Porvoon kaupungin henkilötietojen käsittelyohje

Tietoturvatyöryhmä, 24.1.2018

Sisältö

1 Henkilötietojen käsittelyn periaatteet 2
1.1 Käsitteet 2
1.2 Henkilötietojen käsittelyn vaatimukset 3
2 Henkilötietojen käsittely 3
2.1 Yleiset määräykset ja käsittelijän velvollisuudet 3
2.2 Ohjeet henkilötietojen käsittelijälle 4
2.3 Erityisten henkilötietojen käsittely 4
3 Muut käsittelyä koskevat määräykset 5
3.1 Tietoturva 5
3.2 Käyttöoikeudet 6
3.3 Lokitiedot 6
3.4 Tietoturvaloukkausten ilmoittaminen 6

1 Henkilötietojen käsittelyn periaatteet

Ohje koskee kaupungin omaa henkilökuntaa, sopimuskumppaneita sekä kaikkia muita, jotka käsittelevät Porvoon kaupungin hallussa olevia tai sen keräämiä henkilötietoja. Ohje jaetaan yllämainituille tahoille.

Porvoon kaupunki toteuttaa toiminnassaan kahta osittain vastakkaista perusoikeutta eli hallinnon julkisuutta ja yksityisyydensuojaa. Kaupunki sovittaa toiminnassaan yhteen lainsäädännössä säädetyllä tavalla yksityishenkilöiden yksityisyyden suojan ja hallinnon toiminnan avoimuuden ja julkisuuden:

- Porvoon 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 asian käsittelyn vuoksi tarpeen. Poikkeuksellisesti henkilötietoja voidaan säilyttää pidempiä aikoja, jos henkilötietoja käsitellään yleisen edun mukaista arkistointia, historiallista tutkimusta tai tilastointia varten.

Arkiston- ja tiedonohjaussuunnitelmissa määritellään arkistoitavat tiedot ja niiden säilytysajat. Arkistoitavia tietoja on käsiteltävä ja säilytettävä siten, että rekisteröityjen henkilöiden yksityisyyden suoja voidaan turvata.

Kaupungin keskeisimmät tietoturvallisuuteen ja tietosuojaan liittyvät toimijat ja roolit vastuineen on määritelty kaupungin tietoturvapolitiikassa ja tietosuojapolitiikassa.

1.1 Käsitteet

Henkilötiedolla tarkoitetaan kaikkea tunnistettuun tai tunnistettavissa olevaan henkilöön liittyviä tietoja. Tunnistettavissa olevana pidetään henkilöä, joka voidaan tunnistaa suoraan tai epäsuorasti erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen (esim. ip-osoite) tai henkilölle tunnusomaisten fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella. Henkilötietoja voivat olla muun muassa osoite, sähköpostiosoite, valokuva, ääni- tai videotallenne, auton rekisterinumero, kiinteistötunnus, sormenjälki tai muu biologinen näyte.

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.

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

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

1.2 Henkilötietojen käsittelyn vaatimukset

- Henkilötietoja on käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi: **lainmukaisuus, kohtuullisuus ja läpinäkyvyys**.
- Henkilötietoja on kerättävä tiettyä, nimenomaista ja laillista tarkoitusta varten, eikä niitä saa käsitellä myöhemmin näiden tarkoitusten kanssa yhteensopimattomalla tavalla: **käyttötarkoitussidonnaisuus**.
- Henkilötietojen on oltava asianmukaisia ja olennaisia ja rajoitettuja siihen, mikä on tarpeellista suhteessa niihin tarkoituksiin, joita varten niitä käsitellään: **tietojen minimointi**.
- Henkilötietojen on oltava täsmällisiä ja tarvittaessa päivitettyjä. On toteutettava kaikki mahdolliset kohtuulliset toimenpiteet sen varmistamiseksi, että käsittelyn tarkoituksiin nähden epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä: **täsmällisyysvaatimus**.
- Ne on säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan, kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten: **säilytyksen rajoittaminen**.
- Niitä on käsiteltävä tavalla, jolla varmistetaan henkilötietojen asianmukainen turvallisuus. Tiedot on suojattava luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta**: eheys ja luottamuksellisuus**.

