Tietosuojakäsikirja

Sisällys

1. Johdanto – Tietosuoja on jokaisen oikeus 4
2. Tietosuoja-asioiden vastuunjako Helsingin kaupungilla 6
3. Käsitteiden määritelmiä 8
4. Henkilötietojen käsittelyä koskevat periaatteet 12
   - 4.1 Periaatteet ohjaavat henkilötietojen käsittelyä 12
   - 4.2 Sisäänrakennettu ja oletusarvoinen tietosuoja 13
5. Henkilötietojen käsittelyn perusteet 14
   - 5.1 Henkilötietojen käsittelyn on perustuttava lakiin 14
   - 5.2 Henkilötietojen käsittely muuhun kuin alkuperäiseen käsittelytarkoitukseen 16
   - 5.3 Henkilötunnuksen käsittely 17
   - 5.4 Turvakiellon alaisen osoitteen käsittely 17
6. Erityisiä henkilötietoryhmiä koskeva käsittely 18
   - 6.1 Erityisiä henkilötietoryhmiä koskeva käsittelykielto 19
   - 6.2 Tietosuoja-asetuksen mukainen poikkeus käsittelykiellosta 20
   - 6.3 Tietosuojalain mukainen poikkeus käsittelykiellosta 21
7. Rikostuomioihin ja rikkomuksiin liittyvien henkilötietojen käsittely 24
8. Rekisterinpitäjän velvollisuudet 26
   - 8.1 Rekisteröidyn informointi 26
   - 8.2 Rekisteriselosteet 27
   - 8.3 Seloste käsittelytoimista 27
   - 8.4 Tarvittavat tekniset ja organisatoriset toimenpiteet tietojen suojaamiseksi 27
   - 8.5 Osoitusvelvollisuus 28
   - 8.6 Käsittelijän toiminnan valvominen 29
9. Kaupunki henkilötietojen käsittelijänä 30
10. Rekisteröidyn oikeudet 32
11. Tietoturva 38
   - 11.1 Helsingin tietoturvan ohjeet toimittajalle 39
   - 11.2 Tietoturvaan liittyvät tehtävät ja tietoturvajärjestelyt 40
   - 11.3 Oman työn tietoturvallisuus 42
12. Tietopyyntöjen käsittely 43
   - 12.1 Henkilötietojen pyytäminen ja oikaisuvaatimus 44
   - 12.2 Tietopyyntöjen käsittelyn sähköinen prosessi 44
   - 12.3 Tietopyyntöjen käsittelyn paperiprosessi 44
   - 12.4 Tietojen luovutus ja korjaaminen sekä niistä kieltäytyminen 45

Tietosuojakäsikirja

13. Tietoturvaloukkauksista ilmoittaminen 46
13.1 Henkilötietojen tietoturvaloukkaus 47
13.2 Tietoturvaloukkauksesta ilmoittamisen prosessi 47
13.3 Tietoturvaloukkauksesta ilmoittaminen tietosuojavaltuutetulle 48
13.4 Henkilötietojen tietoturvaloukkauksesta ilmoittaminen rekisteröidylle 48

14. Tietosuojaa koskeva vaikutustenarviointi 49
14.1 Mikä on vaikutustenarviointi ja mitä se sisältää? 49
14.2 Milloin vaikutustenarviointi on tehtävä? 50
14.3 Menettely jo käytössä olevien käsittelytoimien osalta 51
14.4 Vaikutustenarvioinnin tekemisen vastuut 51
14.5 Tietosuojavaltuutetun ennakkokuuleminen korkean jäännösriskin tapauksessa 52
14.6 Helsingin kaupungin vaikutustenarvioinnin työkalut 52
14.6.1 Alkukartoitus 52
14.6.2 Vaikutustenarvioinnin työkalu 52
14.6.3 Vaikutustenarvioinnin riskianalyysi 53
14.6.4 Tietosuojan tarkistuslista 53
14.6.5 Vaikutustenarvioinnin loppuraportti 53

15. Tietosuojalain-säädännön rikkomisen seuraamukset 54
15.1 Oikeus saattaa asia tietosuojavaltuutetun käsiteltäväksi 55
15.2 Oikeus nostaa kanne rekisterinpitäjää tai henkilötietojen käsittelijää vastaan 55
15.3 Oikeus korvauksen saamiseen 55
15.4 Rikosoikeudelliset seuraamukset 56

16. Sopimukset ja hankinnat 57
16.1 Tietosuoja-asetuksen vaikutus sopimusehtoihin 58
16.2 Henkilötietojen käsittely EU/ETA-alueen ulkopuolella 59
16.2.1 Käsittely Euroopan komission hyväksymissä maissa 59
16.2.2 Korkeariskiset henkilötiedot 60
16.2.3 Vähäriskiset henkilötiedot lakisääteisessä toiminnassa 60
16.2.4 Vähäriskiset henkilötiedot muussa kuin lakisääteisessä toiminnassa 60
16.2.5 Lisäedellytykset henkilötietojen käsittelylle 60
16.2.6 EU/ETA-alueen ulkopuolisen henkilötietojen käsittelyn huomioiminen tietosuoja- ja salassapitoliitteessä 61
16.3 Muut tietosuojasopimukset 61
16.3.1 Yhteisrekisterinpitäjien välinen sopimus 61
16.3.2 Tietojen luovuttaminen toiselle rekisterinpitäjälle 61

17. Julkisuuslain ja tietosuoja-asetuksen suhde 62

18. Henkilötietojen suoja päätösvalmistelussa 64
18.1 Henkilötietojen käsittely pöytäkirjassa 65
18.2 Kunnallinen tiedotusintressi 66

1. Johdanto – Tietosuoja on jokaisen oikeus

Tietosuojalla tarkoitetaan henkilötietojen suojaamista. Henkilötietoja ovat tiedot, joiden perusteella henkilö voidaan tunnistaa joko suoraan tai välillisesti yhdistämällä yksittäinen tieto johonkin muuhun tietoon. Jokaisella on oikeus henkilötietojensa suojaan.

EU:n yleistä tietosuoja-asetusta (EU) 2016/679 (*General Data Protection Regulation, GDPR*) alettiin soveltaa 25.5.2018. Asetus on suoraan sovellettavaa lainsäädäntöä. Tietosuoja-asetuksen tavoitteena on parantaa henkilötietojen suojaa, lisätä henkilötietojen käsittelyn läpinäkyvyyttä rekisteröidyille, eli henkilöille, joiden tietoja käsitellään, sekä antaa heille enemmän keinoja hallita henkilötietojensa käsittelyä. Tietosuojan merkitys kasvaa digitalisoituvassa maailmassa. Tietosuoja-asetus pyrkiikin vastaamaan digitalisaation ja globalisaation mukanaan tuomiin tietosuojakysymyksiin.

Tietosuojalaki (1050/2018) tuli voimaan 1.1.2019. Se on henkilötietojen käsittelyyn sovellettava yleislaki, ja siinä on täydennetty ja täsmennetty tietosuoja-asetuksen määräyksiä. Lisäksi monet lait, esimerkiksi laki viranomaisten toiminnan julkisuudesta (621/1999, julkisuuslaki) ja erityislainsäädäntö, ohjaavat sitä, miten henkilötietoja on käsiteltävä.

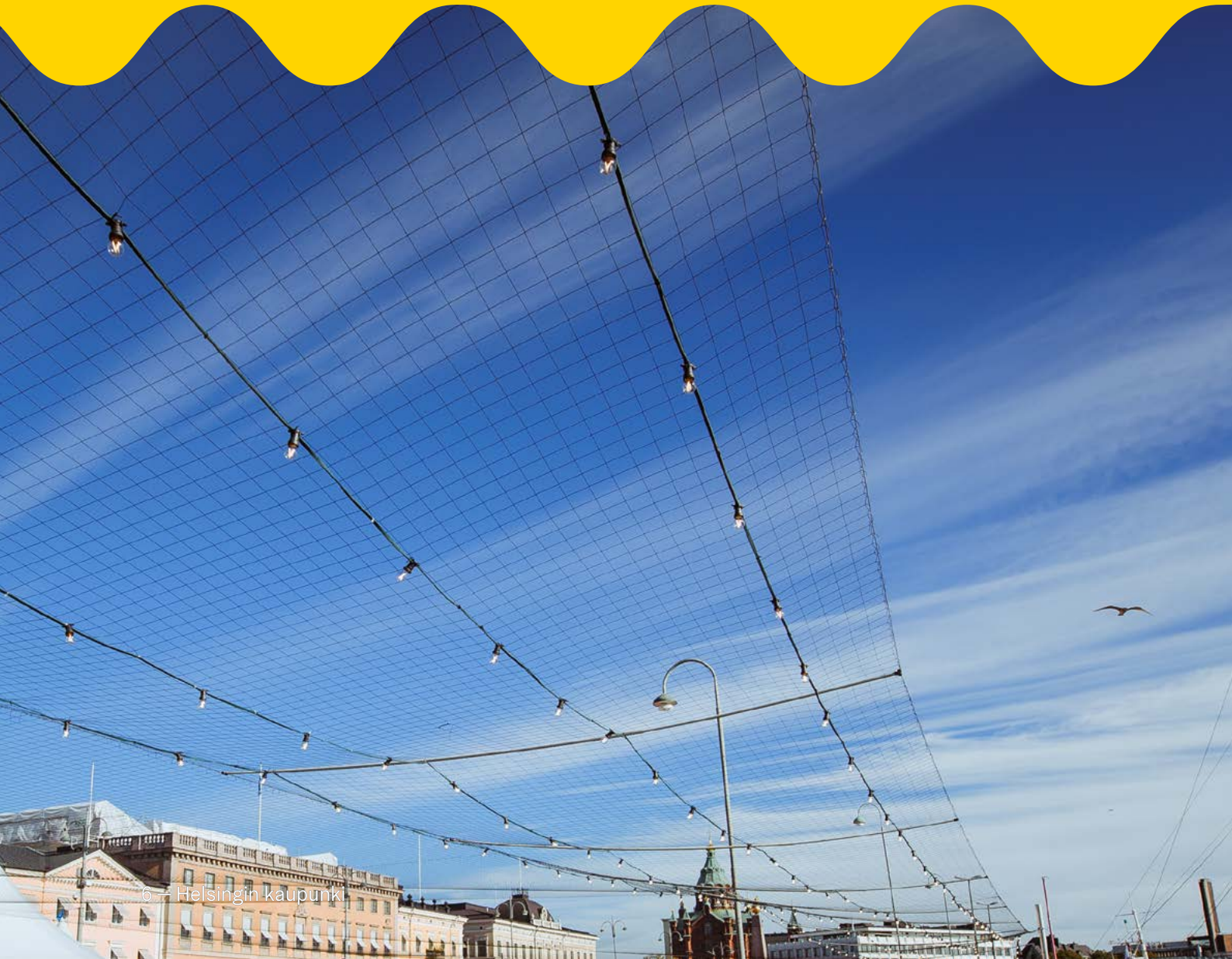
Helsingin kaupungilla on tietosuojalinjaukset (khs 29.4.2019, § 287), jotka sisältävät ohjeita siitä, miten tietosuojalainsäädännön mukaiset velvoitteet täytetään kaupungin toiminnassa.

Tietosuojalainsäädännöllä on merkittäviä vaikutuksia kuntiin rekisterinpitäjinä ja henkilötietojen käsittelijöinä. Rekisterinpitäjyys tarkoittaa sitä, että kunta itse määrittelee, mihin tarkoitukseen ja millä tavalla se käsittelee henkilötietoja. Henkilötietojen käsittelijänä kunta sen sijaan käsittelee henkilötietoja toisen rekisterinpitäjän puolesta. Tämä käsikirja on kirjoitettu siitä lähtökohdasta, että rekisterinpitäjänä toimii Helsingin kaupunki.

Tietosuojakäsikirjassa kerrotaan perustietoa tietosuojalainsäädännöstä sekä ohjeistetaan siitä, miten tietosuojalainsäädännön velvoittamia toimenpiteitä toteutetaan Helsingin kaupungilla. Käsikirja on tarkoitettu yleiseksi ohjeistukseksi kaikille henkilötietoja työssään käsitteleville, joita onkin suurin osa kaupungin työntekijöistä.

2. Tietosuoja-asioiden vastuunjako Helsingin kaupungilla

Hallintosäännön mukaisesti kaupunginhallitus vastaa siitä, että kaupunki täyttää tietosuojalainsäädännön velvoitteet ja valvoo niiden toteutumista. Toimialojen, virastojen ja liikelaitosten johdolla puolestaan on vastuu toiminnan lainmukaisuudesta henkilötietojen käsittelyssä.



Tietosuojavastaava ja tietosuojatiimi

Tietosuoja-asetus velvoittaa kaikkia julkishallintoon kuuluvia organisaatioita nimittämään tietosuojavastaavan. Tietosuojavastaavan tehtäviin kuuluu organisaation neuvonta ja ohjaus kaikissa tietosuojakysymyksissä, tietosuoja-asetuksen noudattamisen valvonta mukaan lukien tähän liittyvät tarkastukset, yhteistyö valvontaviranomaisen kanssa ja rekisteröityjen oikeuksien toteuttamisen tukeminen.

Helsingin kaupungin tietosuojavastaavan ottaa virkaan kaupunginhallitus. Hallinnollisesti tietosuojavastaava sijoittuu kaupunginkanslian hallinto-osastolle. Tietosuojavastaavan asema ja tehtävät määräytyvät suoraan EU:n tietosuoja-asetuksen 38 ja 39 artiklan nojalla.

Tietosuojavastaava raportoi suoraan kaupungin ylimmälle johdolle, ja hänen asemansa kaupunkiorganisaatiossa on autonominen ja riippumaton.

Tietosuojavastaavalla on apunaan tietosuojatiimi. Siihen kuuluvat apulaistietosuojavastaava, joka avustaa tietosuojavastaavaa tämän tehtävissä ja toimii tietosuojavastaavan sijaisena, sekä kaksi tietosuojan asiantuntijaa.

Tietosuojan vastuuhenkilö

Kuhunkin toimialaan, virastoon ja liikelaitokseen on nimetty tietosuojan vastuuhenkilö, joka toimii yhteyshenkilönä oman organisaationsa ja tietosuojavastaavan välillä, opastaa ja neuvoo omaa organisaatiotaan tietosuoja-asioissa, huolehtii rekisteriselosteiden laatimisesta, osallistuu organisaationsa tietosuojan vaikutustenarviointeihin 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 henkilö.

Rekisterin vastuuhenkilö

Kaupunki kerää henkilötietoja henkilörekistereihin tietojen käyttötarkoitusten mukaan. Jokaiselle henkilörekisterille on nimetty vastuuhenkilö, joka omalta osaltaan vastaa kyseisen rekisterin tietosuojasta ja rekisteriselosteen lainmukaisuudesta. Rekisterin vastuuhenkilö on vastuussa rekisteröityjen tietopyyntöihin vastaamisesta sekä rekisteröityjen tiedon korjaamisvaatimusten ja muiden rekisteröityjen oikeuksien toteuttamisesta. Vastuuhenkilöiden lisäksi toimialoilla, virastoilla ja liikelaitoksilla on oltava riittävästi avustavaa henkilöstöä, joka osallistuu erityisesti rekisteröityjen tekemiin tiedusteluihin vastaamiseen.

Rekisterin yhteyshenkilö

Rekisteriselosteessa on nimetty rekisterikohtainen yhteyshenkilö, joka ottaa vastaan tietopyynnöt ja tiedon korjaamisvaatimukset. Hän hakee tarvittavat tiedot rekisteristä ja toimittaa ne rekisterin vastuuhenkilölle.

Tietoturvan vastuuhenkilö

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.

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

Tietosuojatyöryhmä

Kaupungilla on kansliapäällikön asettama tietosuojatyöryhmä, jonka tehtävänä on valmistella kaupungin tietosuojaa koskevaa ohjeistusta ja sisäisiä menettelyjä tietosuojan toteuttamiseksi sekä sen osoittamiseksi, että tietosuoja toteutuu kaupungin toiminnassa. Työryhmän tehtävänä on myös koordinoida kaupungin tietosuojakäytäntöjen yhtenäisyyttä, huolehtia siitä, että kaupungin henkilökunnalle järjestetään riittävästi koulutusta tietosuoja-asioissa sekä ohjeistaa, seurata ja kehittää tietosuojatyötä kaupungilla.

EU:n yleinen tietosuoja-asetus (EU) 2016/679: 37 art., 38 art., 39 art.

3. Käsitteiden määritelmiä

- Anonymisointi ja pseudonymisointi
- Henkilötieto
- Henkilötietojen käsittely
- Käsittelijä
- Rekisteri/henkilörekisteri
- Rekisteriseloste
- Rekisterinpitäjä
- Rekisterin vastuuhenkilö
- Rekisterin yhteyshenkilö
- Rekisteröity
- Seloste käsittelytoimista
- Tietopyyntöjen kokoaja
- Tietosuojavaltuutettu
- Tietosuojavastava
- Tietoturva
- Turvakielto
- Vaikutustenarviointi

Anonymisointi ja pseudonymisointi

Anonymisointi tarkoittaa henkilötietojen käsittelemistä siten, että henkilötietoja ei voida enää yhdistää tiettyyn rekisteröityyn edes käyttämällä lisätietoja. Anonymisoitua tietoa käytetään esimerkiksi tilastotarkoituksissa. Anonymisoidun tiedon käsittely ei ole henkilötietojen käsittelyä eikä se ole tietosuoja-asetuksen soveltamisalan piirissä.

Pseudonymisointi tarkoittaa henkilötietojen käsittelemistä siten, että henkilötietoja ei voida enää yhdistää tiettyyn rekisteröityyn ilman lisätietoja. Lisätiedot säilytetään erillään henkilötiedoista ja varmistetaan, ettei henkilötietojen yhdistämistä tunnistettuun tai tunnistettavissa olevaan henkilöön tapahdu. Pseudonymisoidut tiedot ovat henkilötietoja ja tietosuoja-asetusta sovelletaan niiden käsittelyyn.

Henkilötieto

Henkilötiedolla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja.

Tunnistettavana pidetään sellaista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen tai 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 henkilöön yhdistämällä tiedot muualta saatavaan tietoon.

Henkilötiedolla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja.

Henkilötietojen käsittely

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

Henkilötietojen käsittelyn osalta on hyvä muistaa, että jo pelkkä henkilötietojen katsominen on henkilötietojen käsittelyä, vaikka tietoja ei muutettaisi mitenkään. Kenenkään ei tule käsitellä toisen henkilön henkilötietoja ilman perustetta.

Käsittelijä

Henkilötietojen käsittelijä on ihminen tai organisaatio, joka käsittelee henkilötietoja rekisterinpitäjän lukuun.

