sijoittuu kaupunginkanslian hallinto-osastolle.

Kaupungin tietosuojatiimi
Tietosuojan toteuttamisen varmistamiseksi kaupunginkanslian hallinto-osastolla on tietosuojavastaavan alaisuudessa kolme häntä avustavaa henkilöä, joista yksi on kelpoinen toimimaan tietosuojavastaavan sijaisena.

Tietosuoja toimialoilla, virastoissa ja liikelaitoksissa
Toimialojen, virastojen ja liikelaitosten johdolla on vastuu toiminnan lainmukaisuudesta tietosuoja-asioissa.

Tietosuojan vastuuhenkilö
Kullakin toimialalla, virastossa ja liikelaitoksessa on nimetty tietosuojan vastuuhenkilö, joka toimii tietosuoja-asioissa yhteyshenkilönä kyseisen organisaation ja tietosuojavastaavan välillä, opastaa ja neuvoo omaa organisaatiotaan tietosuoja-asioissa, osallistuu oman organisaationsa tietosuojan vaikutustenarviointiin sekä hankintoihin, jos sopimuksen perusteella toimittaja tulee käsittelemään henkilötietoja kaupungin lukuun.
On suositeltavaa, että tietosuoja-asioiden vastuuhenkilö on koulutukseltaan lakimies. Jos tämä ei ole mahdollista, tulisi vastuuhenkilön olla hallinnon asiantuntijatehtävissä toimiva.

Rekisterin vastuuhenkilö
Jokaiselle henkilörekisterille on nimetty vastuuhenkilö, joka omalta osaltaan vastaa kyseisen rekisterin tietosuojasta ja rekisteriselosteen lainmukaisuudesta. Rekisterin vastuuhenkilö vastaa rekisteröityjen tietopyyntöihin vastaamisesta sekä rekisteröityjen tiedonoikaisemisvaatimusten ja muiden rekisteröityjen oikeuksien toteuttamisesta.

Avustava henkilökunta
Vastuuhenkilöiden lisäksi toimialoilla, virastoilla ja liikelaitoksilla on oltava riittävästi avustavaa henkilökuntaa, joka osallistuu erityisesti rekisteröityjen tekemiin tietopyyntöihin vastaamiseen.

Tietoturva
Tietoturva-asiat liittyvät olennaisesti tietosuojaan. Kaupunginkansliassa tietosuojavastaavan tukena tietoturva-asioissa toimii tietohallinto ja erityisesti tietoturva-asiantuntija. Lisäksi toimialoilla, virastoissa ja liikelaitoksissa on oltava nimetty vastuuhenkilö myös tietoturva-asioissa.

Sijaisjärjestelyt
Kaikkien tietosuoja- ja tietoturva-asioissa vastuussa olevien henkilöiden osalta huolehditaan, että sijaistusjärjestelyt ovat riittävät.

Rekisteröidyn oikeuksista ja rekisterinpitäjän velvollisuuksista

Tietosuoja-asetuksessa säädetään rekisteröidyn oikeuksista. Tietosuoja-asetus asettaa vaatimuksia rekisterinpitäjälle rekisteröidyn henkilötietojen suojaamiseksi ja niiden käytön kontrolloimiseksi. Rekisteröidyn oikeuksien toteuttaminen kuuluu rekisterinpitäjän velvollisuuksiin. Rekisteröidyn oikeuksia on erilaisia ja ne vaihtelevat tietojen käsittelyperusteen mukaan. Erilaisia käsittelyperusteita ovat esimerkiksi rekisterinpitäjän lakisääteinen velvoite tai suostumus.

Rekisteröidyllä on mm. oikeus

- saada pääsy omiin henkilötietoihinsa
- tietojen oikaisemiseen: rekisteröity voi vaatia, että rekisterinpitäjä oikaisee virheelliset tai puutteelliset henkilötiedot
- tulla unohdetuksi eli rekisterinpitäjän on rekisteröidyn pyynnöstä poistettava henkilötiedot, jos henkilötietojen käsittely perustuu suostumukseen eikä henkilötietojen käsittelylle ole muuta laillista perustetta

Rekisteröidyllä on myös oikeus siirtää tiedot järjestelmästä toiseen. Tämä tarkoittaa, että rekisteröidyllä on oikeus saada henkilötietonsa jäsennellyssä, yleisesti käytetyssä ja koneellisesti

luettavassa muodossa, jolloin ne on mahdollista siirtää toiselle rekisterinpitäjälle. Oikeus sisältää myös mahdollisuuden saada henkilötiedot siirrettyä suoraan rekisterinpitäjältä toiselle, mikäli se on teknisesti mahdollista. Tätä rekisteröidyn oikeutta siirtää tiedot järjestelmästä toiseen ei kuitenkaan sovelleta käsittelyyn, joka on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi.