Tietosuoja-asetuksen mukaan rekisterinpitäjä vastaa siitä, että edellä lueteltuja periaatteita noudatetaan. Sen on myös pystyttävä osoittamaan, että näitä periaatteita noudatetaan.

2 Henkilötietojen käsittely

Kun rekisterinpitäjänä toimiva Porvoon kaupunki ulkoistaa erilaisia henkilötietojen käsittelytehtäviä palveluntarjoajille (sopimustoimittajille), palveluntarjoajat ovat lähtökohtaisesti rekisterinpitäjän lukuun henkilötietoja käsitteleviä tahoja. Jos palveluntarjoajalla ei ole itsenäistä päätösvaltaa henkilötietojen säilytyksen ja käyttämisen suhteen, palveluntarjoaja toimii rekisterinpitäjän lukuun henkilötietojen käsittelijänä. Rekisterinpitäjän ja henkilötietojen käsittelijän välillä on oltava kirjallinen sopimus, kun kyse on edellä mainitun laisesta tilanteesta.

Rekisterinpitäjän ja henkilötietojen käsittelijän on sovittava kirjallisesti henkilötietojen käsittelyn kohde ja tarkoitus. Sopimuksessa on myös määriteltävä, kenellä on pääsy henkilötietoihin.

Tietosuoja-asetuksen mukaan sopimuksessa tulee määritellä henkilötietojen käsittelyn **kohde, tarkoitus ja kesto. Lisäksi on sovittava, mitä henkilötietoja käsitellään.**

2.1 Yleiset määräykset ja käsittelijän velvollisuudet

Henkilötietoja saa muun muassa käsitellä, jos

- siihen on rekisteröidyn suostumus,
- käsittely on tarpeen kaupungin lakisääteisten velvoitteiden noudattamiseksi tai julkisen vallan käyttämiseksi,
- rekisteröity henkilö 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.

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

Mikäli Porvoon 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 tällä hetkellä ole.

2.2 Ohjeet henkilötietojen käsittelijälle

Käsittele henkilötietoja ainoastaan tämän ohjeen mukaisesti. Noudata ohjeita myös, kun siirrät, säilytät ja arkistoit henkilötietoja.

Henkilötietojen käsittelijän on noudatettava seuraavia ohjeita:

1. Noudata salassapitovelvollisuutta.

2. Noudata tietoturvallisuutta.

3. Älä ulkoista henkilötietojen käsittelyn tehtäviä ilman rekisterinpitäjän kirjallista ennakkosuostumusta.

4. Käsittelijä auttaa rekisterinpitäjää (Porvoon kaupunkia) rekisteröidyn oikeuksien toteuttamisessa ilman erillistä korvausta.

5. Käsittelijä auttaa rekisterinpitäjää käsittelyn tietoturvallisuuden toteuttamisessa, henkilötietojen tietoturvaloukkausten havaitsemisessa ja niistä ilmoittamisessa sekä vahinkojen minimoinnissa, vaikutustenarviointien tekemisessä ja valvontaviranomaisen ennakkokuulemisessa.

6. Käsittelijä joko poistaa tai palauttaa henkilötiedot rekisterinpitäjälle käsittelypalvelujen päättyessä. Käsittelijän tulee myös poistaa niistä hallussaan olevat kopiot.

7. Käsittelijä sallii rekisterinpitäjän suorittaa auditoinnit ja osallistuu niihin itse. Käsittelijän tulee myös luovuttaa ilman erillistä korvausta rekisterinpitäjälle kaikki sellaiset tiedot, joilla voidaan osoittaa, että asetuksen velvollisuuksia on noudatettu.

2.3 Erityisten henkilötietojen käsittely

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 henkilön seksuaalista käyttäytymistä ja suuntautumista koskevat tiedot.

Mikäli erityisiin henkilötietoryhmiin kuuluvia tietoja aiotaan käsitellä, on huolellisesti selvitettävä, että tietojen käsittely on tietosuoja-asetuksen yhdeksännen 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
- 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.

Rikosrekisteriotteiden käsittelystä on säädetty erityislainsäädännössä, esimerkiksi laki lasten kanssa työskentelevien rikostaustan selvittämisestä, laki julkisista hankinnoista ja käyttöoikeussopimuksista.

