Helsingin kaupungin tietosuojalinjaukset

Henkilötietojen käsittelyperiaatteet

EU:n tietosuoja-asetus (EU 2016/679) tulee voimaan 25.5.2018. Tietosuoja-asetuksessa vahvistetaan säännöt luonnollisten henkilöiden suojelulle henkilötietojen käsittelyssä.

Tämä asiakirja sisältää ohjeita sekä valmistautumisesta tietosuoja-asetuksen voimaantuloon että henkilötietojen käsittelystä tietosuoja-asetuksen voimaan tulon jälkeen. Ohjetta täydennetään, kun valmisteilla oleva kansallisen henkilötietolainsäädännön uudistus etenee ja kun asetuksen soveltamisesta saadaan tarkempia ohjeita valvontaviranomaisilta.

Tietosuoja-asetuksen mukaiset henkilötietojen käsittelyn perusperiaatteet ovat pitkälti nykyisen kansallisen henkilötietolainsäädännön mukaisia. Tietosuoja-asetus antaa kuitenkin rekisteröidylle uusia oikeuksia ja vastaavasti rekisterinpitäjälle ja henkilötietojen käsittelijöille uusia velvollisuuksia.

Tietosuoja-asetus tuo mukaan myös entistä ankarampia seuraamuksia henkilötietojen virheellisestä käsittelystä. Rekisteröidyllä on oikeus saada vahingonkorvausta, kun hänen oikeuksiaan on loukattu, vaikka hänelle ei olisikaan aiheutunut taloudellista vahinkoa. Lisäksi rekisterinpitäjä tai käsittelijä voidaan velvoittaa maksamaan hallinnollista sakkoa. Enimmillään hallinnollisen sakon määrä voi olla 20 miljoonaa euroa tai 4 % rekisterinpitäjän vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta. Hallinnollisen sakon yläraja on korkea, jotta se olisi riittävä pelote suurille monikansallisille yrityksille. Oikeuskäytännössä tulee aikanaan täsmentymään, mille tasoille hallinnolliset sakot tulevat asettumaan. Tiedossa ei vielä ole, koskeeko hallinnollisen sakon maksuvelvollisuus Suomessa julkisyhteisöjä.

Kaupunki kunnioittaa toiminnassaan yksityishenkilöiden oikeutta yksityisyyden suojaan

Kaupungin toiminnassa toteutetaan kahta osittain vastakkaista perusoikeutta eli hallinnon julkisuutta ja yksityisyydensuojaa.

Hallinnon julkisuudesta on säädetty Euroopan unionin perusoikeuskirjan 41-42 artikloissa Euroopan unionin asiakirjojen osalta, tietosuoja-asetuksen 86 artiklassa sekä Suomen perustuslain 12 § 2 momentissa ja kansallisessa julkisuuslainsäädännössä.

Yksityisyyden suojasta on säädetty Euroopan unionin perustusoikeusasiakirjan 7-8 artikloissa ja tietosuoja-asetuksessa sekä Suomen perustuslain 8 § 1 momentissa ja julkisuuslainsäädännön salassapitosäädöksissä.

Suomen perustuslain mukaan viranomaisen hallussa olevat asiakirjat ja muut tallenteet ovat julkisia, jollei niiden julkisuutta ole välttämättömien syiden vuoksi lailla erikseen rajoitettu, ja jokaisella on oikeus saada tieto julkisesta asiakirjasta ja tallenteesta. Hallinnon julkisuudella on Suomessa pitkä perinne. Se on olennainen osa avointa kansalaisyhteiskuntaa ja merkittävä tekijä korruption ehkäisyssä ja hallinnon lainmukaisuuden valvonnassa.

Euroopan unionin tietosuoja-asetus on Suomessa laintasoinen säädös, joten sen säädöksillä voidaan rajoittaa viranomaisen asiakirjojen julkisuutta. Tietosuoja-asetukseen on kuitenkin otettu 86. artikla, jonka mukaan viranomaiset voivat yleisen edun vuoksi toteutetun tehtävän suorittamiseksi luovuttaa viranomaisten hallussa olevien virallisten asiakirjojen sisältämiä henkilötietoja viranomaiseen sovellettavan unionin oikeuden tai jäsenvaltion lainsäädännön mukaisesti, jotta voidaan sovittaa yhteen virallisten asiakirjojen julkisuus ja tietosuoja-asetuksen mukainen oikeus henkilötietojen suojaan. Näin ollen viranomaisten asiakirjoissa ja tallenteissa olevien henkilötietojen julkisuudesta ja saatavuudesta säädetään kansallisella julkisuuslainsäädännöllä.

Kaupunki sovittaa yhteen toiminnassaan yksityishenkilöiden yksityisyyden suojan ja hallinnon toiminnan avoimuuden ja julkisuuden lainsäädännössä säädetyllä tavalla.