Linjaus 2: Rekisteröidyn oikeudet

Kaupunki pyrkii toteuttamaan rekisteröidyn oikeudet mahdollisimman asiakaslähtöisesti. Rekisteröity voi tehdä pyynnön omien tietojensa saamiseksi tai tietojen oikaisemiseksi kaupungin sähköisen asioinnin kautta. Sähköisessä asioinnissa asiakas tunnistetaan vahvaa tunnistautumista käyttäen. Vaihtoehtoisesti pyynnön voi tehdä myös henkilökohtaisesti kaupungin kirjaamossa ja erikseen nimetyssä toimialojen, virastojen ja liikelaitosten toimipisteissä.

Tietosuojalinjausten täytäntöönpanossa tulee pyrkiä kehittämään mahdollisimman helppoja tapoja kaupunkilaisille saada itseään koskevat tiedot käyttöönsä tietosuoja-asetuksen tarkoittamalla tavalla (ns. my data -periaate).

Tietosuoja-asetuksen nojalla rekisteröidyllä on oikeus saada läpinäkyvää informaatiota henkilötietojen käsittelystä. Rekisterinpitäjän on toimitettava henkilötietojen käsittelyä koskevat tiedot rekisteröidylle tiiviisti esitetyssä, läpinäkyvässä, helposti ymmärrettävässä ja saatavilla olevassa muodossa. Näiden tietojen on oltava julkisesti saatavilla ja ajantasaisia.

Rekisteröidylle on ilmoitettava hänen henkilötietojensa käsittelystä. Jos tiedot kerätään rekisteröidyltä itseltään, on ilmoitus tehtävä aina ja informoinnin on tapahduttava ennen tietojen keräämistä.

Linjaus 3: Rekisteröidyn informointi

Rekisteröidyn informointi toteutetaan käyttämällä Helsingin kaupungin internetsivuilla julkaistuja asiakkaan oikeuksista kertovaa sivustoa ja rekisterikohtaisia rekisteriselosteita.

Rekisterinpitäjän osoitusvelvollisuus

Tietosuoja-asetuksen 5 artiklan mukaan rekisterinpitäjän on pystyttävä osoittamaan, että henkilötietojen käsittelyä koskevia periaatteita on noudatettu.

Henkilötietojen käsittelytoimet tulee dokumentoida siinä määrin, että tietosuojaviranomaiset pystyvät jälkikäteen tarkastelemaan henkilötietoja käsittelevien organisaatioiden toimintaa ja tarvittaessa varmistamaan henkilötietojen käsittelyä sisältävien toimien lainmukaisuuden.

Kaikkien käsiteltävien henkilötietojen osalta on laadittava tietosuoja-asetuksen 30 artiklan mukainen seloste käsittelytoimista kaupunkiyhteisen mallin mukaisesti. Rekisterinpitäjän on pyynnöstä esitettävä seloste käsittelytoimista valvontaviranomaiselle.

Rekisterinpitäjän osoitusvelvollisuutta voidaan täyttää laatimalla organisaatio- ja vastuukuvauksia, prosessikuvauksia, järjestelmäkuvauksia, keräämällä lokitietoja henkilötietojen käsittelystä sekä laatimalla henkilötietojen käsittelyyn osallistuvalla henkilöstölle ohjeita ja koulutusmateriaalia.

Tietosuojan toteuttaminen edellyttää sitä, että kaikki henkilötietoja työssään käsittelevät henkilöt tuntevat henkilötietojen oikeat käsittelytavat.

Linjaus 4: Rekisterinpitäjän osoitusvelvollisuus

Jokainen toimiala, virasto ja liikelaitos huolehtii siitä, että se tekee tarpeelliset toimet osoitusvelvollisuuden toteuttamiseksi. Näitä ovat mm. selosteiden laatiminen toimialan/viraston/liikelaitoksen käsittelytoimista ja tietosuojaa edistävien toimenpiteiden dokumentointi. Kaupunki tulee toteuttamaan osoitusvelvollisuutta myös laatimalla tietotilinpäätöksen.