Helsingin kaupunki on yleensä itse rekisterinpitäjä, mutta on niitäkin tilanteita, joissa Helsingin kaupunki ainoastaan käsittelee jonkin toisen tahon rekisterin tietoja rekisterinpitäjän puolesta. Jos useammalla kunnalla on käytössä yhteinen rekisteri, voi olla niin, että kunnat ovat kaikki yhdessä rekisterinpitäjiä tai että yksi kunta toimii rekisterinpitäjänä ja muut kunnat ovat ainoastaan käsittelijöitä.

Rekisteri/henkilörekisteri

Kaupunki kerää henkilötietoja eri rekistereihin tietojen käyttötarkoitusten mukaan. Rekisterissä olevat tiedot siis 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 henkilötiedoista.

Yhden rekisterin tietoja voi olla useassa tietojärjestelmässä ja yhdessä tietojärjestelmässä voi olla usean rekisterin tietoja.

Rekisteriseloste

Rekistereistä laaditaan rekisteriselosteet, joista ilmenee kunkin rekisterin tietojen käsittelyn tarkoitukset ja tietosisältö sekä muuta tarpeellista tietoa, kuten rekisterinpitäjä ja rekisterin yhteyshen-

kilö. Rekisteriselosteet, jotka koskevat kaupungin asiakkaiden henkilötietoja, on julkaistu kaupungin verkkosivuilla ja sisäiset rekisteriselosteet ovat intranetissä.

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 hallintosäännön tai delegointipäätöksen nojalla olevan erityistoimivallan käyttöön.

Rekisterin vastuuhenkilö

Rekisterin vastuuhenkilö on rekisteriselosteessa määritelty viranhaltija, joka vastaa siitä, että rekisteritoiminnot suunnitellaan ja toteutetaan säännösten, määräysten sekä annettujen yleisohjeiden mukaisesti. Lisäksi hän huolehtii rekisteröityjen oikeuksien toteuttamisesta, kuten tietopyyntöihin ja tiedonoikaisemisvaatimuksiin vastaamisesta.

Rekisterin yhteyshenkilö

Rekisteriselosteessa määritelty henkilö, joka ottaa vastaan tietopyynnöt ja tiedon korjaamisvaatimukset. Hän myös kerää tiedot ja toimittaa ne rekisterin vastuuhenkilölle.

Rekisteröity

Rekisteröity tarkoittaa henkilöä, jonka tietoja käsitellään. EU:n tietosuoja-asetus takaa erilaisia oikeuksia rekisteröidylle. Oikeuksia sovelletaan eri tavoin riippuen siitä, mikä on henkilötietojen käsittelyperuste.

Seloste käsittelytoimista

Seloste käsittelytoimista on yleinen kuvaus siitä, miten rekisterinpitäjä käsittelee henkilötietoja. Selosteet laaditaan kaupungin sisäiseen käyttöön ja valvontaviranomaista varten.

Tietopyyntöjen kokoaja

Tietopyyntöjen kokoajan tehtävänä on vastaanottaa tietopyynnöt, huolehtia tietojen keräämisen koordinoinnista eri rekistereistä ja vastauksen toimittamisesta tiedot pyytäneelle henkilölle.

Tietosuojavaltuutettu

Tietosuojavaltuutettu on Suomen kansallinen valvontaviranomainen tietosuoja-asioissa. Tietosuojavaltuutettu valvoo henkilötietojen käsittelyn lainmukaisuutta ja tietosuojaoikeuksien toteutumista.

Tietosuojavastaava

Tietosuojavastaava on kaupunginhallituksen nimittämä viranhaltija, jonka tehtävät ja asema on määritelty tietosuoja-asetuksessa. Tietosuojavastaava mm. neuvoo ja ohjeistaa tietosuojalainsäädännön mukaisista velvollisuuksista, seuraa, että tietosuojalainsäädöksiä kaupungin toiminnassa noudatetaan ja tekee tähän liittyviä tarkastuksia.

Tietoturva

Tietoturva liittyy läheisesti tietosuojaan. Tietoturvalla edistetään tietosuojan toteutumista erilaisin keinoin, esimerkiksi suojaamalla tietojärjestelmiä. Tietoturvalla huolehditaan siitä, että tieto on saatavilla ja käytettävissä, ja se pysyy eheänä ja luottamuksellisena.

Turvakielto

Maistraatti voi myöntää turvakiellon henkilölle, joka epäilee oman tai perheensä turvallisuuden olevan uhattuna. Turvakieltohenkilön kotikunta- ja osoitetietoja ei luovuteta väestötietojärjestelmästä muille kuin niille viranomaisille, joilla on lain mukaan oikeus käsitellä näitä tietoja.

Vaikutustenarviointi

Tietosuojan vaikutustenarviointi auttaa tunnistamaan ja hallitsemaan henkilötietojen käsittelystä aiheutuvia riskejä. Vaikutustenarvioinnissa arvioidaan henkilötietojen käsittelyn vaikutuksia henkilötietojen suojalle. Jos suunniteltu henkilötietojen käsittely todennäköisesti aiheuttaa rekisteröidyn oikeuksille korkean riskin, on ennen käsittelyn aloittamista tehtävä vaikutustenarviointi ja tunnistettava keinoja riskin hallitsemiseksi.

EU:n yleinen tietosuoja-asetus (EU) 2016/679: 4 art. kohdat 1, 2, 5, 6, 7, 8, 21

4. Henkilötietojen käsittelyä koskevat periaatteet

4.1 Periaatteet ohjaavat henkilötietojen käsittelyä

Tietosuoja-asetuksessa säädetään henkilötietojen käsittelyä koskevista periaatteista, jotka ohjaavat rekisterinpitäjää toimimaan henkilötietoja käsiteltäessä rekisteröidyn vapauksia ja oikeuksia kunnioittavalla tavalla. Henkilötietojen käsittelyä koskevat seuraavat periaatteet:

Lainmukaisuus, kohtuullisuus ja läpinäkyvyys
Henkilötietoja on käsiteltävä lainmukaisesti, asianmukaisesti ja läpinäkyvästi. Käsittelylle on aina oltava lain mukainen peruste eikä henkilötietoja saa käyttää väärin. Lisäksi rekisteröidyille tulee kertoa siitä, miten heitä koskevia tietoja kerätään ja käytetään sekä missä määrin henkilötietoja käsitellään.

Käyttötarkoitussidonnaisuus
Henkilötietojen kerääminen on kytköksissä niiden käyttötarkoitukseen. Tiedot on kerättävä tiettyä, nimenomaista ja laillista tarkoitusta varten eikä kerättyä tietoa saa käyttää myöhemmin muuhun tarkoitukseen ilman, että tämä uusi käyttötarkoitus on yhteensopiva alkuperäisen käyttötarkoituksen kanssa.

Tietojen minimointi
Henkilötietoja ei saa käsitellä turhaan. Niitä on käsiteltävä vain, jos käsittelyn tarkoitusta ei voida kohtuullisesti toteuttaa muilla keinoin.

Henkilötietojen on oltava asianmukaisia ja olennaisia, ja niiden käsittelyn pitää rajoittua vain tarpeelliseen.

Täsmällisyys
Henkilötietojen on oltava täsmällisiä ja päivitettyjä. Epätarkat ja virheelliset henkilötiedot on poistettava tai oikaistava viipymättä.

Henkilötiedot on säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten.

Säilytyksen rajoittaminen
Henkilötiedot on säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten.

Rekisterinpitäjän on asetettava määräajat henkilötietojen poistoa tai niiden säilyttämisen tarpeellisuuden määräaikaistarkastelua varten, jotta voidaan varmistaa, ettei henkilötietoja säilytetä pidempään kuin on tarpeen.

Eheys ja luottamuksellisuus
Henkilötietoja on käsiteltävä tavalla, jolla varmistetaan niiden asianmukainen turvallisuus. Tähän sisältyy suojaaminen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta.

4.2 Sisäänrakennettu ja oletusarvoinen tietosuoja

Sisäänrakennettu ja oletusarvoinen tietosuoja tarkoittaa, että rekisterinpitäjän on otettava edellä mainitut tietosuojaperiaatteet huomioon ja sisällytettävä ne kaikkiin henkilötietojen käsittelyn vaiheisiin mahdollisimman varhaisessa vaiheessa. Ne on otettava huomioon jo siinä vaiheessa, kun suunnitellaan henkilötietojen käsittelyä sisältäviä toimintoja ja prosesseja tai kehitetään tietojärjestelmiä. Esimerkiksi tietojärjestelmät on lähtökohtaisesti rakennettava niin, että rekisterinpitäjä voi toteuttaa velvollisuutensa. Näin varmistetaan, että käsittely vastaa tietosuoja-asetuksen vaatimuksia.

Tietosuojaperiaatteiden toteuttamiseksi rekisterinpitäjän tulee tehdä tarvittavat tekniset ja organisatoriset toimenpiteet. Niillä tarkoitetaan esimerkiksi henkilöstön koulutusta, henkilöstölle annettavia ohjeita ja määräyksiä, salassapitositoumuksia, tilojen valvomista, itse toteutettavaa käytönvalvontaa, tietojärjestelmien tietoturvaa, tietojen salausta, tietojen anonymisointia, tietojen pseudonymisointia, auditointeja, tarkastus- ja valvontajärjestelmiä, käytännesääntöjä ja sertfikaatteja.

Helsingin kaupungin toteuttamia teknisiä ja organisatorisia toimenpiteitä kuvataan tarkemmin luvussa 8.4.

Rekisterinpitäjän on lisäksi pystyttävä osoittamaan, että tietosuojaperiaatteita noudatetaan. Helsingin kaupungin toteuttamaa osoitusvelvollisuutta kuvataan luvussa 8.5.

EU:n yleinen tietosuoja-asetus (EU) 2016/679: Johdanto: kohdat 39, 74–77, 78, 5 art., 24 art., 25 art.

5. Henkilötietojen käsittelyn perusteet

5.1 Henkilötietojen käsittelyn on perustuttava lakiin

Henkilötietoja saa käsitellä vain silloin, kun käsittelylle on laista löytyvä peruste. Käsittelyperuste vaikuttaa siihen, mitä oikeuksia rekisteröidyllä on eri tilanteissa. Tietosuoja-asetus määrittelee seuraavat perusteet, joilla henkilötietoja saa käsitellä:

Suostumus

Henkilötietoja saa käsitellä, jos rekisteröity on antanut suostumuksensa henkilötietojen käsittelyyn tiettyä käyttötarkoitusta varten.

Suostumus on annettava vapaaehtoisesti, selkeästi ja siten, että suostumuksen olemassaolo voidaan osoittaa. Käytännössä tämä tarkoittaa sitä, että suostumus on annettava kirjallisesti tai sähköisessä muodossa. Suostumuksesta tulee käydä ilmi yksilöity ja yksiselitteinen tahdonilmaisu, eli minkä henkilötietojen käsittelyyn on suostuttu ja mihin käyttötarkoitukseen suostumus on annettu. Vaikka kirjallinen suostumus on pääsääntö, voidaan suostumus antaa muussakin muodossa, jos kirjallinen suostumus ei ole mahdollinen, esimerkiksi jos asiakas ei kykene kirjoittamaan. Rekisterinpitäjän on joka tapauksessa pystyttävä osoittamaan, että suostumus on olemassa.

Suostumus tulee aina voida peruuttaa yhtä helposti kuin se on annettu.

Suostumusta ei voi antaa jättämällä tekemättä jotain, vaan sen tulee perustua nimenomaiseen toimenpiteeseen. Esimerkiksi jos suostumus annetaan rastittamalla suostumustekstiä vastaava ruutu paperilla tai sähköisessä järjestelmässä, ei kyseinen ruutu saa olla valmiiksi rastitettu, vaan asiakas itse rastittaa sen.

Suostumuksella ei voida ohittaa luvussa 4 lueteltuja henkilötietojen käsittelyä koskevia periaatteita eli rekisteröity ei voi antaa suostumustaan siihen, että hänen tietojaan saa käsitellä vapaasti mihin tahansa tarkoituksiin. Suostumukseen on suhtauduttava erityisen kriittisesti silloin, kun rekisteröidyn ja rekisterinpitäjän välillä on epäsuhta eli esimerkiksi tilanteessa, jossa rekisterinpitäjänä on viranomainen ja jossa on sen vuoksi epätodennäköistä, että suostumus on annettu vapaaehtoisesti kaikissa kyseiseen tilanteeseen liittyvissä olosuhteissa.

Sopimus

Henkilötietoja saa käsitellä, jos käsittely on tarpeen rekisteröidyn kanssa tehdyn sopimuksen täytäntöön panemiseksi tai sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn puolesta.

Sopimuksen tekemisen yhteydessä on yleensä oikeus kerätä myös henkilötunnus mahdollisen pakkotäytäntöönpanon tai sopimukseen perustuvien saatavien perinnän varalta.

Lakisääteinen velvoite

Helsingin kaupungilla on lakisääteisiä velvoitteita, joiden noudattamiseksi on välttämätöntä kerätä henkilötietoja. Tällaisia velvoitteita ovat esimerkiksi perusopetuksen järjestäminen, sosiaali- ja terveydenhuollon järjestäminen ja pysäköinninvalvonnan järjestäminen. Velvoitteen tulee perustua joko kansalliseen tai Euroopan unionin lainsäädäntöön. Henkilötietoja saa kerätä vain siinä laajuudessa kuin se on tarpeen lakisääteisen velvoitteen toteuttamiseksi.

Laissa voidaan säätää henkilötietojen käsittelyn tarkemmista vaatimuksista, kuten rekisterinpitäjästä, käsiteltävien henkilötietojen tyypistä, asianomaisista rekisteröidyistä ja tahoista, joille tietoja voidaan luovuttaa, tietojen säilytysajoista sekä toimenpiteistä, joilla varmistetaan tietojen laillinen ja asianmukainen käsittely.

Tietosuoja-asetuksen ja kansallisen tietosuojalain henkilötietojen käsittelylle asettamien vaatimusten lisäksi on tunnettava kunkin rekisterin osalta tietojen keräämiseen liittyvät mahdolliset erityislainsäädännön vaatimukset, kuten sosiaali- ja terveystoimen asiakastietojen käsittelystä annetut säädökset.

Elintärkeä etu

Henkilötietoja saa käsitellä silloin, kun se on tarpeen ihmisen elintärkeän edun suojelemiseksi. Elintärkeä etu voi olla esimerkiksi fyysisen koskemattomuuden tai hengen uhka. Tämä käsittelyperuste on toissijainen eli sitä tulee käyttää vain silloin, kun käsittelyllä ei ole muuta ilmeistä käsittelyn oikeusperustetta.

Henkilötietoja saa käsitellä vain silloin, kun käsittelylle on laista löytyvä peruste.

Yleinen etu ja julkinen valta

Henkilötietoja saa käsitellä yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi, jos:

- kysymys on henkilön asemaa, tehtäviä sekä niiden hoitoa julkisyhteisössä, elinkeinoelämässä, järjestötoiminnassa tai muussa vastaavassa toiminnassa kuvaavista tiedoista siltä osin kuin käsittelyn tavoite on yleisen edun mukainen ja käsittely on oikeasuhtaista sillä tavoiteltuun oikeutettuun päämäärään nähden
- käsittely on tarpeen ja oikeasuhtaista viranomaisen toiminnassa yleisen edun mukaisen tehtävän suorittamiseksi
- käsittely on tarpeen tieteellistä tai historiallista tutkimusta tai tilastointia varten ja se on oikeasuhtaista sillä tavoiteltuun yleisen edun mukaiseen tavoitteeseen nähden
- henkilötietoja sisältävien tutkimusaineistojen, kulttuuriperintöaineistojen sekä näiden kuvailutietoihin liittyvien henkilötietojen käsittely arkistointitarkoituksessa on tarpeen ja oikeasuhtaista sillä tavoiteltuun yleisen edun mukaiseen tavoitteeseen ja rekisteröidyn oikeuksiin nähden.

Oikeutettu etu

Rekisterinpitäjällä voi olla oikeutettu etu käsitellä rekisteröidyn henkilötietoja esimerkiksi silloin, kun rekisteröidyn ja rekisterinpitäjän välillä on merkityksellinen ja asianmukainen suhde, kuten asiakkuus- tai palvelussuhde. Myös henkilötietojen käsittelyä suoramarkkinointitarkoituksessa voidaan pitää oikeutetun edun toteuttamiseksi suoritettuna, mutta rekisteröidyllä on oikeus kieltää suoramarkkinointi. Rekisterinpitäjällä, joka kuuluu konserniin, saattaa olla oikeutettu etu siirtää konsernin sisällä henkilötietoja esimerkiksi hallinnollisista syistä.

Oikeutettu etu käsittelyperusteena edellyttää erityisen tarkkaa rekisteröidyn etujen ja oikeuksien huomioimista. Rekisterinpitäjän on arvioitava tasapainotestillä, voiko oikeutettua etua käyttää henkilötietojen käsittelyperusteena.

Oikeutettua etua käsittelyperusteena ei sovelleta tietojenkäsittelyyn, jota viranomaiset suorittavat tehtäviensä yhteydessä. Se ei siis voi olla peruste käsittelylle, kun kysymys on kaupungin viranomaistoiminnasta.

5.2 Henkilötietojen käsittely muuhun kuin alkuperäiseen käsittelytarkoitukseen

Henkilötietoja voidaan käsitellä myöhemmin muuhun kuin alkuperäiseen käsittelytarkoitukseen vain, jos käsittely sopii yhteen alkuperäisten tarkoitusten kanssa. Yhteensopivuutta harkittaessa on huomioitava henkilötietojen keräämisen alkuperäisen tarkoituksen ja myöhemmän käsittelyn tarkoituksen väliset yhteydet, henkilötietojen keräämisen asiayhteys erityisesti rekisterinpitäjän ja rekisteröidyn välisen suhteen osalta, henkilötietojen luonne, aiotun myöhemmän käsittelyn seuraukset rekisteröidylle ja asianmukaisten suojatoimien, kuten salaamisen tai pseudonymisoinnin olemassaolo.

Henkilötietojen myöhempi käsittely yleisen edun mukaiseen arkistointitarkoitukseen, tieteellistä tai historiallista tutkimustarkoitusta varten tai tilastollisiin tarkoituksiin on sallittua.

Henkilötietoja voidaan käsitellä myöhemmin muuhun kuin alkuperäiseen käsittelytarkoitukseen vain, jos käsittely sopii yhteen alkuperäisten tarkoitusten kanssa.

5.3 Henkilötunnuksen käsittely

Henkilötunnusta saa käsitellä rekisteröidyn suostumuksella tai jos käsittelystä säädetään laissa. Lisäksi henkilötunnusta saa käsitellä, jos rekisteröidyn yksiselitteinen yksilöiminen on tärkeää:

- laissa säädetyn tehtävän suorittamiseksi
- rekisteröidyn tai rekisterinpitäjän oikeuksien ja velvollisuuksien toteuttamiseksi
- historiallista tai tieteellistä tutkimusta tai tilastointia varten.