Henkilötietojen käsittely

Helsingin kaupunki käsittelee henkilötietoja vain, kun se on kaupungin toimintojen toteuttamiseksi välttämätöntä ja sille on lain mukainen peruste. Henkilötietojen käsittelystä on tiedotettava 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. Poikkeuksellisesti henkilötietoja voidaan säilyttää pidempiä aikoja, jos henkilötietoja käsitellään yleisen edun mukaisia arkistointitarkoituksia tai historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten.

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

Henkilötiedon määritelmä

Henkilötiedolta tarkoitetaan kaikki tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja. Tunnistettavissa olevana pidetään henkilöä, joka voidaan tunnistaa

suoraan tai epäsuorasti erityisesti tunnistetietojen kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen tai henkilölle tunnusomaisten fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella.[1]

Henkilötietoja voivat olla muun muassa osoite, sähköpostiosoite, valokuva, ääni- tai videotallenne, auton rekisterinumero, sormenjälki tai muu biologinen näyte.

Epäsuoralla tunnistamisella tarkoitetaan sitä, että henkilö voidaan tunnistaa yhdistämällä tiedot toisesta lähteestä saatavien tietojen kanssa. Tietoja, joista henkilö on tunnistettavissa vain epäsuorasti, kutsutaan pseudonymisoiduiksi tiedoiksi.

Tietosuoja-asetus ei koske anonymisoituja henkilötietoja. Anonymisoitujen henkilötietojen tunnistettavuus on poistettu siten, ettei rekisteröidyn tunnistaminen ole mahdollista edes yhdistämällä tiedot muualta saataviin tietoihin. Anonymisoituja tietoja käsitellään mm. tilasto- ja tutkimustarkoituksia varten.

Henkilötiedon käsittelyn määritelmä

Henkilötiedon käsittelyllä tarkoitetaan henkilötietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakua, kyselyä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittamista, yhdistämistä, rajoittamista, poistamista tai tuhoamista.[2]

Henkilörekisterin määritelmä

Henkilörekisterillä tarkoitetaan jäsenneltyä henkilötietoja sisältävää tietojoukkoa, josta tiedot on saatavissa tietyin perustein. Henkilörekisteri voi koostua niin sähköisesti kuin paperillekin tallennetuista tiedoista.

Koska henkilötietoja saa käsitellä?

Henkilötietoja saa muun muassa käsitellä, kun

- siihen on rekisteröidyn suostumus
- käsittely on tarpeen kaupungin lakisääteisten velvoitteiden noudattamiseksi tai julkisen vallan käyttämiseksi;
- rekisteröity on sopimusosapuolena ja käsittely on tarpeen sopimuksen täytäntöön panemiseksi tai sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi tai;
- käsittely on tarpeen rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi.[3]

---

[1] Tietosuoja-asetus 4 art.

[2] Tietosuoja-asetus 4 art.

[3] Tietosuoja-asetus 6 art.

Suostumus on pyydettävä rekisteröidyltä selkeällä ja yksinkertaisella kielellä selvästi erillään muista asioista. Rekisteröity voi koska tahansa peruuttaa suostumuksensa. Suostumuksen peruuttamisen on oltava yhtä helppoa kuin sen antaminen.

Mikäli Helsingin kaupunki tarjoaa sähköisiä, etäkäyttöön perustuvia palveluja alle 16-vuotiaille lapsille, on lapsen henkilötietojen käsittelyyn saatava lapsen huoltajan suostumus. Lapsen huoltajan suostumusta ei tarvita silloin, kun lasten henkilötietoja käsitellään esimerkiksi kaupungin lakisääteisten velvoitteiden noudattamiseksi tai julkisen vallan käyttämiseksi. Kansallisesti voidaan säätää alemmasta iästä, joka ei saa olla alle 13 vuotta, mutta tällaista kansallista lainsäädäntöä ei vielä ole.

Erityisiin henkilötietoryhmiin kuuluvien tietojen käsittely (arkaluonteiset tiedot)

Tietosuoja-asetuksessa on määritelty erityiset henkilötietoryhmät, joiden käsittelylle on asetetut tiukemmat perusteet. Erityiset henkilötietoryhmät vastaavat pitkälti nykyisen henkilötietolain arkaluonteisia tietoja. Erityisiä henkilötietoja ovat rotu, etninen alkuperä, poliittinen mielipide, uskonnollinen tai filosofinen vakaumus, ammattiliiton jäsenyys, geneettiset tai biometriset tiedot, joita käytetään henkilön tunnistamiseksi, terveyttä koskevat tiedot sekä luonnollisen henkilön seksuaalista käyttäytymistä ja suuntautumista koskevat tiedot.[4]

Mikäli erityisiin henkilötietoryhmiin kuuluvia tietoja aiotaan käsitellä, on huolellisesti selvitettävä, että tietojen käsittely on tietosuoja-asetuksen 9 artiklan nojalla sallittua.