Kaupungin viranhaltijat ja työntekijät antavat salassapitositoumuksen. Henkilöstön koulutus tehdään suunnitellusti ja huomioiden eri tehtävissä toimivien henkilöiden erilaiset tiedon tarpeet. Viime kädessä esimiehet ovat vastuussa siitä, että heidän alaisensa ovat saaneet riittävän koulutuksen ja perehdytyksen henkilötietojen käsittelyyn. Henkilöstölle annettu koulutusmateriaali, koulutuksen ajankohdat ja koulutettujen henkilöiden nimet tallennetaan, jotta voidaan osoittaa tarvittaessa jälkikäteen, että kaupunki on huolehtinut kouluttamisvelvollisuudesta.

Tietojen suojaaminen

Tietosuoja-asetuksen mukaan rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet. Arvioitaessa sitä, mitä nämä toimenpiteet ovat, on otettava huomioon uusin tekniikka ja toteuttamiskustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä ihmisten oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit.

Linjaus 5: Tietojen suojaaminen

Tietojen suojaamisessa noudatetaan kaupungin tietoturvallisuusohjeita.

Lokitiedot

Lokitiedoilla tarkoitetaan tässä yhteydessä tietojärjestelmien keräämiä tietoja henkilötietojen käsittelystä kuten siitä, kuka on lisännyt, poistanut, muuttanut tai käynyt katsomassa henkilötietoja.

Lokitietoja keräämällä rekisterinpitäjä ja käsittelijä voivat täyttää osoitusvelvollisuutensa siitä, että henkilötietoja ovat käsitelleet vain ne henkilöt, joilla on ollut heidän työtehtäviinsä liittyvä peruste. Lokitietojen kerääminen edellyttää, että käyttöoikeudet ovat henkilökohtaisia.

Uusia tietojärjestelmiä hankittaessa yhtenä järjestelmävaatimuksena on, että järjestelmä kerää lokitiedot henkilötietojen käsittelystä, myös tietojen katselusta.

Nykyisten tietojärjestelmien osalta selvitetään lokitietojen keräämisen mahdollisuudet. Mitä keskeisemmästä tietojärjestelmästä on kyse ja mitä arkaluonteisempia sen keräämät henkilötiedot ovat, sitä välttämättömämpää lokitietojen kerääminen on. Jos järjestelmässä käsitellään salassa pidettävää tai arkaluontoista henkilötietoa, on järjestelmän kerättävä lokitiedot myös henkilötietojen katselusta.

Kerättyjä lokitietoja voidaan hyödyntää väärinkäytösepäilyjen selvittämisessä, rekisteröityjen pyyntöihin ja tiedusteluihin vastaamisessa sekä tietojärjestelmien käyttäjien toiminnan valvonnassa. Lokitietojen säilytysaika on 5 vuotta, ellei perustetta pidemmälle säilyttämiselle ole.

Vaikutustenarviointi: tietosuojan vaatimusten huomioiminen toiminnan kehittämisessä

Tietosuojaa koskeva vaikutustenarviointi (jäljempänä vaikutustenarviointi) on prosessi, jolla pyritään varmistamaan henkilötietojen käsittelyn yhdenmukaisuus tietosuoja-asetuksen vaatimusten kanssa. Samalla toteutetaan rekisterinpitäjän osoitusvelvollisuutta.

Jos tietyntyyppinen käsittely todennäköisesti aiheuttaa ihmisten oikeuksien ja vapauksien kannalta korkean riskin, rekisterinpitäjän on ennen käsittelyä toteutettava arviointi suunniteltujen käsittelytoimien vaikutuksista henkilötietojen suojalle. Rekisterinpitäjä vastaa vaikutustenarvioinnista ja voi suorittaa sen yhdessä käsittelijän kanssa. Tehtyä arviota voidaan käyttää samankaltaisiin vastaavia korkeita riskejä aiheuttaviin käsittelytoimiin. Vaikutustenarvioinnin tarpeellisuutta arvioitaessa on huomioitava käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset.

Vaikutustenarviointia tehdessään rekisterinpitäjän on pyydettävä neuvoja tietosuojavastaavalta, joka seuraa tietosuojavaikutusten arvioinnin suorittamista. Käsittelijän on annettava rekisterinpitäjälle arvioinnin suorittamiseksi tarpeelliset tiedot ja avustettava rekisterinpitäjää vaikutustenarvioinnin tekemisessä.