Henkilötunnusta saa käsitellä luotonannossa tai saatavan perimisessä, vakuutus-, luottolaitos-, maksupalvelu-, vuokraus- ja lainaustoiminnassa, luottotietotoiminnassa, terveydenhuollossa, sosiaalihuollossa ja muun sosiaaliturvan toteuttamisessa tai virka-, työ- ja muita palvelussuhteita ja niihin liittyviä etuja koskevissa asioissa.

Sen lisäksi henkilötunnuksen saa luovuttaa osoitetietojen päivittämiseksi tai moninkertaisten postilähetysten välttämiseksi suoritettavaa tietojenkäsittelyä varten, jos henkilötunnus on jo luovutuksensaajan käytettävissä.

Henkilötunnusta ei saa merkitä tarpeettomasti henkilörekisterin perusteella tulostettuihin tai laadittuihin asiakirjoihin.

5.4 Turvakiellon alaisen osoitteen käsittely

Maistraatti voi myöntää turvakiellon henkilölle, joka epäilee oman tai perheensä turvallisuuden olevan uhattuna. Turvakieltohenkilön kotikunta- ja osoitetietoja ei luovuteta väestötietojärjestelmästä muille kuin niille viranomaisille, joilla on lain mukaan oikeus käsitellä näitä tietoja.

Helsingin kaupungilla on määritelty erikseen työntekijät, joille on anottu Väestörekisterikeskukselta suorakäyttöoikeudet väestötietojärjestelmään, ja he voivat tarvittaessa katsoa turvakieltohenkilön osoitteen. He eivät saa luovuttaa tietoja edelleen eivätkä antaa niitä sivullisen nähtäväksi tai käsiteltäväksi, jollei laissa toisin säädetä.

Turvakieltohenkilölle lähetettävien viestien osoitekenttään ei saa merkitä ”Turvakielto”. Sen sijaan osoitekenttään merkitään teksti ”Osoite ei näy, ota yhteyttä [kaupungin työntekijään, jolla on suorakäyttöoikeudet väestötietojärjestelmään]”. Hakasulkeissa oleva teksti korvataan kaupungin työntekijän nimellä, jolla on suorakäyttöoikeudet väestötietojärjestelmään. Hän selvittää turvakieltohenkilön osoitteen ja huolehtii viestin lähettämisestä vastaanottajalle.

Tilanteessa, jossa turvakiellon alainen osoite on saatu turvakieltohenkilöltä itseltään tiettyyn käyttötarkoitukseen, tulee myös olla erityisen huolellinen, eikä osoitetta saa luovuttaa eteenpäin.

Henkilön yhteystiedot, mukaan lukien osoite, voivat olla salassa pidettäviä myös ilman turvakieltoa, jos henkilö on pyytänyt tietojen salassapitoa ja hänellä on perusteltu syy epäillä itsensä tai perheensä terveyden tai turvallisuuden tulevan uhatuksi.

EU:n yleinen tietosuoja-asetus (EU) 2016/679: Johdanto: kohta 43, 6 art.

Tietosuojalaki 1050/2018: 4 §, 29 §

Laki väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista 21.8.2009/661: 37 §

6. Erityisiä henkilötietoryhmiä koskeva käsittely

6.1 Erityisiä henkilötietoryhmiä koskeva käsittelykielto

Erityisiin henkilötietoryhmiin kuuluvien henkilötietojen käsittely on lähtökohtaisesti kiellettyä. Tällaisista henkilötiedoista ilmenee jokin seuraavista:

- rotu tai etninen alkuperä
- poliittisia mielipiteitä
- uskonnollinen tai filosofinen vakaumus
- ammattiliiton jäsenyys
- geneettisiä ja biometrisia tietoja henkilön tunnistamista varten
- terveyttä koskeva tieto
- ihmisen seksuaalista käyttäytymistä ja suuntautumista koskeva tieto.

Tietosuoja-asetuksessa ja tietosuojalaissa on kuitenkin määritelty poikkeuksia käsittelykieltoon, jolloin edellä mainittuja henkilötietoja saa käsitellä.

6.2 Tietosuoja-asetuksen mukainen poikkeus käsittelykiellosta

Erityisiä henkilötietoryhmiä koskevaa tietoa saa käsitellä, kun:

- rekisteröity on antanut **nimenomaisen suostumuksensa** kyseisten henkilötietojen käsittelyyn yhtä tai useampaa tiettyä tarkoitusta varten
- käsittely on tarpeen rekisterinpitäjän tai rekisteröidyn **velvoitteiden ja erityisten oikeuksien noudattamiseksi työoikeuden, sosiaaliturvan ja sosiaalisen suojelun alalla**, siltä osin kuin se sallitaan unionin oikeudessa tai jäsenvaltion lainsäädännössä tai jäsenvaltion lainsäädännön mukaisessa työehtosopimuksessa, jossa säädetään rekisteröidyn perusoikeuksia ja etuja koskevista asianmukaisista suojatoimista
- käsittely on tarpeen rekisteröidyn tai toisen luonnollisen henkilön **elintärkeiden etujen suojaamiseksi**, jos rekisteröity on fyysisesti tai juridisesti estynyt antamasta suostumustaan
- käsittely suoritetaan poliittisen, filosofisen, uskonnollisen tai ammattiliittotoimintaan liittyvän säätiön, yhdistyksen tai muun voittoa tavoittelemattoman **yhteisön laillisen toiminnan yhteydessä** ja asianmukaisin suojatoimin, sillä edellytyksellä, että käsittely koskee ainoastaan näiden yhteisöjen jäseniä tai entisiä jäseniä tai henkilöitä, joilla on yhteisöihin säännölliset, yhteisöjen tarkoituksiin liittyvät yhteydet, ja että henkilötietoja ei luovuteta yhteisön ulkopuolelle ilman rekisteröidyn suostumusta
- käsittely koskee henkilötietoja, jotka **rekisteröity on nimenomaisesti saattanut julkisiksi**
- käsittely on tarpeen **oikeusvaateen laatimiseksi, esittämiseksi tai puolustamiseksi** tai aina, kun tuomioistuimet suorittavat lainkäyttötehtäviään
- käsittely on tarpeen **tärkeää yleistä etua koskevasta syystä** unionin oikeuden tai jäsenvaltion lainsäädännön nojalla, edellyttäen että se on oikeasuhteinen tavoitteeseen nähden, siinä noudatetaan keskeisiltä osin oikeutta henkilötietojen suojaan ja siinä säädetään asianmukaisista ja erityisistä toimenpiteistä rekisteröidyn perusoikeuksien ja etujen suojaamiseksi
- käsittely on tarpeen **ennalta ehkäisevää tai työterveydenhuoltoa koskevia tarkoituksia varten, työntekijän työkyvyn arvioimiseksi, lääketieteellisiä diagnooseja varten, terveys- tai sosiaalihuollollisen hoidon tai käsittelyn suorittamiseksi taikka terveys- tai sosiaalihuollon palvelujen ja järjestelmien hallintoa varten** unionin oikeuden tai jäsenvaltion lainsäädännön perusteella tai terveydenhuollon ammattilaisen kanssa tehdyn sopimuksen mukaisesti. Henkilötietoja voidaan käsitellä näihin tarkoituksiin, kun kyseisiä tietoja käsittelee tai niiden käsittelystä vastaa ammattilainen tai muu henkilö, jolla on lakisääteinen salassapitovelvollisuus.
- käsittely on tarpeen **kansanterveyteen liittyvän yleisen edun vuoksi**, kuten vakavilta rajat ylittäviltä terveysuhkilta suojautumiseksi tai terveydenhuollon, lääkevalmisteiden tai lääkinnällisten laitteiden korkeiden laatu- ja turvallisuusnormien varmistamiseksi sellaisen unionin oikeuden tai jäsenvaltion lainsäädännön perusteella, jossa säädetään asianmukaisista ja erityisistä toimenpiteistä rekisteröidyn oikeuksien ja vapauksien, erityisesti salassapitovelvollisuuden, suojaamiseksi.
- käsittely on tarpeen **yleisen edun mukaisia arkistointitarkoituksia taikka tieteellisiä ja historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten** tietosuoja-asetuksen mukaisesti unionin oikeuden tai jäsenvaltion lainsäädännön nojalla, edellyttäen että se on oikeasuhteinen käsittelyn tavoitteeseen nähden, siinä noudatetaan keskeisiltä osin oikeutta henkilötietojen suojaan ja siinä säädetään asianmukaisista ja erityisistä toimenpiteistä rekisteröidyn perusoikeuksien ja etujen suojaamiseksi.

Jäsenvaltiot voivat pitää voimassa tai ottaa käyttöön lisäehtoja, mukaan lukien rajoituksia, jotka koskevat geneettisten tietojen, biometristen tietojen tai terveystietojen käsittelyä.

6.3 Tietosuojalain mukainen poikkeus käsittelykiellosta

Seuraava erityisiä henkilötietoryhmiä koskevaa käsittely on sallittua:

- **vakuutuslaitoksen käsitellessä vakuutustoiminnassa saatuja tietoja** vakuutetun ja korvauksenhakijan terveydentilasta, sairaudesta tai vammaisuudesta taikka sellaista häneen kohdistetuista hoitotoimenpiteistä tai niihin verrattavista toimista, jotka ovat tarpeen vakuutuslaitoksen vastuun selvittämiseksi
- **tietojen käsittelyyn, josta säädetään laissa** tai joka johtuu välittömästi rekisterinpitäjälle laissa säädetystä tehtävästä
- **ammattiliittoon kuulumista koskevaan tiedon käsittelyyn**, joka on tarpeen rekisterinpitäjän erityisten oikeuksien ja velvoitteiden noudattamiseksi työoikeuden alalla
- **kun terveydenhuollon palveluntarjoaja järjestäessään tai tuottaessaan palveluja käsittelee tässä toiminnassa saamiaan tietoja** henkilön terveydentilasta tai vammaisuudesta taikka hänen saamastaan terveydenhuollon ja kuntoutuksen palvelusta taikka muita rekisteröidyn hoidon kannalta välttämättömiä tietoja
- **kun sosiaalihuollon palveluntarjoaja järjestäessään tai tuottaessaan palveluja tai myöntäessään etuuksia käsittelee tässä toiminnassa saamiaan tai tuottamiaan tietoja** henkilön terveydentilasta tai vammaisuudesta taikka hänen saamastaan terveydenhuollon ja kuntoutuksen palvelusta taikka muita rekisteröidyn palvelun tai etuuden myöntämisen kannalta välttämättömiä tietoja
- **terveyttä koskevien ja geneettisten tietojen käsittelyyn antidopingtyössä ja vammaisurheilun yhteydessä** siltä osin kuin näiden tietojen käsittely on välttämätöntä antidopingtyön tai vammaisten ja pitkäaikaissairaiden urheilun mahdollistamiseksi
- **tieteellistä tai historiallista tutkimusta taikka tilastointia varten** tehtävään tietojen käsittelyyn
- **tutkimus- ja kulttuuriperintöaineistojen käsittelyyn yleishyödyllisessä** arkistointitarkoituksessa geneettisiä tietoja lukuun ottamatta.

Käsiteltäessä henkilötietoja tietosuojalaissa tarkoitetussa tilanteessa rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava asianmukaiset ja erityiset toimenpiteet rekisteröidyn oikeuksien suojaamiseksi. Näitä toimenpiteitä ovat:

- toimenpiteet, joilla on jälkeenpäin mahdollista varmistaa ja todentaa kenen toimesta henkilötietoja on tallennettu, muutettu tai siirretty
- toimenpiteet, joilla parannetaan henkilötietoja käsittelevän henkilöstön osaamista
- tietosuojavastaavan nimittäminen
- rekisterinpitäjän ja käsittelijän sisäiset toimenpiteet, joilla estetään pääsy henkilötietoihin
- henkilötietojen pseudonymisointi
- henkilötietojen salaaminen
- toimenpiteet, joilla käsittelyjärjestelmien ja henkilötietojen käsittelyyn liittyvien palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus taataan, mukaan lukien kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa
- menettely, jolla testataan, tutkitaan ja arvioidaan säännöllisesti teknisten ja organisatoristen toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi
- erityiset menettelysäännöt, joilla varmistetaan tietosuoja-asetuksen ja tämän lain noudattaminen siirrettäessä henkilötietoja tai käsiteltäessä henkilötietoja muuhun tarkoitukseen
- tietosuojaa koskevan vaikutustenarvioinnin laatiminen
- muut tekniset, menettelylliset ja organisatoriset toimenpiteet.

EU:n yleinen tietosuoja-asetus (EU) 2016/679: 9 art.

Tietosuojalaki 1050/2018: 6 §

Käsiteltäessä henkilötietoja tietosuojalaissa tarkoitetussa tilanteessa rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava asianmukaiset ja erityiset toimenpiteet rekisteröidyn oikeuksien suojaamiseksi

7. Rikostuomioihin ja rikkomuksiin liittyvien henkilötietojen käsittely

Rikostuomioihin ja rikkomuksiin tai niihin liittyviin turvaamistoimiin liittyvien henkilötietojen käsittely luvussa 5 luetelluilla henkilötietojen käsittelyn perusteilla on mahdollista silloin, kun se suoritetaan viranomaisen valvonnassa. Lisäksi rikostuomioihin ja rikkomuksiin tai niihin liittyviin turvaamistoimiin liittyviä henkilötietoja saa käsitellä, jos

- käsittely on tarpeen oikeusvaateen laatimiseksi, esittämiseksi, puolustamiseksi tai ratkaisemiseksi tai
- tietoja käsitellään jossain seuraavista tarkoituksista:
  - vakuutuslaitoksen käsitellessä vakuutustoiminnassa saatuja tietoja vakuutetun ja korvauksenhakijan terveydentilasta, sairaudesta tai vammaisuudesta taikka sellaista häneen kohdistetuista hoitotoimenpiteistä tai niihin verrattavista toimista, jotka ovat tarpeen vakuutuslaitoksen vastuun selvittämiseksi
  - tietojen käsittelyyn, josta säädetään laissa tai joka johtuu välittömästi rekisterinpitäjälle laissa säädetystä tehtävästä
  - tieteellistä tai historiallista tutkimusta tai tilastointia varten tehtävään tietojen käsittelyyn.

Käsiteltäessä rikostuomioihin ja rikkomuksiin tai niihin liittyviin turvaamistoimiin liittyviä henkilötietoja yllä luetelluilla perusteilla rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava asianmukaiset ja erityiset toimenpiteet rekisteröidyn oikeuksien suojaamiseksi. Näitä toimenpiteitä ovat:

- toimenpiteet, joilla on jälkeenpäin mahdollista varmistaa ja todentaa kenen toimesta henkilötietoja on tallennettu, muutettu tai siirretty
- toimenpiteet, joilla parannetaan henkilötietoja käsittelevän henkilöstön osaamista
- tietosuojavastaavan nimittäminen
- rekisterinpitäjän ja käsittelijän sisäiset toimenpiteet, joilla estetään pääsy henkilötietoihin
- henkilötietojen pseudonymisointi
- henkilötietojen salaaminen
- toimenpiteet, joilla käsittelyjärjestelmien ja henkilötietojen käsittelyyn liittyvien palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus taataan, mukaan lukien kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa
- menettely, jolla testataan, tutkitaan ja arvioidaan säännöllisesti teknisten ja organisatoristen toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi
- erityiset menettelysäännöt, joilla varmistetaan tietosuoja-asetuksen ja tämän lain noudattaminen siirrettäessä henkilötietoja tai käsiteltäessä henkilötietoja muuhun tarkoitukseen
- tietosuojaa koskevan vaikutustenarvioinnin laatiminen
- muut tekniset, menettelylliset ja organisatoriset toimenpiteet.

Kattavaa rikosrekisteriä pidetään vain julkisen viranomaisen valvonnassa.

EU:n yleinen tietosuoja-asetus (EU) 2016/679: 10 art.

Tietosuojalaki 1050/2018: 7 §

8. Rekisterinpitäjän velvollisuudet

8.1 Rekisteröidyn informointi

Rekisterinpitäjän on toimitettava rekisteröidylle henkilötietojen käsittelyä koskevat tiedot. Tiedot on annettava tiiviisti esitetyssä, läpinäkyvässä, helposti ymmärrettävässä ja saatavilla olevassa muodossa selkeällä ja yksinkertaisella kielellä. Tiedot on toimitettava kirjallisesti tai muulla tavoin. Tiedot voidaan antaa myös sähköisesti. Jos rekisteröity pyytää, tiedot voidaan antaa suullisesti edellyttäen, että rekisteröidyn henkilöllisyys on vahvistettu.

Rekisterinpitäjän on toiminnallaan helpotettava rekisteröidyn oikeuksien käyttämistä ja varmistettava oikeuksien tehokas toteutuminen. Lisätietoa rekisteröidyn oikeuksista on luvussa 10 ja tietopyyntöjen käsittelystä luvussa 12.

Helsingin kaupunki antaa rekisteröidyille tarvittavan informaation kaupungin internetsivuilla. Sivuilla annetaan yleisinformaatiota henkilötietojen käsittelystä Helsingin kaupungilla sekä kerrotaan rekisteröidyn oikeuksista ja niiden toteuttamisesta. Lisäksi sivuilla on rekisteriselosteet, joissa kerrotaan henkilötietojen käsittelystä rekisterikohtaisesti. Sivuilla kerrotaan myös kaupungin tietosuojavastaavan yhteystiedot.

Rekisterinpitäjän on toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja osoittaa, että henkilötietojen käsittelyssä noudatetaan tietosuoja-asetusta.

Perustiedot tietosuojasta Helsingin kaupungilla, tiedot rekisteröidyn oikeuksista ja niiden toteuttamisesta sekä rekisteriselosteet tulostetaan rekisteröidylle tarvittaessa.

Rekisteröidyn informointi onnistuu parhaiten ensimmäisen asioinnin yhteydessä, jolloin hänelle annetaan tiedot siitä, miten hänen henkilötietojaan käsitellään kyseisessä palvelussa.

8.2 Rekisteriselosteet

Henkilötietoja kerätään eri rekistereihin tietojen käyttötarkoitusten mukaan. Henkilörekistereistä laaditaan rekisteriselosteet, joissa kerrotaan:

- rekisterin nimi
- rekisterinpitäjän ja tämän edustajan yhteystiedot
- henkilötietojen käsittelyn tarkoitukset sekä käsittelyn oikeusperuste
- rekisterin tietosisältö
- tieto henkilötietojen säännönmukaisista luovutuksista
- henkilötietojen säilytysaika tai jos se ei ole mahdollista, tämän ajan määrittämiskriteerit
- henkilötietojen tietolähteet.