Lisäksi rikostuomioihin ja rikkomuksiin liittyvien henkilötietojen käsittelystä on tietosuoja-asetuksessa oma artiklansa. Rikoksiin tai rikkomuksiin liittyviä tietoja ei tulisi käsitellä muutoin kuin silloin kun kyse on kaupunkiin kohdistuvasta rikoksesta tai rikkomuksesta tai kun kyse on kaupungin palveluksessa olevan tekemästä rikoksesta tai rikkomuksesta, jolla on merkitystä henkilön palvelussuhteen kannalta, tai tietojen käsittelylle on muu joko kaupungin tai kolmannen henkilön oikeuksiin ja velvollisuuksiin liittyvä painava peruste.[5]

Rikosrekisteriotteiden käsittelystä on säädetty erityislainsäädännössä kuten laissa lasten kanssa työskentelevien rikostaustan selvittämisestä sekä laissa julkisista hankinnoista ja käyttöoikeussopimuksista.

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.

Osoitusvelvollisuuden täyttämiseksi on kaikista henkilörekistereistä laadittava rekisteriseloste.

---

[4] Tietosuoja-asetus 9 art.

[5] Tietosuoja-asetus 10 art.

Rekisteriselosteen on sisällettävä seuraavat tiedot:

1. Rekisterinpitäjän, rekisterinpitäjän edustajan ja tietosuojavastaavan nimi ja yhteystiedot;

2. Käsittelyn tarkoitukset sekä käsittelyn oikeusperuste;

3. Kuvaus rekisteröityjen ryhmistä ja henkilötietoryhmistä;

4. Henkilötietojen vastaanottajat tai vastaanottajaryhmät;

5. Tarvittaessa tiedot henkilötietojen siirtämisestä kolmanteen maahan tai kansainväliselle järjestölle, sekä asianmukaisia suojatoimia koskevat asiakirjat;

6. Henkilötietojen säilytysaika tai jos se ei ole mahdollista, tämän ajan määrittämiskriteerit,

7. Mahdollisuuksien mukaan yleinen kuvaus teknisistä ja organisatorisista suojatoimista.[6]

Rekisteriselostetta voidaan käyttää hyväksi myös ilmoitettaessa rekisteröidylle hänen henkilötietojensa käsittelystä. Ilmoitus rekisteröidylle on tehtävä aina, jos henkilötietoja kerätään rekisteröidyltä.

Jos tietoja on saatu muusta lähteestä kuin rekisteröidyltä, rekisterinpitäjän on lähtökohtaisesti tehtävä ilmoitus. Ilmoitusta ei tarvitse tehdä, jos rekisteröity on jo saanut tiedot tai kyseisten tietojen toimittaminen osoittautuu mahdottomaksi tai vaatisi kohtuutonta vaivaa tai tietojen hankinnasta tai luovuttamisesta säädetään nimenomaisesti lainsäädännössä, jossa vahvistetaan asianmukaiset toimenpiteet oikeutettujen etujen suojaamiseksi. Esimerkiksi jos viranomaisella on velvollisuus lain nojalla luovuttaa henkilötietoja toiselle viranomaiselle, ei vastaanottava viranomainen ole velvollinen ilmoittamaan rekisteröidylle tämän tietojen vastaanottamisesta.

Rekisteröidylle tehtävän ilmoituksen on sisällettävä edellä mainitut rekisteriselosteen tiedot sekä seuraavat tiedot:

8. Rekisteröidyn oikeus pyytää rekisterinpitäjältä pääsy häntä itseään koskeviin henkilötietoihin sekä oikeus pyytää kyseisten tietojen oikaisemista tai poistamista taikka käsittelyn rajoittamista tai vastustaa käsittelyä sekä oikeutta siirtää tiedot järjestelmästä toiseen,

9. Oikeus peruuttaa mahdollinen suostumus milloin tahansa,

10. Oikeus tehdä valitus valitusviranomaiselle,

11. Onko henkilötietojen antaminen lakisääteinen tai sopimukseen perustuva vaatimus taikka sopimuksen tekemisen edellyttämä vaatimus sekä onko rekisteröidyn pakko toimittaa henkilötiedot ja tällaisten tietojen antamatta jättämisen mahdolliset seuraukset,

---

[6] Tietosuoja-asetus 30 art.

12. Mistä henkilötiedot on saatu sekä tarvittaessa se, onko tiedot saatu yleisesti saatavilla olevasta lähteestä.

13. Mahdollisen automaattisen päätöksenteon kuten profiloinnin olemassaolo.[7]

Jotta ei tarvitse laatia useita asiakirjoja samasta rekisteristä, rekisteriselosteeseen sisällytetään myös rekisteröidylle tehtävän ilmoituksen sisältämät tiedot.

Rekisteriselosteiden lisäksi rekisterinpitäjän osoitusvelvollisuus voidaan täyttää laatimalla organisaatio- ja vastuukuvauksia, prosessikuvauksia, järjestelmäkuvauksia, keräämällä lokitietoja henkilötietojen käsittelystä sekä laatimalla henkilötietojen käsittelyyn osallistuvalla henkilöstölle ohjeita ja koulutusmateriaalia.