Velvollisuus vaikutustenarviointiin koskee käsittelyprosesseja, jotka on aloitettu 25.5.2018 tai sen jälkeen. Myös olennainen muutos käsittelyssä edellyttää vaikutustenarvioinnin tekemistä jo olemassa olevalle käsittelylle, erityisesti jos muutos vaikuttaa käsittelyn riskiin. Arviointi on suoritettava ennen prosessin tai järjestelmän käyttöönottoa.

Jos arvioidut riskit ovat korkeat, eikä niitä saada kaupungin toimenpiteillä hyväksyttävälle tasolle, on rekisterinpitäjällä velvollisuus ennakollisesti kuulla tietosuojaviranomaista sen selvittämiseksi, onko jäännösriski hyväksyttävä. Konsultoinnin yhteydessä tietosuojaviranomaiselle on toimitettava vaikutustenarviointi kokonaisuudessaan.

Linjaus 6: Vaikutustenarvioinnin tekeminen

Tarvetta vaikutustenarvioinnin tekemiseen arvioidaan alkukartoituksella. Vaikutustenarvioinnin tarvetta arvioidaan kokonaisuutena, mutta vaikutustenarviointi tehdään ainakin silloin kun

- käsitellään arkaluonteisia tai hyvin henkilökohtaisia tietoja
- ollaan ottamassa käyttöön uutta teknologiaa, jota ei ole kaupungilla aiemmin käytetty

Kaupungin toiminnan kehittämisessä käytetään Helsingin kaupungin kehittämismenetelmämallin (KEHMET) tietosuojaprosessia, johon on integroitu vaikutustenarvioinnin tekeminen. Hankinnoissa vaikutustenarviointi on aloitettava jo hankintaa suunniteltaessa.

Rekisterinpitäjän on tehtävä tarvittaessa uudelleentarkastelu arvioidakseen, tapahtuuko käsittely tietosuojaa koskevan vaikutustenarvioinnin mukaisesti, ainakin, jos käsittelytoimien sisältämä riski muuttuu. Tämä voi edellyttää alkuperäisen vaikutustenarvioinnin päivittämistä ja uusia riskiä vähentäviä toimenpiteitä.

Toimialojen, virastojen ja liikelaitosten tietohallinnot ja tietosuojan vastuuhenkilöt avustavat vaikutustenarvioinnin suorittamisessa ja ehdottavat arvioinnin tekemistä huomatessaan sen tarpeelliseksi.

Tietoturvaloukkausten ilmoittaminen

Henkilötietojen tietoturvaloukkauksella tarkoitetaan tapahtumaa, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu tai niihin pääsee käsiksi ulkopuolinen taho, jolla ei ole oikeutta käsitellä tietoja. Tietoturvaloukkaus voi tapahtua vahingossa tai tahallisesti.

Henkilötietojen tietoturvaloukkauksia ovat esimerkiksi tietojen lähettäminen väärälle henkilölle, murtautuminen henkilötietoja sisältävään järjestelmään, hakkerointi, kadonnut muistitikku, varastettu tietokone tai kadonnut henkilötietoja sisältävä paperi.

Rekisterinpitäjän tulee tehdä valvontaviranomaiselle ilmoitus henkilötietojen tietoturva-loukkauksesta ilman aiheetonta viivytystä heti ja viimeistään 72 tunnin sisällä siitä, kun loukkaus on tullut rekisterinpitäjän tietoon.

Valvontaviranomaiselle tehtävän ilmoituksen tulee sisältää vähintään seuraavat kohdat:

- kuvaus, mitä on tapahtunut
- mikäli mahdollista, niiden rekisteröityjen ryhmät ja lukumäärät, joita loukkaus on koskenut
- tietosuojavastaavan nimi ja yhteystiedot
- millaisia vaikutuksia henkilötietojen tietoturvaloukkauksella voi todennäköisesti olla rekisteröidylle
- kuvaus niistä toimenpiteistä, jotka rekisterinpitäjä aikoo toteuttaa tai jotka se on jo toteuttanut haittavaikutuksen lieventämiseksi ja tilanteen ratkaisemiseksi.

Jos ilmoitusta ei pystytä tekemään 72 tunnissa, on rekisterinpitäjän ilmoitettava valvontaviranomaiselle perusteltu syy viivästykselle.