Toimialojen, liikelaitosten ja virastojen tietosuojan vastuuhenkilöt huolehtivat rekisteriselosteiden laatimisesta. Selosteet tehdään kaupungin rekisteriselostepohjalle.

Valmiit rekisteriselosteet toimitetaan tietosuojatiimille, joka huolehtii selosteiden julkaisemisesta kaupungin internetsivujen tietosuojasivuilla tai intranetissä niiden rekisteriselosteiden osalta, jotka koskevat vain kaupungin työntekijöiden henkilötietoja.

8.3 Seloste käsittelytoimista

Rekisterinpitäjän on ylläpidettävä selosteita käsittelytoimista. Selosteet käsittelytoimista ovat yleisiä kuvauksia siitä, miten rekisterinpitäjä käsittelee henkilötietoja. Selosteet käsittelytoimista laaditaan sisäiseen käyttöön ja valvontaviranomaista varten. Selosteissa kerrotaan:

- rekisterin tai palvelukokonaisuuden nimi
- rekisterinpitäjä ja yhteystiedot
- tietosuojavastaava ja hänen yhteystietonsa
- henkilötietojen käsittelyn tarkoitukset
- kuvaus rekisteröityjen ryhmistä
- kuvaus henkilötietoryhmistä
- vastaanottajaryhmät
- tietojen säilytysajat
- kuvaus teknisistä ja organisatorisista turvatoimista
- tieto henkilötietojen säännönmukaisista luovutuksista EU/ETA-alueen ulkopuolelle
- viittaus henkilötietojen käsittelijän kanssa solmittuun käsittelyä koskevaan sopimukseen.

Toimialojen, liikelaitosten ja virastojen tietosuojan vastuuhenkilöt laativat selosteet käsittelytoimista hyödyntäen kaupungin mallipohjaa ja erillistä ohjetta.

8.4 Tarvittavat tekniset ja organisatoriset toimenpiteet tietojen suojaamiseksi

Rekisterinpitäjän on toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja osoittaa, että henkilötietojen käsittelyssä noudatetaan tietosuoja-asetusta. Harkittaessa toimenpiteiden tarpeellisuutta on otettava huomioon käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset. Lisäksi on huomioitava ihmisten oikeuksiin ja vapauksiin kohdistuvat todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit. Teknisillä ja organisatorisilla toimenpiteillä varmistetaan, että käsitellään vain kunkin käsittelytarkoituksen kannalta tarpeellisia henkilötietoja, eikä henkilötietoja saateta rajoittamattoman henkilömäärän saataville.

Teknisillä toimenpiteillä tarkoitetaan muun muassa riittävää tietojärjestelmien tietoturvaa

eli esimerkiksi tarvittavia järjestelmän suojaustoimenpiteitä, tietojen salausta, tiedon pseudonymisointia tai tiedon anonymisointia. Teknisillä toimenpiteillä tarkoitetaan myös kykyä taata käsittelyjärjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus sekä kykyä palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa. Teknisiä toimenpiteitä ovat myös tilavalvonta ja kulunvalvonta, käyttöoikeusrajaukset ja käytönvalvonta (esimerkiksi käyttäjälokitietoja hyödyntämällä) sekä tietojärjestelmien auditoinnit. Helsingin kaupungilla käytössä olevia teknisiä toimenpiteitä kuvataan tarkemmin luvussa 11 sekä intranetin tietoturvasivustolla.

Organisatorisia toimenpiteitä ovat muun muassa ohjeistus, koulutus, henkilötietojen käsittelyn minimointi, tehtävien ja henkilötietojen käsittelyn läpinäkyvyys, sekä sen mahdollistaminen, että rekisteröity voi valvoa tietojenkäsittelyä. Organisatorisia toimenpiteitä ovat myös erilaiset tietosuojan toteutumisen seuranta- ja raportointivälineet, kuten vuosittain tehtävä tietotilinpäätös.

Uusien sovellusten, palvelujen ja tuotteiden kehittämisessä, suunnittelussa ja hankinnassa on kiinnitettävä huomioita tietosuojan toteutumiseen, mikäli toimintaan liittyy henkilötietojen käsittelyä.

Uusien sovellusten, palvelujen ja tuotteiden kehittämisessä, suunnittelussa ja hankinnassa on kiinnitettävä huomioita tietosuojan toteutumiseen, mikäli toimintaan liittyy henkilötietojen käsittelyä. Siinä hyödynnetään tietosuojan vaikutustenarviointia, josta kerrotaan lisää luvussa 14. Tietosuojan huomioimisesta sopimuksissa ja hankinnoissa on lisätietoa luvussa 16.

Sisäänrakennetun ja oletusarvoisen tietosuojan toteutumista kehittämistyössä edistetään myös kaupungin sulautetussa kehitysmallissa Kehmetissä, jossa tietosuojavaatimukset ja -toimenpiteet on integroitu kehittämisen vaihemalleihin sekä ketterään että perinteiseen kehittämismalliin.

Perusohjeistus henkilötietoja käsitteleville on Helsingin kaupungilla toteutettu videokoulutuksilla. Videot löytyvät intran tietosuojasivustolta, joka toimii tietosuoja-asioiden pääviestintäkanavana ja tietopankkina. Kaikkien kaupungin palveluksessa olevien, jotka käsittelevät henkilötietoja, tulee suorittaa koulutus ja siihen kuuluva tentti, jonka suorittaminen dokumentoidaan. Lisäksi tietosuojavastaava pitää muita tietosuojakoulutuksia tietosuojatiimin ja toimialojen, virastojen ja liikelaitosten tietosuojan vastuuhenkilöiden kanssa sekä antaa ohjeita tietosuoja-asioissa.

8.5 Osoitusvelvollisuus

Osoitusvelvollisuus tarkoittaa sitä, että organisaation pitää pystyä osoittamaan noudattavansa tietosuoja-asetusta henkilötietojen käsittelyssä sekä toteuttavansa tietosuojaperiaatteita myös käytännössä. Tämä edellyttää sitä, että henkilötietojen käsittelyyn liittyvät prosessit ja tietosuojaperiaatteiden käytännön toteuttaminen dokumentoidaan. Organisaatioilla voi myös olla käytännesääntöjä tai sertifikaatteja, joilla ne osoittavat, että asetusta on noudatettu. Helsingin kaupunki toteuttaa osoitusvelvollisuutta tuottamalla muun muassa seuraavia dokumentteja ja sisältöjä:

- rekisteriselosteet ja kaupungin internetsivuilla oleva muu rekisteröidyn informointi
- rekisteröidyn oikeuksiin liittyvien pyyntöjen dokumentointi
- tietosuojakäsikirja ja muu ohjeistus sekä prosessikuvaukset
- koulutukset, koulutusmateriaalit ja koulutuksen suorittaneiden lukumäärän dokumentointi
- intranetin tietosuojasivustot ja sisäinen tietosuojauutisointi
- tietotilinpäätös
- lokitiedot henkilötietojen käsittelystä
- selosteet käsittelytoimista
- vaikutustenarvioinnit
- tietoturvaloukkausten dokumentointi
- tietosuoja- ja salassapitoliitteen liittäminen sopimuksiin.

8.6 Käsittelijän toiminnan valvominen

Kaupungille palveluja tuottava yritys, yhdistys, säätiö tai toinen viranomainen voi käsitellä henkilötietoja kaupungin puolesta. Tällöin kaupunki on rekisterinpitäjä ja kaupungin puolesta tietoja käsittelevä yritys on käsittelijä.

Kaupunki saa rekisterinpitäjänä käyttää ainoastaan sellaisia henkilötietojen käsittelijöitä, jotka toteuttavat riittävät tekniset ja organisatoriset suojatoimet, ja käsittely täyttää tietosuojalainsäädännön vaatimukset. Tällä varmistetaan rekisteröidyn oikeuksien suojelu myös silloin, kun käsittelyn suorittaa kaupungin puolesta joku muu.

Henkilötietojen käsittelijän kaupungin puolesta suorittamasta käsittelystä on määritettävä sopimuksella, joka sitoo henkilötietojen käsittelijää suhteessa rekisterinpitäjään ja jossa vahvistetaan käsittelyn kohde ja kesto, käsittelyn luonne ja tarkoitus, henkilötietojen tyyppi ja rekisteröityjen ryhmät, rekisterinpitäjän velvollisuudet ja oikeudet. Tästä kerrotaan tarkemmin luvussa 16.

Henkilötietojen käsittelijä ei saa käyttää toisen henkilötietojen käsittelijän palveluksia ilman rekisterinpitäjän erityistä tai yleistä kirjallista ennakkolupaa. Kun kyse on kirjallisesta ennakkoluvasta, henkilötietojen käsittelijän on kerrottava rekisterinpitäjälle kaikista suunnitelluista muutoksista, jotka koskevat muiden henkilötietojen käsittelijöiden lisäämistä tai vaihtamista, ja annettava siten rekisterinpitäjälle mahdollisuus vastustaa tällaisia muutoksia.

Henkilötietojen käsittelijä tai henkilötietojen käsittelijän alaisuudessa toimiva henkilö ei saa käsitellä niitä muuten kuin rekisterinpitäjän ohjeiden mukaisesti.

EU:n yleinen tietosuoja-asetus (EU) 2016/679: Johdanto: kohdat 74– 77, 82, 98–100, 5 art. kohta 2, 13 art., 14 art., 24 art., 30 art., 40–42 art.

Kaupunki saa rekisterinpitäjänä käyttää ainoastaan sellaisia henkilötietojen käsittelijöitä, jotka toteuttavat riittävät tekniset ja organisatoriset suojatoimet, ja käsittely täyttää tietosuojalainsäädännön vaatimukset.

9. Kaupunki henkilötietojen käsittelijänä

Useimmiten kaupunki toimii rekisterinpitäjänä. Tämä käsikirjakin on kirjoitettu siitä lähtökohdasta, että rekisterinpitäjänä toimii Helsingin kaupunki. On kuitenkin mahdollista, että kaupunki käsittelee toisen rekisterinpitäjän tietoja tämän puolesta, eli kaupunki toimii tietosuoja-asetuksessa tarkoitettuna käsittelijänä. Kaupunki saattaa toimia henkilötietojen käsittelijänä esim. silloin, kun se toimii palveluntuottajana ja käsittelee palvelun tuottamiseksi toisen sopijapuolen henkilötietoja.

Kaupungin toimiessa käsittelijänä tulee sen noudattaa tietosuoja-asetuksessa käsittelijälle asetettuja velvoitteita. Kaupungin on muun muassa käsiteltävä tietoja rekisterinpitäjän antamien ohjeiden mukaisesti ja huolehdittava asianmukaisista suojatoimista. Lisäksi tietojen käsittelystä tulee sopia tietosuoja-asetuksen edellyttämällä tavalla.

Kaupunki saattaa toimia henkilötietojen käsittelijänä esim. silloin, kun se toimii palveluntuottajana ja käsittelee palvelun tuottamiseksi toisen sopijapuolen henkilötietoja.

10. Rekisteröidyn oikeudet

- Oikeus saada pääsy tietoihin
- Oikeus tiedon oikaisemiseen
- Oikeus tietojen poistamiseen
- Oikeus käsittelyn rajoittamiseen
- Oikeus siirtää tiedot järjestelmästä toiseen
- Vastustamisoikeus
- Oikeus riitauttaa automaattinen yksittäispäätös
- Oikeus tehdä valitus valvontaviranomaiselle

Tietosuoja-asetuksen mukaan rekisterinpitäjän yhtenä velvollisuutena on toteuttaa rekisteröidyn oikeuksia. Henkilötietojen käsittelyn oikeusperuste vaikuttaa siihen, mitä oikeuksia rekisteröidyllä on. Esimerkiksi oikeutta tietojen poistamiseen ei sovelleta lakisääteisiin rekistereihin eli rekisteröity ei voi vaatia tietojaan poistettavaksi esimerkiksi lastensuojelua koskevasta rekisteristä.

Rekisterinpitäjän on helpotettava rekisteröidyn oikeuksien käyttämistä ja varmistettava oikeuksien tehokas toteutuminen. Rekisteröidyn oikeuksista ja niiden toteuttamisesta kerrotaan kaupungin internetsivujen tietosuojasivuilla. Tietopyyntöihin liittyvistä prosesseista on lisätietoa luvussa 12.

Oikeus saada pääsy tietoihin

Henkilöllä, jonka henkilötietoja kerätään kaupungin palveluissa, on oikeus saada kaupungilta vahvistus siitä, että häntä koskevia henkilötietoja käsitellään tai että niitä ei käsitellä. Rekisteröity voi pyytää jäljennökset omista tiedoistaan. Tämän voi tehdä sähköisesti kaupungin internetsivuilla tai palauttamalla paperilomake kaupungin kirjaamoon tai erikseen määriteltyjen toimialojen palvelupisteisiin. Jos rekisteröity esittää oikeutta koskevan pyynnön sähköisesti, tiedot on toimitettava sähköisessä muodossa, paitsi jos rekisteröity pyytää toimittamaan tiedot muussa muodossa.

Kun rekisteröity pyytää omia tietojaan, tiedot toimitetaan hänelle ilman aiheetonta viivytystä ja joka tapauksessa kuukauden kuluessa pyynnön vastaanottamisesta.

Kun rekisteröity pyytää omia tietojaan, tiedot toimitetaan hänelle ilman aiheetonta viivytystä ja joka tapauksessa kuukauden kuluessa pyynnön vastaanottamisesta. Määräaikaa voidaan tarvittaessa jatkaa enintään kahdella kuukaudella ottaen huomioon pyyntöjen monimutkaisuus ja määrä. Jos määräaikaa jatketaan, kaupunki ilmoittaa tietojen pyytäjälle asiasta kuukauden kuluessa pyynnön vastaanottamisesta sekä viivästymisen syyt.

Jos kaupunki ei toimita tietoja pyynnön perusteella, se ilmoittaa viipymättä ja viimeistään kuukauden kuluessa pyynnön vastaanottamisesta syyt siihen ja kertoo mahdollisuudesta tehdä valitus valvontaviranomaiselle ja käyttää muita oikeussuojakeinoja.

Omat tiedot on oikeus saada maksutta. Jos henkilö kuitenkin pyytää useampia jäljennöksiä, kaupunki voi periä niistä hallinnollisiin kustannuksiin perustuvan kohtuullisen maksun (Voimassaoleva päätös hinnoista: Kvsto 12.12.2001, § 358. Nykyisin toimivalta päättää maksuista on kaupunginhallituksella).

Jos tietopyynnöt ovat ilmeisen perusteettomia tai kohtuuttomia ja jos niitä esitetään toistuvasti, kaupunki voi periä kohtuullisen maksun tai kieltäytyä suorittamasta pyydettyä toimenpidettä. Tällaisissa tapauksissa kaupunki osoittaa pyynnön ilmeisen perusteettomuuden tai kohtuuttomuuden.

Kaupungin on toimitettava rekisteröidylle jäljennös käsiteltävistä henkilötiedoista. Jäljennöksen toimittaminen rekisteröidyn henkilötiedoista ei saa kuitenkaan vaikuttaa haitallisesti muiden oikeuksiin ja vapauksiin. Rekisteröidylle ei anneta esimerkiksi sellaisia tietoja, jotka ovat liikesalaisuuksia tai sisältävät myös muiden henkilöiden henkilötietoja.

Tietojen tarkastusoikeus ei ole rajoittamaton. Rekisteröidyllä ei esimerkiksi ole oikeutta tutustua hänestä kerättyihin tietoihin, jos tiedon antaminen saattaisi vahingoittaa kansallista turvallisuutta, puolustusta tai yleistä järjestystä ja turvallisuutta, haitata rikosten ehkäisemistä tai selvittämistä, tiedon antamisesta saattaisi aiheutua vakavaa vaaraa rekisteröidyn terveydelle tai hoidolle tai rekisteröidyn oikeuksille tai jonkun muun oikeuksille.

Oikeus tiedon oikaisemiseen

Henkilöllä on oikeus vaatia, että kaupunki oikaisee häntä koskevat epätarkat ja virheelliset henkilötiedot ilman aiheetonta viivytystä. Vaatimuksen voi tehdä sähköisesti kaupungin internetsivuilla tai palauttamalla paperilomakkeen kaupungin kirjaamoon tai erikseen määriteltyjen toimialojen palvelupisteisiin.

Puutteelliset tiedot on oikeus saada täydennetyiksi muun muassa toimittamalla lisäselvityksiä. Tietojen mahdollinen puutteellisuus ratkaistaan ottamalla huomioon, mitä tarkoitusta varten henkilötietoja käsitellään. Jos tietoja, joita henkilö on vaatinut lisättäväksi, ei tarvita rekisterin käyttötarkoituksen täyttämiseksi, vaadittuja tietoja ei tarvitse täydentää. Jos henkilön tietoja käsitellään esimerkiksi kirjastopalvelujen käyttämisessä, hänen tietoihinsa ei tarvitse lisätä koulutusta tai liikuntapalvelujen käyttämistä koskevia tietoja.

Jollei kaupunki hyväksy henkilön vaatimusta tiedon oikaisemisesta, kaupungin on ilmoitettava tästä kirjallisesti hänelle. Ilmoituksessa on mainittava myös ne syyt, joiden vuoksi vaatimusta tietojen oikaisemisesta ei ole hyväksytty. Lisäksi on kerrottava mahdollisuudesta saattaa asia tietosuojavaltuutetun käsiteltäväksi ja käyttää muita oikeussuojakeinoja. Ilmoitus on annettava kuukauden kuluessa pyynnön vastaanottamisesta.

Oikeus tietojen poistamiseen

Rekisteröidyllä on oikeus saada kaupunki poistamaan häntä koskevat tiedot tietyissä tapauksissa. Oikeus tietojen poistamiseen eli oikeus tulla unohdetuksi tarkoittaa rekisteröidyn oikeutta pyytää kaupunkia poistamaan esimerkiksi vanhentuneet henkilötiedot. Mikäli rekisteröidyllä on oikeus tietojensa poistamiseen, henkilötiedot on poistettava ilman aiheetonta viivytystä. Kaupungin velvollisuutena on ilmoittaa myös kaupungin puolesta henkilötietoja käsitteleville, että rekisteröity on pyytänyt poistamaan henkilötietonsa.

Oikeus tietojen poistamiseen on kuitenkin rajoitettu. Esimerkiksi tietojen poistaminen ei ole mahdollista rekistereistä, jotka ovat olemassa kaupungin lakisääteisen velvoitteen noudattamiseksi tai kaupungille kuuluvan julkisen vallan käyttämistä varten. Lisäksi oikeutta tulla unohdetuksi ei sovelleta esimerkiksi silloin, jos käsittely on tarpeen oikeudellisen vaateen laatimiseksi, esittämiseksi tai puolustamiseksi.