Mitä keskeisemmästä henkilörekisteristä on kyse ja mitä arkaluontoisempia sen sisältämät henkilötiedot ovat, sitä huolellisemmin on rekisterinpitäjän osoitusvelvollisuus täytettävä.

Kaupungin henkilöstön henkilötietojen käsittely

Kaupungin palveluksessa olevien henkilöiden palvelussuhteeseen liittyvien henkilötietojen käsittelyssä noudatetaan samoja tietosuoja-asetuksen mukaisia periaatteita kuin muidenkin henkilötietojen osalta. Huomioon on kuitenkin otettava näitä tietoja koskeva erityislainsäädäntö kuten nimikirjalaki ja laki yksityisyyden suojasta työelämässä.

Nimikirjalain nojalla kaupungin henkilöstön palkkatiedot ovat julkisia. Yksityisyyden suojasta työelämässä annettu laki taasen rajoittaa tiettyjen henkilötietojen kuten luottotietojen tai psykologisista arvioinneista saatujen tietojen käsittelyä.

Rekisteröityjen oikeudet

Tietosuoja-asetuksessa säädetään rekisteröidyn oikeuksista. Osa oikeuksista on jo nykyisen voimassa olevan kansallisen lainsäädännön mukaisia, mutta asetus luo myös uusia oikeuksia rekisteröidylle ja yksityiskohtaisempia vaatimuksia rekisterinpitäjälle rekisteröidyn henkilötietojen suojaamiseksi ja niiden käytön kontrolloimiseksi. Rekisteröidyn oikeuksien toteuttaminen kuuluu rekisterinpitäjän velvollisuuksiin. On kuitenkin huomioitava, että rekisteröidyn oikeudet riippuvat monissa tapauksissa tietojen käsittelyperusteesta eli siitä, perustuuko tietojen käsittely esimerkiksi suostumukseen vai julkisen vallan käyttöön.

Oikeus saada läpinäkyvää informaatiota ja oikeus saada tieto tietoturvaloukkauksesta

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, esimerkiksi tietosuoja- tai rekisteriselosteessa. Näiden tietojen on oltava lisäksi julkisesti saatavilla ja ajantasaisia.

---

[7] Tietosuoja-asetus 13 ja 14 art.

Mikäli tiedot kerätään rekisteröidyltä itseltään, informoinnin on tapahduttava ennen tietojen keräämistä. Jos tietoja on kerätty muusta lähteestä kuin rekisteröidyltä, tietyin poikkeuksin tieto henkilötietojen käsittelystä on toimitettava rekisteröidylle kohtuullisen ajan kuluttua, ja viimeistään kuukauden kuluessa henkilötietojen saamisesta. Rekisteröidylle annettavan ilmoituksen on rekisteriselosteen tietojen lisäksi sisällettävä tietoa muun muassa rekisteröidyn oikeuksista ja niiden toteuttamisesta.

Asetuksen mukaisesti rekisteröidyllä on myös oikeus saada tieto henkilötietojensa tietoturvaloukkauksista: rekisterinpitäjän uutena velvollisuutena on ilmoittaa henkilötietojen tietoturvaloukkaustilanteista, joissa henkilötietojen luottamuksellisuus on vaarantunut (rekisterinpitäjän ilmoitusvelvollisuus).

Oikeus saada pääsy tietoihin

Tietosuoja-asetuksen mukaisesti rekisteröidyllä on oikeus saada pääsy omiin henkilötietoihinsa (oikeus saada pääsy tietoihin). Rekisterinpitäjän on rekisteröidyn pyytäessä ilmoitettava, käsitelläänkö häntä koskevia henkilötietoja sekä toimitettava jäljennös käsiteltävistä henkilötiedoista. Tietosuoja-asetuksessa pyynnölle ei ole säädetty määrämuotoa. Mikäli pyyntö käyttää tätä oikeutta esitetään sähköisesti, rekisterinpitäjän on toimitettava tiedot yleisesti käytetyssä sähköisessä muodossa, ellei rekisteröity toisin pyydä. Oikeuden käyttäminen on lähtökohtaisesti maksutonta.

Oikeus tulla unohdetuksi sekä oikeus tietojen oikaisuun, käsittelyn rajoittamiseen ja käsittelyn vastustamiseen

Tietosuoja-asetuksella luotu uusi oikeus on rekisteröidyn oikeus tulla unohdetuksi. Tämä tarkoittaa, että rekisterinpitäjän on rekisteröidyn pyynnöstä poistettava henkilötiedot, ellei käsittelylle ole muuta laillista perustetta. Tähän liittyen rekisteröidyllä on aina oikeus peruuttaa antamansa suostumus henkilötietojensa käsittelyyn, ja mahdollisuudesta tämän oikeuden käyttämiseen on informoitava selkeästi.