Jos loukkaus todennäköisesti aiheuttaa suuren riskin yksilön oikeuksille ja vapauksille, erimerkiksi identiteettivarkauksien, maksuvälinepetosten tai muun rikollisen toiminnan muodossa, on henkilötietojen tietoturvaloukkauksesta ilmoitettava rekisteröidyille.

Rekisterinpitäjä voi ilmoittaa vuodosta julkisella tiedonannolla, esimerkiksi median välityksellä, jos henkilökohtaisten ilmoitusten lähettäminen vaatisi kohtuutonta vaivaa.

Linjaus 7: Tietoturvaloukkaukset

Helsingin kaupunki varmistaa kyvykkyytensä havaita tietoturvapoikkeamat, selvittää poikkeamien syyt ja seuraukset sekä vaikutukset yksityisyydensuojaan. Kaupunki minimoi poikkeamien aiheuttamat vahingot sekä tekee tarvittavat ilmoitukset.

Tietoturvaloukkausten osalta noudatetaan kaupungin tietoturvaloukkausprosessia ja se sisältyy kaupungin kriisiviestintäprosesseihin.

Hankinnat ja sopimukset

Rekisterinpitäjä saa käyttää ainoastaan sellaisia henkilötietojen käsittelijöitä, jotka toteuttavat riittävät tekniset ja organisatoriset suojatoimet. Käsittelyn on täytettävä tietosuoja-asetuksen vaatimukset ja varmistettava rekisteröidyn oikeuksien suojelu. Tämä voi edellyttää vaikutustenarvioinnin tekemistä jo hankinnan suunnitteluvaiheessa.

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

Henkilötietojen käsittelijän suorittamaa käsittelyä on määritettävä rekisterinpitäjän ja käsittelijän välisellä sopimuksella. Sopimuksessa on sovittava erityisesti, että henkilötietojen käsittelijä

- käsittelee henkilötietoja ainoastaan rekisterinpitäjän antamien dokumentoitujen ohjeiden mukaisesti
- varmistaa, että henkilöt, joilla on oikeus käsitellä henkilötietoja, ovat sitoutuneet noudattamaan salassapitovelvollisuutta
- auttaa rekisterinpitäjää täyttämään rekisterinpitäjän velvollisuuden vastata pyyntöihin, jotka koskevat rekisteröityjen oikeuksien käyttämistä, sekä
- auttaa rekisterinpitäjää täyttämään tietoturvaloukkauksia koskevan ilmoitusvelvollisuuden.

Henkilötietojen käsittelijä on vastuussa vahingosta, joka on aiheutunut tietosuoja-asetuksen vastaisesta käsittelystä vain, jos se ei ole noudattanut tietosuoja-asetuksessa sille asetettuja velvoitteita tai jos se ei ole toiminut rekisterinpitäjän lainmukaisten ohjeiden mukaisesti.

Linjaus 8: Sopimukset

Tämän ohjeen liitteenä on malli rekisterinpitäjän ja käsittelijän väliseen sopimukseen liitettävästä tietosuoja- ja salassapitoliitteestä, jossa on määritelty henkilötietojen käsittelyn edellytykset. Lähtökohtaisesti kaupungin sopimuksissa käytetään tämän mallin mukaista liitettä. Tietosuoja- ja salassapitoliite tai muut tietosuoja-asetuksen 28 artiklan vaatimukset täyttävät ehdot sisällytetään kaikkiin uusiin sopimuksiin, joiden perusteella käsittelijä käsittelee henkilötietoja kaupungin lukuun.

Tietosuoja- ja salassapitoliite on osa kaupungin antamaa henkilötietojen käsittelyä koskevaa ohjeistusta.

Uusissa sopimuksissa on lisäksi huomioitava, että

- rekisteröityjä koskevat tiedot voidaan luovuttaa konekielisessä muodossa silloin, kun siihen on velvollisuus
- tietojärjestelmät keräävät käyttäjälokitietoja tietojen käsittelystä (mukaan lukien tietojen katsominen)
- tiedot pystytään poistamaan järjestelmästä joko rekisteröidyn pyynnöstä tai käyttötarkoituksen mukaisen säilytysajan päättyessä.

Voimassaolevat sopimukset, joiden perusteella käsittelijä käsittelee henkilötietoja kaupungin lukuun, käydään läpi sen arvioimiseksi, ovatko sopimuksen sisältämät henkilötietojen käsittelyä koskevat ehdot riittäviä takaamaan sen, että henkilötietojen käsittely on lainmukaista.