Oikeutta tietojen poistamiseen voidaan käyttää esimerkiksi seuraavissa tilanteissa:

- Henkilötietoja ei enää tarvita niihin tarkoituksiin, joita varten ne kerättiin tai joita varten niitä muutoin käsiteltiin. Esimerkiksi jos tietoja ei tarvita enää järjestetyn tapahtuman jälkeen, jota varten tiedot on kerätty.
- Henkilötietojen käsittely perustuu rekisteröidyn suostumukseen ja rekisteröity peruuttaa suostumuksen eikä käsittelylle ole muuta laillista perustetta. Esimerkiksi rekisteröity on antanut suostumuksensa uutiskirjeen jakeluun ja hän peruuttaa suostumuksensa.
- Rekisteröity vastustaa käsittelyä asetuksessa säädetyn vastustamisoikeutensa nojalla. Mikäli rekisteröity vastustaa muuta käsittelyä kuin käsittelyä suoramarkkinointia varten, on lisäedellytyksenä se, että käsittelyyn ei ole olemassa perusteltua syytä.
- Henkilötietoja on käsitelty lainvastaisesti. Esimerkiksi joku henkilö on esiintynyt toisena henkilönä.

Siitä huolimatta, että jokin edelle mainittu edellytys täyttyisi, tietoja ei kuitenkaan tarvitse poistaa esimerkiksi, jos käsittely on tarpeen sananvapautta ja tiedonvälityksen vapautta koskevan oikeuden käyttämiseksi tai kansanterveyteen liittyvää yleistä etua koskevista syistä asetuksen edellyttämin tavoin.

Oikeus käsittelyn rajoittamiseen

Henkilöllä, jonka tietoja on kerätty kaupungin palveluissa, on oikeus siihen, että kaupunki rajoittaa henkilötietojen käsittelyä seuraavissa tapauksissa:

- henkilö kiistää henkilötietojen paikkansapitävyyden, jolloin käsittelyä rajoitetaan siksi ajaksi, jonka kuluessa kaupunki voi varmistaa tietojen paikkansapitävyyden
- käsittely on lainvastaista ja henkilö vastustaa henkilötietojen poistamista ja vaatii sen sijaan niiden käytön rajoittamista
- kaupunki rekisterinpitäjänä ei enää tarvitse kyseisiä henkilötietoja käsittelyn tarkoituksiin, mutta rekisteröity henkilö tarvitsee niitä oikeudellisen vaateen laatimiseksi, esittämiseksi tai puolustamiseksi
- rekisteröity on vastustanut henkilötietojen käsittelyä odotettaessa sen todentamista, syrjäyttävätkö rekisterinpitäjän oikeutetut perusteet rekisteröidyn perusteet.

Jos kaupunki on rajoittanut käsittelyä edellä mainituilla perusteilla, näitä henkilötietoja saa säilyttää. Lisäksi tietoja saa käsitellä seuraavissa tapauksissa:

- kaupungin oikeudellisen vaateen laatimiseksi, esittämiseksi tai puolustamiseksi
- toisen luonnollisen henkilön tai oikeushenkilön oikeuksien suojaamiseksi
- tärkeän unionin tai sen jäsenvaltion yleistä etua koskevista syistä.

Jos henkilötietojen käsittelyä on rajoitettu edellä mainituilla perusteilla ja rajoitus poistetaan, henkilölle on ilmoitettava asiasta ennen rajoituksen poistamista.

Henkilöllä on oikeus vaatia, että kaupunki oikaisee häntä koskevat epätarkat ja virheelliset henkilötiedot ilman aiheetonta viivytystä.

Kaupunki pyrkii tietosuojalinjausten mukaisesti edistämään tietojen siirrettävyyttä silloinkin, kun se ei ole tietosuoja-asetuksen mukaan pakollista.

Oikeus siirtää tiedot järjestelmästä toiseen

Jos rekisteröity on toimittanut kaupungille omia henkilötietojaan, hänellä on oikeus siirtää kyseiset henkilötiedot toiselle rekisterinpitäjälle esimerkiksi toiselle kunnalle. Kyseinen oikeus on ainoastaan silloin, jos henkilötietojen käsittely perustuu suostumukseen tai sopimukseen, ja jos käsittely suoritetaan automaattisesti. Tätä oikeutta ei sovelleta käsittelyyn, joka on tarpeen yleistä etua koskevan tehtävän suorittamista tai kaupungille kuuluvan julkisen vallan käyttämistä varten. Kyseinen oikeus ei saa myöskään vaikuttaa haitallisesti muiden oikeuksiin ja vapauksiin eikä rajoittaa muiden rekisteröidyn oikeuksien käyttöä.

Kaupunki pyrkii tietosuojalinjausten mukaisesti edistämään tietojen siirrettävyyttä silloinkin, kun se ei ole tietosuoja-asetuksen mukaan pakollista.

Tietosuoja-asetuksen mukaan tiedot on voitava siirtää yleisesti käytetyssä, jäsennellyssä ja koneellisesti luettavassa muodossa. Sen lisäksi, että tiedot voidaan siirtää rekisteröidylle suoraan, siirtooikeuteen kuuluu myös tietojen siirtäminen suoraan rekisterinpitäjältä toiselle edellyttäen, että se on teknisesti mahdollista. Ennen tietojen luovuttamista toiselle rekisterinpitäjälle, kaupungin on varmistettava, että toinen rekisterinpitäjä toimii rekisteröidyn puolesta. Kaupunki ei ole kuitenkaan vastuussa toisen rekisterinpitäjän suorittamasta käsittelystä.

Oikeus siirtää tiedot järjestelmästä toiseen koskee vain rekisteröidyn toimittamia tietoja. Henkilötiedot, jotka on johdettu tai päätelty rekisteröidyn toimittamista tiedoista, eivät kuulu tietojen siirtämistä koskevan oikeuden soveltamisalaan.

Mikäli kaupunki vastaanottaa siirto-oikeuden perusteella luovutettuja tietoja, sen on huolehdittava siitä, että kyseisten tietojen käsittelylle on asetuksen mukainen peruste eli tietojen on oltava palvelun kannalta olennaisia ja tarpeellisia. Jos tietojen käsittelylle ei ole perustetta, tiedot tulee viivytyksettä poistaa järjestelmistä.

Se, että rekisteröity käyttää siirto-oikeuttaan, ei rajoita hänen oikeutta poistaa tietoja tai muita oikeuksia. Näin ollen siirto-oikeuden käyttämisen jälkeen kaupungilla on oikeus käsitellä henkilön tietoja normaalisti, mikäli tietojen käsittelylle on edelleen olemassa jokin asetuksessa todettu peruste. Tietojen siirtäminen järjestelmästä toiseen ei tarkoita kuitenkaan sitä, että kaupunki olisi velvollinen säilyttämään henkilötietoja pidempään kuin on tarpeen tai määritellyn säilytysajan jälkeen.

Vastustamisoikeus

Henkilöllä on oikeus henkilökohtaiseen, erityiseen tilanteeseensa perustuen milloin tahansa vastustaa henkilötietojensa käsittelyä silloinkin, kun käsittely perustuu yleistä etua koskevan tehtävän suorittamiseen tai kaupungille kuuluvan julkisen vallan käyttämiseen. Sama oikeus on silloin, kun käsittely perustuu rekisterinpitäjän tai kolmannen osapuolen oikeutettuun etuun.

Tässä tapauksessa tietoja voidaan käsitellä edelleen vain, jos käsittelyyn on olemassa huomattavan tärkeä ja perusteltu syy, jonka kaupunki voi osoittaa. Käsittelyä saa jatkaa myös, jos käsittely on tarpeen oikeusvaateen laatimiseksi, esittämiseksi tai puolustamiseksi.

Vastustamisoikeutta ei ole, kun henkilötietojen käsittely perustuu kaupungin lakisääteiseen velvoitteeseen. Henkilötietojen käsittelyä ei siten voi vastustaa esimerkiksi, kun on kysymys koulun oppilaista tai varhaiskasvatuksessa olevista lapsista ja heidän huoltajistaan pidettävästä rekisteristä.

Oikeus riitauttaa automaattinen yksittäispäätös

Henkilöllä on oikeus olla joutumatta automaattiseen henkilötietojen käsittelyyn perustuvan päätöksen kohteeksi, jos päätöksestä aiheutuu hänelle oikeudellisia vaikutuksia tai se vaikuttaa häneen muulla vastaavalla tavalla merkittävästi. Tällaista automaattista päätöksentekoa on esimerkiksi henkilötietojen profilointi, kuten henkilötietojen automaattiseen käsittelyyn perustuva online-luottohakemuksen epääminen tai sähköisen rekrytoinnin käytännöt ilman ihmisen osallistumista.

Oikeus tehdä valitus valvontaviranomaiselle

Henkilöllä, jonka henkilötietoja on kaupungin henkilörekistereissä, on oikeus tehdä valitus valvontaviranomaiselle, jos hän katsoo, että häntä koskevien henkilötietojen käsittelyssä rikotaan EU:n yleistä tietosuoja-asetusta. Suomessa tämä valvontaviranomainen on tietosuojavaltuutettu. Tämän lisäksi henkilöllä on oikeus käyttää muita hallinnollisia muutoksenhakukeinoja sekä oikeussuojakeinoja.

EU:n yleinen tietosuoja-asetus (EU) 2016/679:
12 art., 15 art., 16 art., 17 art., 18 art., 20 art., 21 art., 22 art., 77 art.

11. Tietoturva

Kukin toimiala, virasto ja liikelaitos vastaa itse siitä, että tietoturvan taso niiden rekistereissä on riittävä. Asianmukaisen turvallisuustason arvioimisessa on kiinnitettävä huomiota käsittelyn sisältämiin riskeihin, erityisesti siirrettyjen, tallennettujen tai muutoin käsiteltyjen henkilötietojen vahingossa tapahtuvan tai laittoman tuhoamisen, häviämisen, muuttamisen, luvattoman luovuttamisen tai henkilötietoihin pääsyn vuoksi. Turvatoimia arvioitaessa on otettava huomioon käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset. Lisäksi on huomioitava uusin tekniikka ja toteuttamiskustannukset.

Rekisterinpitäjän ja käsittelijän, esimerkiksi ostopalvelun tuottajan tai järjestelmätoimittajan, on sovittava siitä, että käsittelijä käsittelee henkilötietoja ainoastaan rekisterinpitäjän antamien dokumentoitujen ohjeiden mukaisesti. Tämän vuoksi rekisterinpitäjän on sopimuksenteon yhteydessä annettava erillinen ohjeistus edellytetystä tietoturvan tasosta.

11.1 Helsingin tietoturvan ohjeet toimittajalle

Sopimukseen liittyvät työtavat ja tietoturvajärjestelyt tulee antaa toimittajalle. Ne voidaan liittää sopimukseen omana asiakirjanaan. Tällainen asiakirja voi olla esimerkiksi järjestelmän vaatimusdokumentti, tietoturvasuunnitelma tai palveluun liittyvä työohje.

Mikäli palvelulle tai järjestelmälle ei ole sopimuksen solmimisen yhteydessä käytettävissä nimenomaan tätä solmittavaa sopimusta varten toimitettua tietoturvan ohjetta, niin ohjeen voi laatia soveltamalla Helsingin yleisiä tietoturvan ohjeita toimittajille. Se soveltuu tietoturvan yleiseksi ohjeeksi palvelu- tai järjestelmätoimittajalle. Asiakirja tulee lukea läpi ennen sopimukseen liittämistä ja muokata tarvittaessa. Asiakirjan sisältö saattaa soveltua toimittajan ohjeeksi ilman muokkaustakin, mutta se sisältää vain yleisellä tasolla olevia toimintaohjeita.

Yleisiin ohjeisiin tulee lisätä ainakin toimittajayrityksen tiedot, erityisesti yhteystiedot palveluseurantaa varten. Palveluseurantaa varten tarvittavat Helsingin ja toimittajan henkilöiden yhteystiedot voi liittää sopimukseen omana liitesivunaankin, jolloin niitä voi olla helpompi pitää ajan tasalla sekä julkaista niitä tarvitseville. Palveluseurantaa varten tarvittavia yhteystietoja voivat olla ainakin tietosuojailmoituksiin, tietoturvailmoituksiin ja palvelun kehittämiseen liittyvät nimi, tehtävänimike, osoite, sähköposti ja puhelinnumero.

Yleisiä tietoturvan ohjeita kannattaa tarkentaa sopimuskohtaisesti kuvaamalla sopimukseen liittyvät käytössä olevat tarkat työtavat. Tarkkoja työtapoja voivat olla esimerkiksi, kuinka tietoja käytännössä siirretään Helsingin ja palvelutoimittajan välillä, millaisia tietoliikenne-, palomuuri-, haitta-ohjelma- tai päivitysjärjestelyjä vaaditaan, miten tiedot tulee hävittää ja kuinka pidetään käyttökirjanpitoa tietojen käsittelystä (lokeja).

Kirjallinen kuvaus tietoturvan yleisistä ohjeista voi olla julkinen asiakirja.

Kirjallinen kuvaus tietoturvan yleisistä ohjeista voi olla julkinen asiakirja. Sujuvan toiminnan kannalta yleensä onkin perusteltua toimittaa tietoturvan yleiset ohjeet toimittajalle sellaisena, että ne eivät tarvitse salassa pitoa. Palveluseurantaa varten tarvittavat yhteystiedot taas eivät välttämättä ole tarpeen saattaa vapaasti saataville, vaan ainoastaan työssään tarvitseville.

Myös tarkat tekniset ratkaisut voivat vaatia salassa pitoa. Salassa pidon peruste voi olla esimerkiksi henkilöiden, rakennusten tai tieto- ja viestintäjärjestelmien turvajärjestelyjä koskevat yksityiskohdat, silloin kun tieto niistä vaarantaa turvajärjestelyjen tarkoituksen.

11.2 Tietoturvaan liittyvät tehtävät ja tietoturvajärjestelyt

Tarkkoja tietoturvaan liittyviä järjestelyjä (tietoturvakontrolleja) ovat erilaiset suunnitelmat, työmenetelmät ja tekniset ratkaisut. Tietoturvakontrollit kuvataan tyypillisesti järjestelmän vaatimusdokumentissa, tietoturvasuunnitelmassa tai palveluun liittyvässä työohjeessa.

Mikäli sopimuksen solmimisen ajankohtana ei ole käytettävissä jo olemassa olevaa asiakirjaa, jossa tietoturvaan liittyvät järjestelyt ovat tarkasti kuvattu, niin tietoturvakontrollit voi kuvata soveltamalla Helsingin yleisiin tietoturvan ohjeisiin liittyvää tietoturvaan liittyvien tehtävien ja tietoturvajärjestelyiden taulukkoa. Taulukkoa voi käyttää myös arvioimaan tietoturvajärjestelyiden riittävyyttä.

Taulukossa luetellaan eri työvaiheita ja millaisia tietoturvaan liittyviä tehtäviä niissä kuuluisi tehdä. Noudattamalla työvaiheiden tehtäväluetteloa palvelun tai järjestelmän tietoturvajärjestelyt tulevat toteutetuksi.

Tehtäväluettelossa kuvataan mitä tulisi tehdä. Kun tehtävä saadaan tehtyä, on syntynyt jokin tietoturvaan liittyvä vaihetuote tai toimenpide. Esimerkiksi, kun tehdään sovelluksen riskianalyysi, niin sen seurauksena tietoihin liittyvät riskit on saatu kuvatuksi. Tai kun suoritetaan tietoturvavaatimusten dokumentointi, niin on saatu aikaan kirjallinen kuvaus tarvittavista tietoturvajärjestelyistä. Käyttöoikeustasojen ja kirjautumisratkaisujen määrittelyn tekeminen johtaa sopivan teknisen tietoturvajärjestelyn valintaan.

Erilaisia tehtäviä on lueteltu useita kymmeniä. Taulukko on tiivistetty VAHTI-ohjeisiin sisältyvistä vielä laajemmista taulukoista. VAHTI-ohjeiden taulukoiden avulla voi siis tehdä vastaavan tarkastelun. Esimerkiksi VAHTI 3/2012 teknisen ympäristön tietoturvataso-ohje sisältää liitteinään vielä laajempia taulukoita erilaisista tietoturvajärjestelyistä (mm. liite 3: TTT – Tietojärjestelmien hallinnan vaatimukset).

Tietoturvaan liittyvien tehtävien taulukkoa voi hyödyntää siten, että sen avulla tarkistetaan, ovatko kaikki palvelun tai järjestelmän kannalta tarpeelliset tietoturvajärjestelyt tehty. Varsinaiset tietoturvajärjestelyiden tekniset kuvaukset tulee löytyä palvelun tai järjestelmän dokumentaatiosta.

Tietoturvaan liittyvien tehtävien taulukkoa voi muokata sopimukseen paremmin soveltuvaksi. Esimerkiksi Suositus-sarakkeen suosituksia voi muuttaa sopimuksen kannalta parhaiten sopiviksi.

Tietoturvaan liittyvien tehtävien taulukko voi olla julkinen asiakirja jopa arvio-sarake täytettynä, sillä kyse on varsin yleisen tasoisesta tiedosta. Tietoturvajärjestelyiden tarkat kuvaukset taas voivat olla rajoitettu vain niitä työssään tarvitseville. Salassa pidon peruste voi olla esimerkiksi henkilöiden, rakennusten tai tieto- ja viestintäjärjestelmien turvajärjestelyjä koskevat yksityiskohdat.

Tietoturvaan liittyvien tehtävien taulukon sarakkeet ovat seuraavat:

TYÖVAIHE	Työvaiheet ovat esiselvitys, vaatimusmäärittely, hankinta, suunnittelu, järjestelmätoteutus, testaus ja laadunvarmistus, ylläpito ja tuotantokäyttö sekä käytöstä poisto. Lisäksi taulukon lopussa on kohta erityisvaatimuksille, jos sellaisia tulee. Jos palvelua tai järjestelmää tuotetaan ketterillä menetelmillä, niin tehtäviä suoritetaan toisteisesti. Tällöin taulukkoa voidaan käyttää pitkin matkaa tukena eri vaiheiden toteutumisen seurantaan. Ketterilläkin menetelmillä tulee loppujen lopuksi kaikki työvaiheet läpikäydyksi. Ketterästi tehdyn järjestelmän tietoturvajärjestelyt tulee joka tapauksessa olla asianmukaiset järjestelmän luonnostelusta, tuotantoon otosta, käyttöön ja poistoon.
TEHTÄVÄ-KOKONAISUUS	Työvaiheita on jaoteltu tehtäväkokonaisuuksiksi. Tämä helpottaa jäsentämään, mitä kaikkia tehtäviä on tarpeen tehdä.
TEHTÄVÄ	Tehtäväkokonaisuudet sisältävät useita varsinaisia tehtäviä, jotka tulee tehdä tietoturvajärjestelyiden aikaan saamiseksi.
KUVAUS	Tehtävien kuvauksissa kerrotaan tiivistetysti, millaisia asioita odotetaan tehtävän. Kuvauksen mukaisen tehtävän suorittaminen voidaan joko osoittaa palvelun tai järjestelmän dokumentaatioon liittyvällä kirjauksella tai tehdyillä toimenpiteillä. Työvaiheen ja tehtäväkokonaisuuden kuvaus antaa yleiskuvan siitä, mitä siihen liittyvillä tehtävillä tavoitellaan.
SUOSITUS	Suositus-sarakkeessa on ehdotettu kutakin tehtävää joko pakolliseksi, vahvasti suositelluksi tai valinnaiseksi. Pakolliseksi suositeltu tehtävä on yleensä kaikkien palveluiden ja järjestelmien yhteydessä todella hyödyllinen tehtävä, jotta tietoturvajärjestelyt tulevat toteutettua riittävän huolellisesti. Erittäin huolellista työtä tehtäessä sekä vahvasti suositellut että valinnaiset kohdat käydään läpi. Tällöin tietoturvajärjestelyt tulevat suurella varmuudella olemaan riittävät.
ARVIO	Arvio-sarakkeen avulla voidaan mitata tehtävien suorittamista ja niistä toteutuneita tietoturvajärjestelyjä. Tyhjä solu tarkoittaa, että asiaa ei ole arvioitu. Solun arvoilla on seuraava merkitys. 2 Tehtävään liittyvä asia on todettu olevan kunnossa. 1 Asia on osittain kunnossa, mutta ei aivan tyydyttävällä tavalla. 0 Asia ei ole kunnossa, se vaatii vielä tekemistä.