Rekisteröidyllä on asetuksen mukaisesti myös oikeus tietojen oikaisemiseen: rekisteröity voi vaatia, että rekisterinpitäjä oikaisee virheelliset tai puutteelliset henkilötiedot. Rekisteröidyllä on myös tietyissä asetuksessa mainituissa tilanteissa oikeus rajoittaa omien tietojensa aktiivista käsittelyä (oikeus käsittelyn rajoittamiseen). Tällöin rekisterinpitäjä saa edelleen säilyttää tietoja, muttei muutoin käsitellä niitä ilman rekisteröidyn suostumusta.

Mikäli tietojen käsittely perustuu yleistä etua koskevan tehtävän suorittamiseen tai rekisterinpitäjälle kuuluvan julkisen vallan käyttöön taikka rekisterinpitäjän tai kolmannen oikeutetun edun toteuttamiseen, rekisteröidyillä on oikeus vastustaa henkilötietojensa käsittelyä. Tällöin rekisterinpitäjä ei lähtökohtaisesti saa käsitellä rekisteröidyn henkilötietoja ellei huomattavan tärkeästä ja perustellusta syytä muuta johdu.

Oikeus siirtää tiedot järjestelmästä toiseen

Tietosuoja-asetuksen mukaisesti 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.

Oikeus vastustaa automaattista päätöksentekoa ja profilointia

Asetuksen mukaan rekisteröidyllä on oikeus vaatia, että tiedot käsittelee rekisterinpitäjän puolesta luonnollinen henkilö. Päätöksenteko ei siis saa perustua pelkästään automaattiseen tietojenkäsittelyyn, kuten profilointiin. Rekisteröity on myös oikeutettu esittämään kantansa asiassa ja riitauttamaan tehdyn päätöksen (oikeus vastustaa automaattista päätöksentekoa ja profiloinnin kieltäminen).

Tietojen suojaaminen

Tietoturvan huomioiminen tietosuojaa vaativia tietoja käsiteltäessä

Käsiteltiinpä henkilötietoja tietojärjestelmissä, paperilla, kuvina, keskustelemalla puhelimessa tai kasvokkain, niin aina tulee huolehtia, etteivät henkilötiedot joudu asiattomien saataville.

henkilötietoja käsitellessä tulee varmistua siitä, että paikka soveltuu henkilötietojen käsittelyyn. Asiattomien ei tule voida kuulla mitä puhutaan tai katsella mitä tietoja käytetään.

Henkilötietojen käsittely tietojärjestelmissä tehdään aina työtehtävään perustuen ja omalla henkilökohtaisella käyttäjätunnuksella, toisten henkilöiden tunnuksia ei saa käyttää. Verkon ja ohjelmistojen käyttöoikeudet ovat henkilökohtaisia. Jokainen vastaa omilla käyttöoikeuksillaan tehdyistä henkilötietojen käsittelystä eikä käyttötunnuksia tule antaa muiden käyttöön.

Henkilötietoja ei tule kopioida tietojärjestelmästä sen ulkopuolelle. Henkilötietoja saa siirtää vain sellaisiin tallennuspaikkoihin, joissa ne säilyvät rekisteriselosteen mukaisesti.

Turvapostia voidaan käyttää henkilötietojen toimittamiseen osapuolten välillä. Turvapostin viestien hakemisto ei ole henkilötietojen säilytyspaikka, vaan henkilötietoja sisältävät viestit tulee hävittää, kun viesti on toimitettu.

Jos henkilötiedot joudutaan siirtämään esimerkiksi muistitikulle tai hakemistoon, niin ne tulee tallettaa salattuna. Salaukseen voidaan käyttää salasanasuojattua muistitikkua tai ohjelmallista salausta (esimerkiksi bitlocker-ohjelmalla), joihin käyttöopastuksen saa toimialan tietohallinnolta. Henkilötietojen käsittelyn tulee tällöinkin olla aina rekisteriselosteensa mukaista.

Paperitulosteiden käyttöä kannattaa mahdollisuuksien mukaan välttää. Jos tulosteita tarvitaan, henkilötietoja sisältävät aineisto tulee säilyttää siten, että ne eivät voi joutua asiattomien ulottuville. Henkilötietoja sisältävät paperit tuhotaan tietosuojamateriaalina.

Käyttöoikeudet

Kaikkien henkilötietoja sisältävien tietojärjestelmien osalta järjestelmään kirjautumisen edellytyksenä tulisi olla henkilökohtainen käyttöoikeus. Omia tunnuksia ei myöskään saa antaa kenenkään toisen käyttöön. Jokainen on vastuussa kaikista toimenpiteistä, joita on hänen omilla tunnuksillaan tehty.

Käyttöoikeuksien hallinta on olennainen osa tietosuojaa ja -turvaa. Käyttöoikeuksia myönnetään vain niille henkilöille, jotka tarvitsevat niitä työtehtäviensä suorittamiseksi, ja vain siinä

laajuudessa kuin se on työtehtävien vuoksi tarpeen. Suositeltavaa on, että isot tietojärjestelmät suunnitellaan siten, että henkilöt saavat käyttöoikeudet vain niihin tietoryhmiin, jotka ovat työtehtävien vuoksi välttämättömiä.