Voimassa olevien sopimusten osalta voidaan joutua neuvottelemaan sopimusmuutoksista myös, jos järjestelmät eivät täytä kaikkien tietosuoja-asetuksen edellyttämiä teknisiä vaatimuksia (esim. oikeus saada henkilötiedot itselleen konekielisessä muodossa, tietojen poistaminen joko rekisteröidyn pyynnöstä tai säilytysajan päättyessä).

Henkilötietojen käsittely EU/ETA-alueen ulkopuolella

Henkilötietojen siirtäminen EU/ETA alueen ulkopuolelle voi heikentää luonnollisten henkilöiden mahdollisuuksia käyttää oikeuttaan tietosuojaan ja erityisesti mahdollisuutta suojella henkilötietoja henkilötietojen tietoturvaloukkaustilanteissa. EU/ETA-alueen ulkopuolella henkilötietoja voidaan käsitellä vain, jos EU/ETA alueen ulkopuolisten maiden tietosuojan taso on tietosuoja-asetuksen asettamien edellytysten mukaisesti riittävällä tasolla.

Pseudonymisointi tarkoittaa henkilötietojen käsittelemistä siten, että henkilötietoja ei voida enää yhdistää tiettyyn rekisteröityyn käyttämättä lisätietoja. Tällaiset lisätiedot säilytetään erillään henkilötiedoista varmistaen, ettei henkilötietojen yhdistämistä tunnistettuun tai tunnistettavissa olevaan henkilöön tapahdu.

Linjaus 9: Yleistä henkilötietojen käsittelystä EU/ETA-alueen ulkopuolella

Henkilötietojen käsittelyn EU/ETA-alueen ulkopuolella tulee aina perustua tietosuoja-vaikutusten ja -riskien arviointiin.

Suunniteltaessa hankintaa, joka sisältää tietojen käsittelyä Suomen ulkopuolella, otetaan huomioon, että hankittava tietojärjestelmä täyttää Helsingin kaupunkikonsernin valmiusohjeessa ja kaupungin tietoturvallisuusohjeissa asetetut vaatimukset tietojärjestelmien tietoturvasta ja varautumisesta. Lisäksi huolehditaan siitä, että voimassaole-via sopimuksia muutettaessa otetaan huomioon alkuperäisessä sopimuksessa sovittu henkilötietojen käsittelyalue. Esimerkiksi on voitu sopia siitä, että tietyt palvelimet sijaitsevat Suomessa.

Linjaus 10: Korkeariskisten henkilötietojen käsittely EU/ETA-alueen ulkopuolella

Korkeariskisillä henkilötiedoilla tarkoitetaan näissä linjauksissa sekä lakisääteisessä toiminnassa että muussa toiminnassa käsiteltäviä:

- salassa pidettäviä henkilötietoja
- erityisiä henkilötietoryhmiä koskevia henkilötietoja
- muita sellaisia henkilötietoja, jotka ovat omiaan aiheuttamaan korkean riskin rekisteröidyn oikeuksille ja vapauksille (kuten henkilötunnus).

Euroopan komission hyväksymillä mailla tarkoitetaan näissä linjauksissa EU/ETA –alueen ulkopuolisia maita, joiden tietosuojan tason komissio on hyväksynyt riittäväksi. Jos komissio on hyväksynyt tietosuojan tason riittäväksi tietyillä erityisjärjestelyillä, kuten Yhdysvalloissa Privacy Shield -järjestelyyn kuuluvien yritysten osalta, kaupunki sallii henkilötietojen käsittelyn vain seuraavilla edellytyksillä:

- palveluntuottajan pysymistä järjestelyn piirissä seurataan
- palvelusta voidaan tarvittaessa luopua, jos yritys poistuu erityisjärjestelyn piiristä

Pääsääntöisesti kaupunki ei salli korkeariskisten henkilötietojen käsittelyä EU/ETA-alueen ulkopuolella lakisääteisessä toiminnassaan eikä kaupungin muussa toiminnassa.

Poikkeuksellisesti kaupunki sallii korkeariskisten henkilötietojen käsittelyn Euroopan komission hyväksymissä maissa silloin, kun salassa pidettävän tiedon tai muun korkeariskisen tiedon luonne on sellainen, että kaupungin omista lähtökohdista (esim. valmiuskysymykset) ei muodostu estettä käsittelylle.