Kun henkilötietoja tulostetaan yhteiskäyttöiselle tulostimelle, pitää käyttää turvatulostusta. Silloin paperit tulostuvat vasta sitten, kun tulostimelle antaa laitteen äärellä tulostusluvan.

11.3 Oman työn tietoturvallisuus

Henkilötietoja sisältäviä papereita ja muita tallenteita tulee aina käsitellä huolellisesti. Niitä ei saa jättää avoimesti saataville pöydälle tai laittaa tavalliseen roskakoriin. Henkilötietoja sisältävät paperit tulee hävittää laittamalla ne lukolliseen tietosuojaroskikseen tai silppuriin.

Työasema tulee lukita, kun sen äärestä poistutaan, jotta työntekijän käyttäjätunnuksilla saatavilla olevia henkilötietoja eivät näe muut kuin kyseinen työntekijä. Työasemaa käyttäessä tulee myös huolehtia, että sivullinen ei näe työasemalla käsiteltäviä henkilötietoja. Sama koskee kaikenlaisia tietoteknisiä laitteita, kuten tablettitietokoneita tai älypuhelimia.

Kun henkilötietoja tulostetaan yhteiskäyttöiselle tulostimelle, pitää käyttää turvatulostusta. Silloin paperit tulostuvat vasta sitten, kun tulostimelle antaa laitteen äärellä tulostusluvan.

Henkilötiedoista puhuttaessa tulee olla huolellinen, tapahtuipa keskustelu kasvokkain, puhelimessa tai verkkokokouksessa. Henkilötiedot eivät saa päätyä ulkopuolisten tietoon. Ulkopuolisia ovat sellaiset henkilöt, joiden tehtäviin kyseisten henkilötietojen käsittely ei kuulu.

Jos jostain poikkeuksellisesta syystä henkilötietoja joutuu tallentamaan siirrettävälle muistilaitteelle (esimerkiksi muistitikulle) tai yleiskäyttöiselle muulle muistialueelle, pitää tiedot tallentaa salakirjoitettuna. Henkilötietojen käsittelyn tulee kaikissa tapauksissa olla käyttötarkoituksen mukaista, myös silloin kun niitä jostain syystä joudutaan tallentamaan muistivälineille. Tallenteet tulee tuhota asianmukaisesti.

Työsopimuslomakkeessaan työntekijä allekirjoituksellaan sitoutuu työsuhteen aikana ja sen päätyttyä olemaan ilmaisematta sivullisille salassa pidettäviä tietoja kuten henkilön perhe-elämää tai muita henkilökohtaisia oloja koskevia tietoja. Sitoutuminen siis kattaa tietosuojaa koskevan huolellisuusvelvoitteen jokaiselle hänen omissa töissään.

Työnantajan vastuulla on, että esimies järjestää työntekijälle henkilötietojen käsittelyyn liittyvät käyttöoikeudet ja osoittaa töihin soveltuvat tietoturvalliset välineet sekä riittävän koulutuksen. Käyttöoikeudet tulee poistaa, kun tehtävien muuttuttua niitä ei enää tarvita. Kaikkien käyttäjätunnusten ajanmukaisuus tulee määräajoin tarkastaa.

Laki viranomaisten toiminnan julkisuudesta (621/1999): 24 §, kohta 7

12. Tietopyyntöjen käsittely

12.1 Henkilötietojen pyytäminen ja oikaisuvaatimus

Rekisteröidyllä on oikeus saada kaupungilta tiedot siitä, käsitelläänkö hänen henkilötietojaan ja mitä henkilötietoja käsitellään. Lisäksi hänellä on oikeus vaatia, että häntä koskevat virheelliset tiedot oikaistaan. Rekisteröidyn oikeuksista kerrotaan lisää luvussa 10.

Rekisteröity voi pyytää jäljennökset omista tiedoistaan sekä vaatia virheellisten tietojen korjaamista joko sähköisesti kaupungin internetsivuilla tai palauttamalla paperilomake kaupungin kirjaamoon tai erikseen määriteltyjen toimialojen palvelupisteisiin. Jos rekisteröity esittää oikeutta koskevan pyynnön sähköisesti, tiedot on toimitettava sähköisessä muodossa, paitsi jos rekisteröity pyytää toimittamaan tiedot muussa muodossa.

Rekisteröidyllä on oikeus saada kaupungilta tiedot siitä, käsitelläänkö hänen henkilötietojaan ja mitä henkilötietoja käsitellään.

12.2 Tietopyyntöjen käsittelyn sähköinen prosessi

Asiakas kirjautuu asiointi.hel.fi-sivuille suomi.fi:n vahvaa tunnistautumista käyttäen ja täyttää lomakkeen tietojensa pyytämiseksi tai vaatimukseksi tietojensa korjaamiseksi.

Toimialan, viraston tai liikelaitoksen tietopyyntöjen kokoaja (sähköpostiosoite, jolla on useampi nimetty käyttäjä) saa sähköpostiin herätteen tietopyynnön saapumisesta. Hän lukee pyynnön asioinnin virkailijakansiossa ja kopioi pyynnön tiketöintijärjestelmään ja tekee alitiketit kunkin pyynnön kohteena olevan rekisterin vastuuhenkilölle.

Rekisterin vastuuhenkilö saa herätteen, lukee pyynnön ja asettaa vastuutahoksi alitiketille rekisterin yhteyshenkilön.

Rekisterin yhteyshenkilö saa herätteen alitiketistä. Hän noutaa tiedot rekisteristä ja kopioi tiedot alitikettiin. Hän päivittää alitiketin statuksen ja asettaa alitiketin vastuuhenkilöksi rekisterin vastuuhenkilön.

Rekisterin vastuuhenkilö saa herätteen ja tarkastaa tiedot. Jos tiedot ovat oikein, hän asettaa alitiketin vastuutahoksi tietopyyntöjen kokoajan. Jos tiedot eivät ole oikein, rekisterin vastuuhenkilö asettaa uudelleen vastuutahoksi rekisterin yhteyshenkilön, jotta tämä huolehtii siitä, että lähtevät tiedot ovat oikein.

Tietopyyntöjen kokoaja saa herätteen, kerää tiedot mahdollisista useista alitiketeistä ja koostaa vastauksen. Hän joko kopioi vastauksen asiointiin tai toimittaa tiedot suojatulla sähköpostilla.

Asiakas saa herätteen saapuneesta vastauksesta. Hän pääsee lukemaan tiedot asioinnista tai suojatusta sähköpostista.

Kun kyseessä on asiakkaan tekemä tietojen korjausvaatimus, toimitaan vastaavalla tavalla kuin tietopyyntöprosessissa.

12.3 Tietopyyntöjen käsittelyn paperiprosessi

Asiakas täyttää henkilötietojen tarkastuspyyntö- tai korjausvaatimuslomakkeen, jonka hän saa kirjaamosta tai tulostamalla lomakkeen kaupungin verkkosivuilta.

Asiakas tuo henkilökohtaisesti lomakkeen Helsingin kirjaamon asiakaspalveluun tai toimialan ilmoittamaan palvelupisteeseen.

Kirjaamo tarkastaa asiakkaan henkilöllisyyden ja kuittaa tarkastamisen asiakkaan täyttämälle lomakkeelle. Lisäksi kirjaamo kuittaa lomakkeelle vastaanottomerkinnät päivämäärätietoineen ja skannaa saapuneen lomakkeen PDF-muotoon.

Kirjaamo lähettää skannatun lomakkeen suojatulla sähköpostilla toimialan, viraston tai liikelaitoksen tietopyyntöjen kokoajan sähköpostiin.

Toimialalla, virastossa tai liikelaitoksessa tietopyyntöjen kokoaja vastaanottaa suojatun sähköpostin, jonka liitteenä on henkilötietojen tarkastuspyynnön tai korjausvaatimuksen lomake. Hän kopioi pyynnön tiketöintijärjestelmään ja tekee alitiketit kunkin pyynnön kohteena olevan rekisterin vastuuhenkilölle.

Rekisterin vastuuhenkilö lukee pyynnön kuvauksen ja asettaa vastuutahoksi alitiketille rekisterin yhteyshenkilön.

Rekisterin yhteyshenkilö saa herätteen alitiketistä. Hän noutaa tiedot rekisteristä ja kopioi tiedot alitikettiin. Hän päivittää alitiketin statuksen ja asettaa alitiketin vastuuhenkilöksi rekisterin vastuuhenkilön.

Rekisterin vastuuhenkilö saa herätteen ja tarkastaa tiedot. Jos tiedot ovat oikein, hän asettaa

alitiketin vastuutahoksi tietopyyntöjen kokoajan. Jos tiedot eivät ole oikein, rekisterin vastuuhenkilö asettaa uudelleen vastuutahoksi rekisterin yhteyshenkilön, jotta tämä huolehtii siitä, että lähtevät tiedot ovat oikein.

Tietopyyntöjen kokoaja saa herätteen, kerää tiedot mahdollisista useista alitiketeistä ja koostaa vastauksen.

Tietopyyntöjen kokoaja toimittaa tiedot asiakkaalle tämän pyytämällä tavalla. Asiakas voi pyytää tietojaan sähköisesti, suojatulla sähköpostilla tai kirjeellä. Asiakas voi myös haluta noutaa tiedot, jolloin tietopyyntöjen kokoaja lähettää tiedot postitse kirjaamoon. Jos asiakas haluaa noutaa tiedot kirjaamosta tai muusta asiakaspalvelupisteestä, tietopyyntöjen kokoaja ilmoittaa asiakkaalle tietopyynnön valmistumisesta ja ajankohdasta, milloin tiedot ovat noudettavissa.

Asiakkaan tullessa noutamaan tietojaan kirjaamosta tai toimialan palvelupisteestä, kirjaamo tai palvelupiste tarkistaa asiakkaan henkilöllisyyden ja luovuttaa asiakkaalle hänen tietonsa.

Kun kyseessä on asiakkaan tekemä tietojen korjausvaatimus, toimitaan vastaavalla tavalla kuin tietopyyntöprosessissa.

12.4 Tietojen luovutus ja korjaaminen sekä niistä kieltäytyminen

Asiakkaan pyytämät tiedot tulee toimittaa hänelle ilman aiheetonta viivytystä ja joka tapauksessa kuukauden kuluessa pyynnön vastaanottamisesta. Myös asiakkaan vaatimat korjaukset tulee tehdä ilman aiheetonta viivytystä ja viimeistään kuukauden kuluessa vaatimuksen vastaanottamisesta. Määräaikaa voidaan tarvittaessa jatkaa enintään kahdella kuukaudella ottaen huomioon pyyntöjen monimutkaisuus ja määrä. Jos määräaikaa jatketaan, asiakkaalle tulee ilmoittaa asiasta kuukauden kuluessa vaatimuksen vastaanottamisesta sekä myös syy viivästymiselle tulee ilmoittaa. Samalla tulee kertoa, että asiakkaalla on oikeus tehdä valitus tietosuojavaltuutetulle ja käyttää muita oikeussuojakeinoja.

Jollei kaupunki hyväksy tietopyyntöä, kaupungin on ilmoitettava tästä kirjallisesti pyytäjälle. Ilmoituksessa on mainittava myös ne syyt, joiden vuoksi tietotopyyntöä ei ole hyväksytty. Lisäksi on kerrottava mahdollisuudesta saattaa asia tietosuojavaltuutetun käsiteltäväksi ja käyttää muita oikeussuojakeinoja. Ilmoitus on annettava kuukauden kuluessa pyynnön vastaanottamisesta. Ilmoituksen antaa rekisterin vastuuhenkilö.

Omat tiedot on oikeus saada maksutta. Jos henkilö kuitenkin pyytää useampia jäljennöksiä, kaupunki voi periä niistä hallinnollisiin kustannuksiin perustuvan kohtuullisen maksun.

Omat tiedot on oikeus saada maksutta. Jos henkilö kuitenkin pyytää useampia jäljennöksiä, kaupunki voi periä niistä hallinnollisiin kustannuksiin perustuvan kohtuullisen maksun. Jos tietopyynnöt ovat ilmeisen perusteettomia tai kohtuuttomia ja jos niitä esitetään toistuvasti, kaupunki voi periä kohtuullisen maksun tai kieltäytyä suorittamasta pyydettyä toimenpidettä. Tällaisissa tapauksissa kaupunki osoittaa pyynnön ilmeisen perusteettomuuden tai kohtuuttomuuden.

Jäljennöksen toimittaminen rekisteröidyn henkilötiedoista ei saa vaikuttaa haitallisesti muiden oikeuksiin ja vapauksiin. Rekisteröidylle ei tarvitse antaa esimerkiksi sellaisia tietoja, jotka ovat liikesalaisuuksia tai sisältävät myös muiden henkilöiden henkilötietoja.

Tietojen tarkastusoikeus ei ole rajoittamaton. Rekisteröidyllä ei esimerkiksi ole oikeutta tutustua hänestä kerättyihin tietoihin, jos tiedon antaminen saattaisi vahingoittaa kansallista turvallisuutta, puolustusta tai yleistä järjestystä ja turvallisuutta, haitata rikosten ehkäisemistä tai selvittämistä, tai tiedon antamisesta saattaisi aiheutua vakavaa vaaraa rekisteröidyn terveydelle tai hoidolle tai rekisteröidyn tai jonkun muun oikeuksille. Tällöin rekisteröidylle ilmoitetaan syyt siihen, miksi hänen tietojaan ei luovuteta, ellei tämä vaaranna rajoituksen tarkoitusta. Rekisteröidylle tulee myös kertoa hänen mahdollisuudestaan tehdä valitus tietosuojavaltuutetulle ja käyttää muita oikeussuojakeinoja.

EU:n yleinen tietosuoja-asetus (EU) 2016/679: 15 art., 16 art., 77 art.

13. Tietoturva-loukkauksista ilmoittaminen

13.1 Henkilötietojen tietoturvaloukkaus

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, kadonnut henkilötietoja sisältävä paperi, omaan työhön kuulumattomien henkilötietojen katselu, kadonnut muistitikku, varastettu tietokone tai murtautuminen henkilötietoja sisältävään järjestelmään.

Henkilötietojen tietoturvaloukkauksia ovat esimerkiksi tietojen lähettäminen väärälle henkilölle, kadonnut henkilötietoja sisältävä paperi, omaan työhön kuulumattomien henkilötietojen katselu, kadonnut muistitikku, varastettu tietokone tai murtautuminen henkilötietoja sisältävään järjestelmään

13.2 Tietoturvaloukkauksesta ilmoittamisen prosessi

Kuka tahansa kaupungin työntekijä, asiakas tai palveluntuottaja, voi havaita tietoturvaloukkauksen. Kun kaupungin työntekijä saa tiedon loukkauksesta, on hänen ilmoitettava siitä välittömästi omalle esimiehelleen sekä oman organisaation tietosuojan vastuuhenkilölle.

Esimiehen tehtävänä on ilmoittaa asiasta oman organisaationsa tietosuojan vastuuhenkilölle.

Tietosuojan vastuuhenkilö arvioi, onko kyseessä oleva loukkaus todellinen henkilötietoihin kohdistunut tietoturvaloukkaus vai ei. Jos on, on hänen ilmoitettava asiasta välittömästi tietosuojavastaavalle ja apulaistietosuojavastaavalle. Mikäli loukkaus liittyy järjestelmässä olevaan haavoittuvuuteen, ilmoittaa tietosuojan vastuuhenkilö asiasta myös oman organisaationsa tietoturvasta vastaavalle henkilölle. Jos tietoturvaloukkaus edellyttää harkitsemaan työoikeudellisia kurinpitotoimia, tutkintapyynnön tekemistä poliisille tai jos kaupungille on esitetty vahingonkorvausvaatimus, konsultoidaan kaupunginkanslian oikeuspalveluita.

Kun kaupungin työntekijä saa tiedon tietoturvaloukkauksesta, on hänen ilmoitettava siitä välittömästi omalle esimiehelleen sekä oman organisaation tietosuojan vastuuhenkilölle.

Tietoturvasta vastaava henkilö selvittää asiaa ja ryhtyy toimenpiteisiin vahingon minimoimiseksi, mikäli tietosuojan vastuuhenkilö on ollut häneen yhteydessä. Mikäli tietoturvasta vastaava henkilö havaitsee järjestelmähaavoittuvuuden tai muun tietoturvapoikkeaman, tulee hänen ilmoittaa asiasta oman organisaationsa tietosuojan vastuuhenkilölle. Tietoturvasta vastaava henkilö ilmoittaa tarvittaessa Liikenne- ja viestintäviraston (Traficomin) Kyberturvallisuuskeskukselle tapahtuneesta tietoturvaloukkauksesta, kuten tietojenkalastelusta tai palvelunestohyökkäyksestä.

Tietosuojavastaava ja apulaistietosuojavastaava arvioivat tapahtuneen loukkauksen ja pyytävät tarvittaessa lisätietoa tietosuojan vastuuhenkilöltä. Jos tapahtuneesta tietoturvaloukkauksesta aiheutuu rekisteröidyn oikeuksille ja vapauksille riski, ilmoittaa tietosuojavastaava tai apulaistietosuojavastaava asiasta tietosuojavaltuutetulle, kaupungin johdolle ja viestintään sekä tarvittaessa oikeuspalveluihin. Viestintä ryhtyy tarvittaessa kriisiviestintätoimenpiteisiin kriisiviestintäprosessin mukaisesti. Jos tietosuojavastaava ja apulaistietosuojavastaava arvioivat tapahtuneen loukkauksen aiheuttavan korkean riskin rekisteröidyn oikeuksille, ovat he yhteydessä tietosuojan vastuuhenkilöön ja pyytävät häntä ilmoittamaan tapahtuneesta rekisteröidylle.