Mikäli työtehtävät muuttuvat tai henkilö lähtee pois kaupungin palveluksesta, tulee käyttöoikeudet välittömästi poistaa.

Käyttöoikeuksia myönnettäessä tulee käyttäjiltä ottaa sitoumus siitä, että he käyttävät käyttöoikeuksiaan vain työtehtäviin eivätkä käy edes katsomassa sellaisia henkilötietoja, joita eivät työssään tarvitse.

Erityisen tarkka tulee olla myönnettäessä käyttöoikeuksia järjestelmiin, jotka sisältävät salassa pidettäviä tai arkaluonteisia henkilötietoja.

Lokitiedot

Lokitiedoilla tarkoitetaan tässä yhteydessä tietojärjestelmien keräämää 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.

Helsingin kaupungilla tällä hetkellä olevista tietojärjestelmistä vain lähinnä sosiaali- ja terveystoimen tietyt tietojärjestelmät keräävät lokitietoja kattavasti. Uusia tietojärjestelmiä hankittaessa tulee yhtenä järjestelmävaatimuksena olla, että järjestelmä kerää lokitiedot henkilötietojen käsittelystä.

Nykyisten tietojärjestelmien osalta tulee selvittää lokitietojen keräämisen mahdollisuudet. Mitä keskeisemmästä tietojärjestelmästä on kyse ja mitä arkaluonteisempia sen keräämät henkilötiedot ovat, sitä välttämättömämpää lokitietojen kerääminen on.

Kerättyjä lokitietoja voidaan hyödyntää väärinkäytösepäilyjen selvittämisessä, rekisteröityjen pyyntöihin ja tiedusteluihin vastaamisessa sekä tietojärjestelmien käyttäjien toiminnan valvonnassa. Lokitietojen säilytysaika tulisi olla vähintään 5 vuotta.

Koulutus

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

Henkilöstön koulutus on tehtävä 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.

Tietoturvaloukkausten ilmoittaminen

Yksi asetuksen uusista rekisterinpitäjän velvollisuuksista on tietoturvaloukkauksista ilmoittaminen. Rekisterinpitäjän tulee tehdä valvontaviranomaisella ilmoitus henkilötietojen tietoturvaloukkauksesta 72 tunnin sisällä siitä, kun loukkaus on havaittu.

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 median välityksellä, jos henkilökohtaisten ilmoitusten lähettäminen vaatisi kohtuutonta vaivaa.

Ilmoitusten lähettäminen tulee ottaa osaksi Helsingin kaupungin kriisiviestintää.

Jotta ilmoitusvelvollisuus voidaan täyttää, on Helsingin kaupungilla oltava kyvykkyys havaita poikkeamat, selvittää poikkeamien syyt ja seuraukset sekä vaikutukset yksityisyydensuojaan ja eristää poikkeaman leviäminen sekä analysoida, onko tarvetta asetuksen mukaisille ilmoituksille.

Tietojärjestelmien hankinta ja niitä koskevat sopimukset

Uusien tietojärjestelmien hankinta

Rekisterinpitäjä saa käyttää ainoastaan sellaisia henkilötietojen käsittelijöitä, jotka toteuttavat riittävät tekniset ja organisatoriset suojatoimet niin, että henkilötietojen käsittely täyttää tietosuoja-asetuksen vaatimukset ja sillä varmistetaan rekisteröidyn oikeuksien suojelu.

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 sekä
- auttaa rekisterinpitäjää täyttämään niin rekisterinpitäjän velvollisuuden vastata pyyntöihin, jotka koskevat rekisteröityjen oikeuksien käyttämistä, kuin rekisterinpitäjän tietoturvaloukkauksia koskevan ilmoitusvelvollisuuden.

Tämän ohjeen liitteenä on malli rekisterinpitäjän ja käsittelijän väliseen sopimukseen liitettävästä tietoturvallisuusliitteestä, jossa on määritelty henkilötietojen käsittelyn edellytykset. Tietoturvallisuusliite tai sitä vastaavat ehdot on sisällytettävä kaikkiin uusiin henkilötietoja käsittelevien järjestelmien hankintasopimuksiin.

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.

Uusien tietojärjestelmien hankinnassa on lisäksi huomioitava, että rekisteröityjä koskevat tiedot voidaan luovuttaa konekielisessä muodossa silloin, kun siihen on velvollisuus, että tietojärjestelmät keräävät tarvittavia lokitietoja ja että tiedot pystytään poistamaan järjestelmästä joko rekisteröidyn pyynnöstä tai käyttötarkoituksen mukaisen säilytysajan päättyessä.