Poikkeuksellisesti kaupunki sallii korkeariskisten henkilötietojen käsittelyn EU/ETA –alueen ja Euroopan komission hyväksymien maiden ulkopuolella silloin, kun jokin seuraavista edellytyksistä täyttyy:

- käsittely on vähäistä ja väliaikaista (esimerkiksi käsittelijä käsittelee korkeariskisiä henkilötietoja poikkeustilanteessa kuten vikatilanteessa)

- käsittelyn pääasiallinen tarkoitus ei ole henkilötietojen käsittely vaan siinä on kysymys vain järjestelmän tekniseen ylläpitoon liittyvistä tehtävistä, jolloin käsittelijä käsittelee korkeariskisisiä henkilötietoja pseudonymisoituina
- rekisteröity on antanut suostumuksensa käsittelylle ja
    - kaupungin palvelun luonne on sellainen, että käsittely voidaan perustaa suostumukseen ja suostumukseen perustuva käsittely ei vaaranna palvelun käyttäjien tasapuolista kohtelua
    - lakisääteiseen palveluun voidaan tuottaa ylimääräinen lisäpalvelu, joka perustuu suostumukseen. Tällöin lakisääteinen palvelu pitää kuitenkin voida tuottaa myös ilman suostumukseen perustuvaa lisäpalvelua

Lisäksi seuraavien edellytysten on aina täytyttävä:

- tietosuojan tosiasiallinen riittävä taso varmistetaan ennen sopimuksen tekemistä
- noudatetaan tietosuoja-asetuksen asettamia edellytyksiä tietojen siirrolle kolmansiin maihin.

Linjaus 11: Vähäriskisten henkilötietojen käsittely lakisääteisessä toiminnassa EU/ETA-alueen ulkopuolella

Vähäriskisillä henkilötiedoilla tarkoitetaan näissä linjauksissa muita kuin erityisiä henkilötietoryhmiä koskevia henkilötietoja, salassa pidettäviä henkilötietoja tai luonteeltaan muuten korkeariskisiä henkilötietoja.

Pääsääntöisesti kaupunki sallii lakisääteisessä toiminnassa käsiteltävien vähäriskisten henkilötietojen käsittelyn vain EU/ETA-alueella ja Euroopan komission hyväksymissä maissa.

Poikkeuksellisesti käsittely EU/ETA-alueen ja Euroopan komission hyväksymien maiden ulkopuolella sallitaan seuraavilla edellytyksillä:

- käsittely on poikkeuksellisesti tarpeellista
- tietosuojan tosiasiallinen riittävä taso varmistetaan ennen sopimuksen tekemistä
- noudatetaan tietosuoja-asetuksen asettamia edellytyksiä tietojen siirrolle kolmansiin maihin.

Linjaus 12: Vähäriskisten henkilötietojen käsittely muussa kuin lakisääteisessä toiminnassa EU/ETA-alueen ulkopuolella

Muussa kuin lakisääteisessä toiminnassaan kaupunki sallii vähäriskisten henkilötietojen käsittelyn EU/ETA-alueella ja Euroopan komission hyväksymissä maissa. Niiden ulkopuolella käsittely hyväksytään seuraavilla edellytyksillä:

- tietosuojan tosiasiallinen riittävä taso varmistetaan ennen sopimuksen tekemistä
- noudatetaan tietosuoja-asetuksen asettamia edellytyksiä tietojen siirrolle kolmansiin maihin.

Lisätietoja

Työntekijät saavat ohjeistusta henkilötietojen käsittelystä esimiehiltään, rekisteriselosteessa mainituilta vastuuhenkilöiltä, toimialan, viraston tai liikelaitoksen tietosuojan vastuuhenkilöltä tai tietosuojavastaavalta.

Tietoturvaan liittyvissä kysymyksissä neuvovat kunkin toimialan, viraston tai liikelaitoksen tietoturvan asiantuntijat.

Sopimuksiin ja hankintoihin liittyvissä kysymyksissä neuvoo kukin toimiala, virasto ja liikelaitos omien sopimustensa osalta. Tarvittaessa voi olla yhteydessä kaupunginkanslian oikeus-palveluiden sopimukset ja hankinnat -tiimiin.

Tietoa rekisteröidyn oikeuksista ja henkilötietojen käsittelystä Helsingin kaupungilla on sivustolla www.hel.fi/tietosuoja.

Liite: Tietosuoja- ja salassapitoliite