13.3 Tietoturvaloukkauksesta ilmoittaminen tietosuojavaltuutetulle

Tietosuojavastaava tai apulaistietosuojavastaava ilmoittaa tietoturvaloukkauksesta tietosuojavaltuutetulle, jos loukkauksesta voi aiheutua riski luonnollisten henkilöiden oikeuksille ja vapauksille. Ilmoitus tehdään ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa siitä, kun loukkaus on tullut ilmi. Jos ilmoitusta ei tehdä 72 tunnin kuluessa, on tietosuojavaltuutetun toimistolle toimitettava perusteltu selitys.

Ilmoituksen on sisällytettävä vähintään seuraavat tiedot:

- kuvaus henkilötietojen tietoturvaloukkauksesta, mukaan lukien mahdollisuuksien mukaan asianomaisten rekisteröityjen ryhmät ja arvioidut lukumäärät sekä henkilötietotyyppien ryhmät ja arvioidut lukumäärät
- tietosuojavastaavan nimi ja yhteystiedot tai muu yhteyspiste, josta voi saada lisätietoa
- kuvaus henkilötietojen tietoturvaloukkauksen todennäköisistä seurauksista
- toimenpiteet, joita rekisterinpitäjä on ehdottanut tai jotka se on toteuttanut henkilötietojen tietoturvaloukkauksen johdosta, tarvittaessa myös toimenpiteet mahdollisten haittavaikutusten lieventämiseksi.

Jos ja siltä osin kuin tietoja ei ole mahdollista toimittaa samanaikaisesti, tiedot voidaan toimittaa vaiheittain ilman aiheetonta viivytystä.

Jos päädytään siihen, että tietoturvaloukkauksesta ei tarvitse ilmoittaa tietosuojavaltuutetulle, dokumentoidaan, millä perusteella ilmoitus on katsottu tarpeettomaksi.

Tietosuojavastaava tai apulaistietosuojavastaava ilmoittaa tietoturvaloukkauksesta tietosuojavaltuutetulle, jos loukkauksesta voi aiheutua riski luonnollisten henkilöiden oikeuksille ja vapauksille.

13.4 Henkilötietojen tietoturvaloukkauksesta ilmoittaminen rekisteröidylle

Toimialan, viraston tai liikelaitoksen, jolla loukkaus on tapahtunut, on ilmoitettava tietoturvaloukkauksesta lähtökohtaisesti myös rekisteröidylle. Ilmoituksen tekemisestä vastaa tietosuojan vastuuhenkilö. Ilmoitus on tehtävä ainoastaan, jos loukkaus todennäköisesti aiheuttaa korkean riskin henkilöiden oikeuksille ja vapauksille, ja tietosuojavastaava tai apulaistietosuojavastaava pyytää ilmoittamaan rekisteröidylle. Rekisteröidylle on ilmoitettava tapahtuneesta tietoturvaloukkauksesta ilman aiheetonta viivytystä, mutta tuntimääräistä aikarajaa ei ole määritelty.

Rekisteröidylle on ilmoitettava:

- selkeä ja yksinkertainen kuvaus tapahtuneesta
- tietosuojavastaavan nimi ja yhteystiedot
- henkilötietojen tietoturvaloukkauksen todennäköiset seuraukset
- yleisen tason kuvaus niistä toimenpiteistä, joita rekisterinpitäjä aikoo toteuttaa tai jotka se on jo toteuttanut haittavaikutusten lieventämiseksi ja tilanteen ratkaisemiseksi
- tieto siitä, että kaupungin tietosuojavastaava tekee ilmoituksen tietosuojavaltuutetun toimistoon, ja että ilmoitus tehdään ilman nimiä.

Jos rekisteröidylle annetaan edellä mainitut tiedot puhelimitse, ne lähetetään hänelle myös postitse, jos rekisteröity tätä toivoo.

Rekisteröidylle annettavassa ilmoituksessa ei saa olla muihin aihepiireihin liittyvää tietoa.

Lähtökohtaisesti ilmoitus on tehtävä suoraan rekisteröidylle. Jos tietoturvaloukkaus kohdistuu suureen henkilömäärään, voidaan loukkauksesta kertoa median välityksellä julkisena tiedonantona tai muuna vastaavana toimenpiteenä.

EU:n yleinen tietosuoja-asetus (EU) 2016/679: 33 art., 34 art.

14. Tietosuojaa koskeva vaikutustenarviointi

14.1 Mikä on vaikutustenarviointi ja mitä se sisältää?

Tietosuojaa koskevan vaikutustenarvioinnin tarkoituksena on tunnistaa, arvioida ja hallita henkilötietojen käsittelyyn liittyviä riskejä. Vaikutustenarvioinnista säädetään tietosuoja-asetuksessa.

Vaikutustenarviointi on toteutettava ennen käsittelyä ja se on aloitettava mahdollisimman aikaisin käsittelytoimen suunnitteluvaiheessa, vaikka kaikki toiminnan osat eivät vielä olisi tiedossa. Sen tekeminen on jatkuva prosessi, ei kertaluonteinen tehtävä.

Tietosuoja-asetuksen mukaan arvioinnin on sisällettävä vähintään:

- järjestelmällinen kuvaus suunnitelluista käsittelytoimista, ja käsittelyn tarkoituksista, mukaan lukien tarvittaessa rekisterinpitäjän oikeutetut edut
- arvio käsittelytoimien tarpeellisuudesta ja oikeasuhteisuudesta tarkoituksiin nähden
- arvio rekisteröityjen oikeuksia ja vapauksia koskevista riskeistä ja
- suunnitellut toimenpiteet riskeihin puuttumiseksi, mukaan lukien suoja- ja turvallisuustoimet ja mekanismit, joilla varmistetaan henkilötietojen suoja ja osoitetaan, että tätä asetusta on noudatettu ottaen huomioon rekisteröityjen ja muiden asianomaisten oikeudet ja oikeutetut edut

Vaikutustenarvioinnin tuloksena syntyy näkemys tarvittavista hallintakeinoista, joita tarvitaan pienentämään riskitasoa ja varmistamaan asetuksen vaatimusten toteuttaminen.

14.2 Milloin vaikutustenarviointi on tehtävä?

Vaikutustenarviointi on tehtävä silloin, kun käsittelystä todennäköisesti seuraa korkea riski ihmisten oikeuksille ja vapauksille.

Yhtä arviointia voidaan käyttää samankaltaisiin vastaavia korkeita riskejä aiheuttaviin käsittelytoimiin.

Vaikutustenarviointi tulee tehdä mahdollisimman aikaisessa vaiheessa, kun suunnitellaan uutta järjestelmää, sovellusta tai palvelua, jossa käsitellään henkilötietoja. Arvioinnin tavoite on arvioida suunniteltujen käsittelytoimien vaikutukset henkilötietojen suojalle.

Vaikutustenarviointi on tehtävä erityisesti silloin, kun:

- ollaan ottamassa käyttöön teknologiaa, jota ei ole aiemmin käytetty
- käsitellään arkaluonteisia tai muuten hyvin henkilökohtaisia tietoja
- käsitellään biometrisiä tietoja
- käsitellään geneettisiä tietoja
- käsitellään henkilöiden sijaintitietoja
- käsitellään henkilötietoja Whistleblowing-tarkoituksiin eli ns. eettisen kanavan tai vihjelinjan yhteydessä
- käsitellään erityisiä henkilötietoryhmiä tieteellistä tai historiallista tutkimustarkoitusta varten
- henkilötietoja käytetään arviointiin ja analysointiin, kuten profilointiin ja ennakointiin
- on kyse automaattisista päätöksistä, joilla on ihmisiä koskevia oikeusvaikutuksia tai jotka vaikuttavat vastaavalla tavalla merkittävästi
- on kyse järjestelmällisestä valvonnasta, jossa käsittelyllä tarkkaillaan, valvontaan ja kontrolloidaan ihmisiä
- käsitellään henkilötietoja laajamittaisesti
- henkilötiedot on yhdistetty, esimerkiksi kahdesta tai useammasta käsittelytoiminnasta, joilla on eri tarkoitus ja/tai eri rekisterinpitäjät, sillä tavoin, että se ylittää rekisteröityjen kohtuulliset odotukset siitä, miten heidän henkilötietojaan käsitellään
- käsitellään heikommassa asemassa olevien ihmisten henkilötietoja
- siirretään henkilötietoja kolmansiin maihin EU:n ulkopuolelle

Vaikutustenarviointi on tehtävä silloin, kun käsittelystä todennäköisesti seuraa korkea riski ihmisten oikeuksille ja vapauksille.

Mitä useammasta kohdasta kyseisessä käsittelyssä on kyse, sitä suurempaa riskiä käsittelystä saattaa aiheutua. EU:n tietosuojatyöryhmän kanta on, että mikäli ainakin kaksi tai useampia arviointikriteerejä täyttyy, tulee vaikutustenarviointi tehdä.

Rekisterinpitäjä voi kuitenkin eräissä tapauksissa katsoa, että vain yhden näistä kriteereistä täyttävä käsittely edellyttää vaikutustenarvioinnin tekemistä. Esimerkiksi jos sairaala käsittelee potilaiden terveystietoja sairaalan tietojärjestelmässä ja tiedot ovat arkaluontoisia, vaaditaan todennäköisesti vaikutustenarviointia.

Käytännössä rekisterinpitäjän on jatkuvasti arvioitava riskejä, joita sen tekemät henkilötietojen käsittelytoimet aiheuttavat. Näin voidaan tunnistaa, milloin tietyntyyppinen käsittely todennäköisesti aiheuttaa ihmisten oikeuksien ja vapauksien kannalta korkean riskin.

Käsittelytoimi voi toisaalta vastata edellä mainittuja tapauksia, ja rekisterinpitäjä voi silti katsoa, ettei se todennäköisesti aiheuta korkeaa riskiä. Näissä tapauksissa rekisterinpitäjän olisi perusteltava ja dokumentoitava syyt, joiden vuoksi se ei tee vaikutustenarviointia. Lisäksi sen olisi sisällytettävä perusteluihin tai kirjattava muulla tavalla tietosuojavastaavan näkemykset.

14.3 Menettely jo käytössä olevien käsittelytoimien osalta

Tietosuoja-asetuksen mukaisia vaikutustenarvioinnin tekemistä koskevia vaatimuksia tulee noudattaa myös niiden käsittelytoimien osalta, jotka ovat käynnistyneet ennen tietosuoja-asetuksen soveltamisen aloittamista (25.5.2018).

Erityisesti, jos käsittelyssä on tapahtunut merkittävä muutos toukokuun 2018 jälkeen, voidaan henkilötietojen käsittely näissä tapauksissa katsoa uudeksi käsittelytoimeksi, joka saattaa vaatia vaikutustenarvioinnin tekemistä. Tällainen muutos voisi olla esimerkiksi uuden teknologian käyttöönotto tai henkilötietojen käyttäminen uutta tarkoitusta varten.

Rekisterinpitäjän on tarvittaessa uudelleentarkasteltava käsittelyä arvioidakseen, tapahtuuko käsittely tietosuojaa koskevan vaikutustenarvioinnin mukaisesti, ainakin jos käsittelytoimien sisältämä riski muuttuu. Ainakin, mikäli henkilötietojen käsittelyyn liittyvä riskiarvio muuttuu, tulee vaikutustenarviointia uudelleen tarkastella.

EU:n tietosuojatyöryhmä suosittaa, että vaikutustenarviointia tulisi päivittää ja uudelleen tarkastella vähintään joka kolmas vuosi tai useamminkin riippuen käsittelyn luonteesta ja muutoksista.

Tietosuoja-asetuksen mukaisia vaikutustenarvioinnin tekemistä koskevia vaatimuksia tulee noudattaa myös niiden käsittelytoimien osalta, jotka ovat käynnistyneet ennen tietosuoja-asetuksen soveltamisen aloittamista (25.5.2018).

14.4 Vaikutustenarvioinnin tekemisen vastuut

Rekisterinpitäjä tekee vaikutustenarvioinnin yhdessä henkilötietojen käsittelijöiden kanssa. Vastuu vaikutustenarvioinnin tekemisestä on sillä toimialalla, virastolla tai liikelaitoksella, jonka rekisteriin suunniteltu käsittely kuuluu. Vaikutustenarviointia tehdessään rekisterinpitäjän on pyydettävä neuvoja tietosuojavastaavalta.

Jos vaikutustenarviointi jätetään tekemättä silloin, kun se olisi tullut tehdä, voi tietosuojavaltuutetun mukaan olla kyseessä rikoslain mukainen tietosuojarikkomus.

14.5 Tietosuojavaltuutetun ennakkokuuleminen korkean jäännösriskin tapauksessa

Rekisterinpitäjän on ennen henkilötietojen käsittelyä kuultava tietosuojavaltuutettua, jos vaikutustenarviointi osoittaa, että käsittely aiheuttaisi korkean riskin, ja jos rekisterinpitäjä ei ole toteuttanut toimenpiteitä riskin pienentämiseksi.

Jos siis vaikutustenarvioinnissa esiin tulleisiin riskeihin ei omilla riskienhallinnan toimenpiteillä pystytä vaikuttamaan, mutta käsittelyä haluttaisiin silti alkaa tehdä, on tietosuojavaltuutetun ennakkokuuleminen pakollinen. Käsittelyä ei saa aloittaa ennen tietosuojavaltuutetun kirjallisia ohjeita ennakkokuulemisen johdosta.

Kaupungin tietosuojavastaava antaa loppuarvionsa valmistuneesta vaikutustenarvioinnista ja toimii yhteyspisteenä tietosuojavaltuutetun toimistoon päin eli lähettää valmistuneen vaikutustenarvioinnin ja oman loppuarvionsa tietosuojavaltuutetun toimistoon.

14.6 Helsingin kaupungin vaikutustenarvioinnin työkalut

14.6.1 Alkukartoitus

Vaikutustenarvioinnin alkukartoitus tulee tehdä aina, kun ryhdytään suunnittelemaan uutta prosessia, järjestelmähankintaa tai järjestelmän rakentamista kaupungin omassa järjestelmäkehityksessä.

Alkukartoitus on tehtävä myös silloin, kun suunnitellaan merkittäviä muutoksia olemassa oleviin prosesseihin ja järjestelmiin.

Alkukartoituksessa selvitetään ensin, käsitelläänkö henkilötietoja.

Jos henkilötietoja käsitellään, alkukartoituksen kysymyksiin vastaamalla selviää, tuleeko tehdä vaikutustenarviointi vai ottaa tietosuoja kehittämisessä huomioon tietosuojan tarkistuslistan avulla.

14.6.2 Vaikutustenarvioinnin työkalu

Jos alkukartoitus on osoittanut, että vaikutustenarviointi tulee tehdä, otetaan käyttöön vaikutustenarviointityökalu.

Vaikutustenarvioinnin tekemisessä on havaittu hyväksi työpajamenetelmä, jossa pidetään ensin alkukokous, johon kutsutaan tarvittavat asiantuntijat. Alkukokouksessa sovitaan vastuunjaosta. Alkukokouksen jälkeen olevassa vaikutustenarvioinnin työpajassa (tai työpajoissa) asiantuntijat ovat jo ennakkoon selvittäneet vastuualueillaan olevia asioita, jolloin tietojen dokumentointi työkaluun voidaan tehdä yhteisesti. Aineisto kaikkiin työpajoihin pitää saada hyvissä ajoin asiantuntijoiden tutustuttavaksi.

Vaikutustenarvioinnin työkalu on jaettu kolmeen eri osa-alueeseen:

1. järjestelmällinen kuvaus suunnitelluista käsittelytoimista
2. henkilötietojen käsittelyn tarpeellisuuden ja oikeellisuuden arviointi
3. rekisteröidyn oikeuksille aiheutuvien riskien arviointi.

Kuhunkin osa-alueeseen liittyy tietosuojavaatimuksia, joiden toteutumista arvioidaan työkalun avulla.

Vastuu vaikutustenarvioinnin tekemisestä on sillä toimialalla, virastolla tai liikelaitoksella, jonka rekisteriin suunniteltu käsittely kuuluu.

14.6.3 Vaikutustenarvioinnin riskianalyysi

Kun tehdään vaikutustenarviointia sille tarkoitetulla työkalulla, samalla käytetään riskianalyysilomaketta riskien vaikuttavuuden ja todennäköisyyden arvioimiseen sekä riskien hallintatoimenpiteiden dokumentoimiseen ja seuraamiseen.

Riskianalyysiin kirjataan tunnistetut riskit riskiluokittain, näiden todennäköisimmät seuraukset riskin toteutuessa sekä arvio riskin seurausten vakavuudesta ja toteutumisen todennäköisyydestä.

Riskianalyysissä on keskeistä tunnistaa riskin toteutumiseen johtavat tekijät tai tapahtumaketjut, joihin hallintatoimenpiteillä pyritään vaikuttamaan.

Tunnistetuille riskeille määriteltyjen hallintatoimenpiteiden toteuttamisen jälkeen arvioidaan, ovatko toimenpiteet olleet riittäviä. Tämän jälkeen asiassa voidaan edetä.

Vaikutustenarvioinnissa määritellyillä hallintatoimenpiteillä voi olla vaikutuksia esimerkiksi sopimusehtoihin sekä järjestelmille ja palveluille asetettaviin vaatimuksiin.

14.6.4 Tietosuojan tarkistuslista

Jos alkukartoitus on osoittanut, että henkilötietoja käsitellään, mutta varsinaista vaikutustenarviointia ei tarvitse tehdä, tulee käyttöön tietosuojan tarkistuslista.

Tietosuojan tarkistuslistalta löytyvät ne asiat, jotka on aina otettava huomioon kehittämisen aikana, vaikka ei käsiteltäisi erityisen arkaluonteista tai muutoin riskialtista henkilötietoa.

14.6.5 Vaikutustenarvioinnin loppuraportti

Vaikutustenarvioinnista voidaan tarvittaessa laatia loppuraportti. Loppuraportin tarkoituksena on antaa kattava yleiskatsaus vaikutustenarvioinnin tuloksista ja niistä tehdyistä johtopäätöksistä ilman, että lukijan tarvitsee käydä läpi varsinaista vaikutustenarvioinnin työkalua. Loppuraportti voi olla erityisesti tarpeen laajoissa ja vaativissa vaikutustenarvioinneissa sekä silloin, kun vaikutustenarvioinnin perusteella tehdään päätöksiä esim. johtoryhmässä.

EU:n yleinen tietosuoja-asetus (EU) 2016/679: 35 art., 36 art.