Vanhojen sopimusten läpikäynti

Voimassaolevat henkilötietoja käsitteleviä tietojärjestelmiä koskevat sopimukset on syytä käydä läpi sen arvioimiseksi, ovatko sopimuksen sisältämät henkilötietojen käsittelyä koskevat ehdot riittäviä takaaman sen, että henkilötietojen käsittely on lainmukaista.

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

Tietosuojavaikutusten arviointi

Tietosuojavaikutusten arviointi on prosessi, jolla toteutetaan rekisterinpitäjän osoitusvelvollisuutta.

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

Tietosuojavaikutusten arviointia tehdessään rekisterinpitäjän on pyydettävä neuvoja tietosuojavastaavalta, joka seuraa tietosuojavaikutusten arvioinnin suorittamista. Käsittelijän on annettava rekisterinpitäjälle arvioinnin suorittamiseksi tarpeelliset tiedot ja avustettava rekisterinpitäjää vaikutusten arvioinnin tekemisessä. Toimialojen, virastojen ja liikelaitosten tietohallinnot ja tietosuojavastuuhenkilöt avustavat arvioinnin suorittamisessa ja voivat myös ehdottaa arvioinnin tekemistä huomatessaan sen tarpeelliseksi.

Tietosuoja-asetuksessa ei ole tyhjentävää listaa tilanteista, joissa tietosuojavaikutusten arviointi on tehtävä. Se on tehtävä kuitenkin erityisesti seuraavissa tapauksissa:

a) luonnollisten henkilöiden henkilökohtaisten ominaisuuksien järjestelmällinen ja laajamittainen arviointi, joka perustuu henkilötietojen automaattiseen käsittelyyn (kuten profilointiin), jos sillä on henkilölle oikeudellisia tai muuten merkittäviä vaikutuksia

b) laajamittainen käsittely, joka kohdistuu tietosuoja-asetuksen mukaisiin erityisiin henkilötietoryhmiin tai rikostuomioita tai rikkomuksia koskeviin tietoihin; tai

c) yleisölle avoimen alueen laajamittainen järjestelmällinen valvonta

Arvioitaessa sitä, aiheuttaako käsittely todennäköisesti korkean riskin ihmisten oikeuksille ja vapauksille, tulisi arvioida seuraavia kriteereitä:

1. Arviointi ja pisteytys (profilointi). Tästä on kyse esimerkiksi, kun kerätään tietoa henkilöiden liikkeistä, käyttäytymisestä tai terveystiedoista ja verrataan sitä olemassa olevaan tietoon.

2. Automaattinen päätöksenteko silloin, kun sillä on henkilöön oikeudellisia tai muuten merkittäviä vaikutuksia.

3. Järjestelmällinen seuranta. Käsittely, jolla henkilöä tarkkaillaan, havainnoidaan tai kontrolloidaan, mukaan lukien julkisen paikan systemaattinen tarkkailu.

4. Arkaluonteinen tieto. Arkaluonteisella tiedolla tarkoitetaan tietosuoja-asetuksen mukaisia erityisiä henkilötietoryhmiä koskevaa käsittelyä, kuten poliittisia mielipiteitä ja henkilötietoja, jotka liittyvät tehtyihin rikoksiin ja niistä saatuihin tuomioihin.

5. Laajamittainen henkilötietojen käsittely

6. Henkilötietojen yhdistäminen useasta eri lähteestä

7. Haavoittuvaisia henkilöitä koskevan tiedon käsittely

8. Innovatiivisten uusien teknologisten ja organisatoristen ratkaisujen käyttö

9. Henkilötietojen siirto EU:n alueen ulkopuolelle

10. Käsittely, joka voi estää rekisteröityä käyttämästä oikeuksiaan tai saamasta palvelua tai sopimusta

Mitä useampi kriteeri täyttyy, sitä todennäköisemmin kysymys on korkean riskin aiheuttavasta käsittelystä. Nyrkkisääntönä voidaan pitää, että kahden kriteerin täyttyessä on todennäköisesti kysymys korkean riskin aiheuttavasta käsittelystä. Asiaa on arvioitava tapauskohtaisesti ja joskus jopa yhden kriteerin täyttyminen voi aiheuttaa korkean riskin.

Tietosuojavaikutusten arviointia ei tarvita, jos käsittelyn luonne, laajuus, konteksti ja tarkoitus on hyvin samanlainen kuin aiemmalla prosessilla, jonka osalta vaikutusten arviointi on suoritettu. Arviointia ei myöskään tarvitse suorittaa silloin, kun käsittely perustuu lakiin ja vaikutukset on arvioitu osana lainsäädäntöprosessia. Tietosuojaviranomainen voi myös määritellä käsittelyn tietosuojavaikutusten arvioinnin vapaaehtoiseksi.

Tietosuojavaikutusten arviointia on tehtävä jatkuvasti, mutta uudelleenarviointi tulisi tehdä vähintään kolmen vuoden välein.