3 Muut käsittelyä koskevat määräykset

3.1 Tietoturva

Henkilötietojen käsittelijän on aina huolehdittava, etteivät henkilötiedot joudu asiattomien saataville riippumatta siitä, käsitelläänkö tietoja tietojärjestelmissä, paperilla, kuvina, keskustelemalla puhelimessa tai kasvokkain.

Henkilötietoja käsitellessä on varmistettava, että paikka soveltuu henkilötietojen käsittelyyn. Ulkopuoliset eivät saa 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 käsittelyistä eikä käyttötunnuksia saa antaa muiden käyttöön.

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

Turvapostia voidaan käyttää henkilötietojen lähettämiseen 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, ne on talletettava salattuna. Salaukseen voidaan käyttää salasanasuojattua muistitikkua tai ohjelmallista salausta esimerkiksi BitLocker-ohjelmalla. Henkilötietojen käsittelyn tulee tällöinkin olla aina rekisteriselosteensa mukaista.

Paperitulosteiden käyttöä kannattaa mahdollisuuksien mukaan välttää. Jos tulosteita tarvitaan, henkilötietoja sisältävät aineisto on säilytettävä siten, että se ei voi joutua asiattomien ulottuville. Erityistä huomiota tulee kiinnittää postittaessa asiakirjoja. Myös tietojen siirtämisessä tilasta toiseen tulee kiinnittää erityistä huolellisuutta. Henkilötietoja sisältävät paperit tuhotaan tietosuojamateriaalina.

3.2 Käyttöoikeudet

Kaikkiin henkilötietoja sisältäviin tietojärjestelmiin kirjaudutaan henkilökohtaisella tunnuksella. Omia tunnuksia ei saa antaa kenenkään toisen käyttöön. Lähtökohtaisesti jokaisella työntekijällä (tai kumppanin edustajalla) on henkilökohtainen tunnus ja jokaisella käyttäjätunnuksella on vain yksi käyttäjä. Käyttäjä vastaa kaikista toimenpiteistä, joita hänen tunnuksillaan tehdään tai on 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.

Mikäli työtehtävät muuttuvat tai henkilö lähtee pois kaupungin/sopimuskumppanin palveluksesta, on käyttöoikeudet välittömästi poistettava, ellei niiden säilyttämiselle ole perustetta.

Kun käyttöoikeuksia myönnetään, on käyttäjien sitouduttava siihen, että he käyttävät käyttöoikeuksiaan vain työtehtäviin eivätkä käy katsomassa sellaisia henkilötietoja, joita eivät työssään tarvitse.

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

3.3 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.

3.4 Tietoturvaloukkausten ilmoittaminen

Henkilötietojen käsittelijän on ilmoitettava henkilötietoja koskevasta loukkauksesta osoitteeseen tietosuojavastaava@porvoo.fi. Loukkaus voi olla esimerkiksi tietojen muuttuminen, tuhoutuminen tai vuotaminen sivullisille. Tiedot voivat olla esimerkiksi sähköisessä tai paperisessa muodossa. Tapahtumasta on ilmoitettava välittömästi kun se havaitaan.

Ilmoituksen tulee sisältää vähintään seuraavat kohdat:

- kuvaus, mitä on tapahtunut,
- mikäli mahdollista, niiden rekisteröityjen henkilöiden ryhmät ja lukumäärät, joita loukkaus on koskenut,
- millaisia vaikutuksia henkilötietojen tietoturvaloukkauksella voi todennäköisesti olla.

Jotta ilmoitusvelvollisuus voidaan täyttää, on henkilötietojen käsittelijällä oltava kyvykkyys havaita poikkeamat, selvittää poikkeamien syyt ja seuraukset sekä vaikutukset yksityisyydensuojaan.

3.5 Henkilötietolainsäädännön noudattaminen

Näiden käsittelyohjeiden lisäksi henkilötietojen käsittelijän tulee toiminnassaan noudattaa voimassaolevaa lainsäädäntöä koskien henkilötietoja. Siltä osin kuin nämä ohjeet ovat ristiriidassa lainsäädännön kanssa, noudatetaan lainsäädännön vaatimuksia. Ohjeet päivitetään mikäli lainsäädäntö tai kansallinen ohjeistus sitä vaatii ja muutenkin tarvittaessa. Porvoon kaupungin tietosuojaryhmä huolehtii päivittämisestä.