Velvollisuus tietosuojavaikutusten arviointiin koskee käsittelyprosesseja, jotka aloitetaan 25.5.2018 tai sen jälkeen. Suositus kuitenkin on, että uusille käsittelyprosesseille tietosuojavaikutusten arviointi tehdään jo ennen kevättä 2018. Myös olennainen muutos käsittelyssä voi vaatia tietosuojavaikutusten arvioinnin tekemistä jo olemassa olevalle prosessille, erityisesti jo muutos vaikuttaa käsittelyn riskiin. Arviointi on suoritettava ennen prosessin käyttöönottoa. Jos arvioidut riskit ovat korkeat, eikä niitä saada hyväksyttävälle tasolle, on rekisterinpitäjällä velvollisuus konsultoida tietosuojaviranomaista. Konsultoinnin yhteydessä tietosuojaviranomaiselle on toimitettava tietosuojavaikutusten arviointi kokonaisuudessaan.

Tietosuojavaikutusten arviointi voidaan tehdä monella eri tavalla ja sillä pyritään varmistamaan henkilötietojen käsittelyn yhdenmukaisuus tietosuoja-asetuksen vaatimusten kanssa. Prosessin laiminlyöminen voi johtaa tietosuoja-asetuksen mukaisiin hallinnollisiin sanktioihin.

Tietosuoja-asioiden vastuunjako helsingin kaupungin organisaatiossa

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

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.

Helsingin kaupungin tietosuojavastaava on kaupunginhallituksen virkaan ottama viranhaltija. Hallinnollisesti tietosuojavastaava sijoittuu kaupunginkanslian hallinto-osastolle hallintojohtajan suoraan alaisuuteen. Tietosuojavastaava raportoi suoraan kaupungin ylimmälle johdolle eikä hänelle saa antaa ohjeita siitä, kuinka hän suorittaa tehtävänsä. Tietosuojavastaavan asema ja tehtävät määräytyvät tietosuoja-asetuksen 38 ja 39 artiklan nojalla.

Rekisterinpitäjän on tuettava tietosuojavastaavaa antamalle tälle resurssit, jotka ovat tarpeen tämän tehtävien täyttämisessä, samoin kuin pääsyn henkilötietoihin ja käsittelytoimiin. Tietosuojavastaavan riippumattoman toiminnan turvaamiseksi kaupunginkanslian hallinto-osastolla on oltava tietosuojavastaavan alaisuudessa häntä avustavaa henkilökuntaa, joista yhden on oltava kelpoinen toimimaan tietosuojavastaavan sijaisena.

Kuhunkin toimialaan, virastoon ja liikelaitokseen on nimettävä tietosuoja-asioiden vastuuhenkilö, joka toimii yhteyshenkilönä kyseisen organisaation ja tietosuojavastaavan välillä, opastaa ja neuvoo omaa organisaatiotaan tietosuoja-asioissa, osallistuu oman organisaationsa

tietosuojavaikutusten arviointiin sekä uusien tietojärjestelmien hankintoihin, mikäli tietojärjestelmät käsittelevät henkilötietoja.

On suositeltavaa, että tietosuoja-asioiden vastuuhenkilö on koulutukseltaan lakimies. Mikäli tämä ei ole mahdollista, tulisi vastuuhenkilön olla hallinnon asiantuntijatehtävissä toimiva. Lisäksi jokaisen henkilörekisterin osalta tulee olla nimetty vastuuhenkilö, joka omalta osaltaan vastaa kyseisen rekisterin tietosuojasta ja rekisteriselosteen lainmukaisuudesta. Vastuuhenkilöiden lisäksi toimialoilla, virastoilla ja liikelaitoksilla on oltava riittävästi avustavaa henkilökuntaa, joka osallistuu erityisesti rekisteröityjen tekemiin tiedusteluihin vastaamiseen.

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

Kaikkien tietosuoja- ja tietoturva-asioissa vastuuta kantavien henkilöiden osalta on huolehdittava, että sijaistusjärjestelyt ovat riittävät.

Lisätietoja

Mikäli et ole varma, kuinka käsittelet henkilötietoja oikein, niin selvitä asia asianomaisiin henkilötietoihin liittyvässä rekisteriselosteessa mainituilta yhdyshenkilöiltä, toimialasi tietosuojavastuuhenkilöltä, kaupunginkanslian oikeuspalveluista tai tietosuojavastaavalta.

Tietoturvaan liittyvissä kysymyksissä voit kysyä neuvoa toimialasi tietoturvan asiantuntijoilta.

Sopimuksiin ja hankintoihin liittyvissä kysymyksissä voit kääntyä kaupunginkanslian oikeuspalveluiden sopimukset ja hankinnat –yksikön puoleen.

Helmi>Yhteiset palvelut>Tietosuoja (http://helmi.hel.fi/yhteisetpalvelut/tietosuoja)

Helmi>Yhteiset palvelut>Tietoturva (http://helmi.hel.fi/yhteisetpalvelut/tietoturva)

Liite Tietoturvallisuusliite tietojärjestelmien hankintasopimuksiin