Tietosuojaa koskevan vaikutustenarvioinnin tarkoituksena on tunnistaa, arvioida ja hallita henkilötietojen käsittelyyn liittyviä riskejä.

15. Tietosuojalain-säädännön rikkomisen seuraamukset

15.1 Oikeus saattaa asia tietosuojavaltuutetun käsiteltäväksi

Tietosuoja-asetuksen mukaan jokaisella rekisteröidyllä on oikeus tehdä valitus valvontaviranomaiselle, jos rekisteröity katsoo, että häntä koskevien henkilötietojen käsittelyssä rikotaan tietosuoja-asetusta. Valituksen voi tehdä siinä maassa, jossa valittajan vakinainen asuinpaikka tai työpaikka sijaitsee tai jossa väitetty rikkominen on tapahtunut. Suomessa valvontaviranomaisena toimii tietosuojavaltuutettu.

Valvontaviranomaisella on laajat tutkintavaltuudet mm. oikeus saada rekisterinpitäjältä ja henkilötietojen käsittelijältä pääsy kaikkiin henkilötietoihin ja kaikkiin tietoihin, jotka ovat tarpeen sen tehtävien suorittamista varten, sekä saada pääsy kaikkiin rekisterinpitäjän ja käsittelijän tiloihin, tietojenkäsittelylaitteet ja -keinot mukaan lukien.

Tietosuojavaltuutettu voi mm.

- antaa huomautuksen rekisterinpitäjälle tai henkilötietojen käsittelijälle, jos käsittelytoimet ovat olleet tietosuoja-asetuksen vastaisia
- määrätä rekisterinpitäjän tai käsittelijän noudattamaan rekisteröidyn pyyntöjä, jotka koskevat asetukseen perustuvien rekisteröityjen oikeuksien käyttöä
- määrätä rekisterinpitäjän tai käsittelijän saattamaan käsittelytoimet asetuksen sääntöjen mukaisiksi
- määrätä rekisterinpitäjän ilmoittamaan tietoturvaloukkauksesta rekisteröidylle
- asettaa väliaikaisen tai pysyvän rajoituksen käsittelylle
- määrätä henkilötietojen oikaisemisesta tai poistamisesta
- määrätä tiedonsiirron keskeyttämisestä kolmannessa maassa olevalle vastaanottajalle.

Tietosuojavaltuutettu voi asettaa uhkasakon antamiensa määräysten tehosteeksi.

Tietosuojavaltuutetun päätöksestä voi valittaa hallintovalituksena hallinto-oikeuteen.

15.2 Oikeus nostaa kanne rekisterinpitäjää tai henkilötietojen käsittelijää vastaan

Jokaisella rekisteröidyllä on oikeus nostaa kanne rekisterinpitäjää tai henkilötietojen käsittelijää vastaan, jos hän katsoo, että hänen henkilötietojensa käsittelyssä ei ole noudatettu tietosuoja-asetusta.

Kanne nostetaan sen jäsenvaltion tuomioistuimissa, jossa rekisterinpitäjällä tai henkilötietojen käsittelijällä on toimipaikka. Vaihtoehtoisesti tällainen kanne voidaan nostaa sen jäsenvaltion tuomioistuimissa, jossa rekisteröidyn vakinainen asuinpaikka on, paitsi jos rekisterinpitäjä tai henkilötietojen käsittelijä on jäsenvaltion viranomainen, jonka toiminta liittyy sen julkisen vallan käyttöön.

Mikäli henkilötietojen käsittelyssä ei ole kyse julkisen vallan käytöstä, voi Helsingin kaupunki joutua vastaamaan toisessa jäsenvaltiossa asuvan henkilön henkilötietoja koskevaan kanteeseen kyseisessä jäsenvaltiossa. Pääsääntöisesti Helsingin kaupungin ollessa rekisterinpitäjä tai käsittelijä, kanteet käsitellään Helsingin käräjäoikeudessa.

15.3 Oikeus korvauksen saamiseen

Jos henkilölle aiheutuu tietosuoja-asetuksen rikkomisesta aineetonta tai aineellista vahinkoa, hänellä on oikeus saada korvaus rekisterinpitäjältä tai käsittelijältä.

Henkilötietojen käsittelijä on vastuussa vahingosta vain, jos se ei ole noudattanut nimenomaisesti henkilötietojen käsittelijälle osoitettuja tietosuoja-asetuksen mukaisia velvoitteita tai jos se on toiminut rekisterinpitäjän lainmukaisten ohjeistusten ulkopuolella tai sen vastaisesti.

Tämän vuoksi on tärkeää, että Helsingin kaupunki rekisterinpitäjänä antaa sen sopimuskumppaneina oleville henkilötietojen käsittelijöille asianmukaiset ohjeet henkilötietojen käsittelystä.

Korvausasia käsitellään sen jäsenvaltion tuomioistuimessa, jossa rekisterinpitäjällä tai henkilötietojen käsittelijällä on kotipaikka. Vaihtoehtoisesti tällainen kanne voidaan nostaa sen jäsenvaltion tuomioistuimissa, jossa rekisteröidyn vakinainen asuinpaikka on, paitsi jos rekisterinpi-

Henkilötietojen käsittelijä on vastuussa vahingosta vain, jos se ei ole noudattanut nimenomaisesti henkilötietojen käsittelijälle osoitettuja tietosuoja-asetuksen mukaisia velvoitteita tai jos se on toiminut rekisterinpitäjän lainmukaisten ohjeistusten ulkopuolella tai sen vastaisesti.

täjä tai henkilötietojen käsittelijä on jäsenvaltion viranomainen, jonka toiminta liittyy sen julkisen vallan käyttöön.

Mikäli henkilötietojen käsittelyssä ei ole kyse julkisen vallan käytöstä, voi Helsingin kaupunki joutua vastaamaan toisessa jäsenvaltiossa asuvan henkilön henkilötietoja koskevaan kanteeseen kyseisessä jäsenvaltiossa. Pääsääntöisesti Helsingin kaupungin ollessa rekisterinpitäjä tai käsittelijä kanteet käsitellään Helsingin käräjäoikeudessa.

15.4 Rikosoikeudelliset seuraamukset

Aina on syytä muistaa, että henkilötietoja käsittelevä henkilö voi rikkoessaan tietosuojalainsäädäntöä syyllistyä rikokseen, mikäli rikoslain säätämät rikoksen tunnusmerkistöt täyttyvät.

Rikoslain 38 luvun 9 §:ssä säädetään tietosuojarikoksesta. Tietosuojarikoksesta voidaan rangaista mm. jos muutoin kuin rekisterinpitäjänä tai käsittelijänä tahallaan tai törkeästä tuottamuksesta hankkii, luovuttaa tai siirtää henkilötietoja tietosuojalainsäädännön vastaisesti ja siten loukkaa rekisteröidyn yksityisyyden suojaa tai aiheuttaa hänelle muuta vahinkoa tai olennaista haittaa.

Lisäksi on salassapitorikos, josta säädetään rikoslain 38 luvun 1 §:ssä. Sen mukaan salassapitorikoksesta voidaan rangaista, mikäli salassapitovelvollisuuden vastaisesti paljastaa asemassaan, toimessaan tai tehtävää suorittaessaan saamansa salassa pidettävän tiedon tai käyttää sitä omaksi tai toisen hyödyksi.

Erikseen on säädetty rangaistavaksi viestintäsalaisuuden loukkaus, sen törkeä tekomuoto sekä tietomurto ja sen törkeä tekomuoto.

Viranhaltijan rikosoikeudellinen asema on ankarampi kuin työntekijän. Viranhaltija ja muu virkavastuulla toimiva henkilö voi tulla tuomituksi virkavelvollisuuden rikkomisesta tai muusta rikoslain 40 luvun mukaisesta virkarikoksesta, jos hän rikkoo virkatoiminnassa noudatettavia säännöksiä.

EU:n yleinen tietosuoja-asetus (EU) 2016/679: 77 art., 79 art., 82 art.

Rikoslaki 39/1889: 38 luku 1 §, 9 §, 40 luku

16. Sopimukset ja hankinnat

16.1 Tietosuoja-asetuksen vaikutus sopimusehtoihin

Arvioitaessa tietosuoja-asetuksen asettamia velvoitteita sopimusehtojen kannalta, lähtökohdaksi on otettava asetuksen asettama velvollisuus sopia henkilötietojen käsittelystä sopimuksella. Se kohdistuu sekä rekisterinpitäjään että henkilötietojen käsittelijään.

Tämä velvollisuus ei tarkoita sitä, että käsittelystä olisi tehtävä erillinen sopimus. Useimmiten asetuksen edellyttämät kohdat on järkevämpää sisällyttää palvelua tai järjestelmää koskevaan sopimukseen, tai esimerkiksi siihen liitettävään kaupungin tietosuoja- ja salassapitoliitteeseen. Erillisen henkilötietojen käsittelyä koskevan sopimuksen solmimiselle ei kuitenkaan ole estettä silloin, kun se katsotaan tarkoituksenmukaisemmaksi toimintatavaksi.

Lähtökohtaisesti kaupungin sopimuksissa käytetään kaupungin tietosuoja- ja salassapitoliitteeseen 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.

Sopimusehtojen lisäksi on arvioitava, onko tarvetta tehdä tietosuojan vaikutustenarviointi (ks. luku 14) sekä huomioitava tietosuojavaatimukset järjestelmälle tai palvelulle asetettavissa vaatimuksissa.

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.

16.2 Henkilötietojen käsittely EU/ETA-alueen ulkopuolella

Helsingin kaupunginhallituksen tietosuojalinjaukset sisältävät neljä linjausta koskien henkilötietojen käsittelyä EU/ETA-alueen ulkopuolella. Tietosuojalinjauksissa määritellään, missä tilanteissa ja millä tavoin Helsingin kaupunki sallii henkilötietojensa käsittelyn EU/ETA-alueen ulkopuolella.

Henkilötietojen käsittelyn EU/ETA-alueen ulkopuolella tulee aina perustua tietosuojavaikutusten ja -riskien arviointiin. Vaikutustenarvioinnista kerrotaan lisää luvussa 14.

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

Tietosuojalinjauksissa henkilötiedot on jaettu kolmeen eri kategoriaan:

1. Korkeariskiset henkilötiedot
2. Vähäriskiset henkilötiedot lakisääteisessä toiminnassa
3. Vähäriskiset henkilötiedot muussa kuin lakisääteisessä toiminnassa

Korkeariskisillä henkilötiedoilla tarkoitetaan tietosuojalinjauksissa sekä lakisääteisessä toiminnassa että muussa toiminnassa käsiteltäviä:

- salassa pidettäviä henkilötietoja
- erityisiä henkilötietoryhmiä koskevia henkilötietoja (ks. luku 6)
- muita sellaisia henkilötietoja, jotka ovat omiaan aiheuttamaan korkean riskin rekisteröidyn oikeuksille ja vapauksille (kuten henkilötunnus).

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

Seuraavassa käydään ensin läpi henkilötietojen käsittely Euroopan komission hyväksymissä maissa, ja tämän jälkeen henkilötietojen käsittely EU/ETA-alueen ja komission hyväksymien maiden ulkopuolella. Lopuksi kerrotaan, miten siirtomahdollisuus tulee huomioida tietosuoja- ja salassapitoliitteessä.

16.2.1 Käsittely Euroopan komission hyväksymissä maissa

Euroopan komission hyväksymillä mailla tarkoitetaan tietosuojalinjauksissa EU/ETA-alueen ulkopuolisia maita, joiden tietosuojan tason komissio on hyväksynyt riittäväksi.

Kaupunki sallii vähäriskisten henkilötietojen käsittelyn komission hyväksymissä maissa. Korkeariskisten henkilötietojen käsittelyn kaupunki sallii komission hyväksymissä maissa silloin, kun kyseisten tietojen luonne on sellainen, että kaupungin omista lähtökohdista (esim. valmiuskysymykset) ei muodostu estettä käsittelylle.

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

Helsingin kaupunginhallituksen tietosuojalinjaukset sisältävät neljä linjausta koskien henkilötietojen käsittelyä EU/ETA-alueen ulkopuolella.

16.2.2 Korkeariskiset henkilötiedot

Kaupunki sallii korkeariskisten henkilötietojen käsittelyn EU/ETA-alueen ja Euroopan komission hyväksymien maiden ulkopuolella vain 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 korkeariskisiä 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 lisäedellytysten henkilötietojen käsittelylle (luku 16.2.5) on täytyttävä.

16.2.3 Vähäriskiset henkilötiedot lakisääteisessä toiminnassa

Kaupunki sallii lakisääteisessä toiminnassa käsiteltävien vähäriskisten henkilötietojen käsittelyn EU/ETA-alueen ja Euroopan komission hyväksymien maiden ulkopuolella vain silloin, kun käsittely on poikkeuksellisesti tarpeellista. Lisäksi henkilötietojen käsittelyn lisäedellytysten (luku 16.2.5) on täytyttävä.

16.2.4 Vähäriskiset henkilötiedot muussa kuin lakisääteisessä toiminnassa

Kaupunki sallii vähäriskisten henkilötietojen käsittelyn EU/ETA-alueen ja Euroopan komission hyväksymien maiden ulkopuolella. Käsittelyn lisäedellytysten (luku 16.2.5) on kuitenkin täytyttävä.

16.2.5 Lisäedellytykset henkilötietojen käsittelylle

Edellytyksenä sekä korkeariskisten että vähäriskisten henkilötietojen käsittelylle EU/ETA-alueen ja Euroopan komission hyväksymien maiden ulkopuolella on:

- tietosuojan tosiasiallisen riittävän tason varmistaminen ja
- tietosuoja-asetuksen asettamien edellytysten noudattaminen siirrossa kolmansiin maihin.

Tietosuojan tosiasiallinen tason varmistamisessa tulee käyttää kokonaisharkintaa ja huomioida käsittelyyn ja kyseisiin tietoihin liittyvät riskit.

Tätä varten kaupunki vaatii toimittajalta täsmällisen kuvauksen siitä, millä tavoin tietojen käsittely tullaan suorittamaan. Tällöin toimittajalta tulisi saada kaikki palvelun tietosuojaa koskeva dokumentaatio. Tapauskohtaisesti harkitaan, riittääkö käsittelytoimien kuvaus ja tietosuojan tarkistuslistan käyttö vai onko tehtävä tietosuojan vaikutustenarviointi (ks. luku 14).

Tietosuoja-asetuksen asettamien edellytysten noudattaminen siirrossa kolmansiin maihin tarkoittaa tietosuoja-asetuksen 46 artiklassa tarkoitettuja suojatoimia, joilla henkilötietojen siirtäminen tai muu käsittelyn aloittaminen voidaan toteuttaa. Näistä yleisimmin käytettyjä ovat Euroopan komission hyväksymät mallisopimuslausekkeet. Ennen henkilötietojen siirtämistä tai niiden käsittelyn aloittamista EU/ETA-alueen ulkopuolella on siis huolehdittava, että henkilötietojen käsittelystä on sovittu mallisopimuslausekkeiden mukaisesti. Jos toimittaja käsittelee henkilötietoja kolmannessa maassa, käytetään mallisopimuslausekkeita kaupungin ja toimittajan välillä. Jos henkilötietoja käsittelee kolmannessa maassa sijaitseva toimittajan alihankkija, toimittajan on huolehdittava mallisopimuslausekkeista alihankkijansa kanssa.

Ennen henkilötietojen siirtämistä tai niiden käsittelyn aloittamista EU/ETA-alueen ulkopuolella on siis huolehdittava, että henkilötietojen käsittelystä on sovittu mallisopimuslausekkeiden mukaisesti.

16.2.6 EU/ETA-alueen ulkopuolisen henkilötietojen käsittelyn huomioiminen tietosuoja- ja salassapitoliitteessä

Tietosuoja- ja salassapitoliitteen malliehdossa henkilötietojen käsittely EU/ETA-alueen ulkopuolella on kiellettyä (ks. mallin kohta 10 (5)). Mikäli kyseinen käsittely halutaan sallia, tulee tietosuoja- ja salassapitoliitteen kohta 10 (5) korvata esim. seuraavalla malliehdolla:

Malliehto tietosuoja- ja salassapitoliitteeseen otettavasta ehdosta, jolla EU/ETA-alueen ulkopuolinen henkilötietojen käsittely mahdollistetaan:

> Toimittaja saa käsitellä, siirtää tai luovuttaa Tilaajan henkilötietoja EU tai ETA-alueen ulkopuolelle vain Tilaajan hyväksynnällä. Tilaajan hyväksynnän lisäksi edellytyksenä on, että henkilötietojen käsittely, siirto tai luovutus toteutetaan lainsäädännön mukaisesti EU:n mallilausekkeita käyttämällä. Mallilausekkeita ei tarvitse käyttää, mikäli käsittely, siirto tai luovutus tapahtuu sellaiseen valtioon, jonka tietosuojan tason Euroopan komission on hyväksynyt riittäväksi. [Palvelimien tulee sijaita EU- tai ETA-alueella ja Toimittajan tulee ilmoittaa Tilaajalle niiden sijoituspaikat.] Toimittajan on ilmoitettava Tilaajalle etukäteen, jos palvelimien sijaintipaikka muuttuu. Jos Pääsopimuksessa on sovittu käsittelyn tai palvelinten sijainnista edellä mainittua tiukemmin, kuten että palvelimet sijaitsevat Suomessa, sovelletaan Pääsopimusta.

16.3 Muut tietosuojasopimukset

16.3.1 Yhteisrekisterinpitäjien välinen sopimus

Jos käsittelyn tarkoitukset ja keinot määritetään yhdessä, on kysymys yhteisrekisterinpitäjistä.

Yhteisrekisterinpitäjien on määriteltävä sopimuksella yhteisrekisterinpitäjien vastuualueet asetuksessa vahvistettujen velvoitteiden noudattamiseksi.

Käytännössä tämä tarkoittaa sen määrittelemistä, kuka vastaa mistäkin, erityisesti rekisteröityjen oikeuksien käytön ja rekisteröidyn informoinnin osalta. Lisäksi sopimuksessa on todettava rekisterinpitäjien todelliset roolit ja suhteet rekisteröityihin nähden. Sopimuksen yhteydessä voidaan nimetä rekisteröidyille yhteyspiste.

16.3.2 Tietojen luovuttaminen toiselle rekisterinpitäjälle

Kun on kyse tietojen luovuttamisesta toisen rekisterinpitäjän käsiteltäväksi sen omaan lukuun, ei tietosuoja-asetuksen 28 artiklan mukaista sopimusta tarvitse tehdä. Kaupunki vastaa siitä, että luovutukselle on laillinen peruste ja luovutuksen saajalla on oikeus tallettaa ja käyttää henkilötietoja. Tämän vuoksi jokainen luovutus on arvioitava etukäteen tapauskohtaisesti. Kaupungin edun mukaista on sopia tietojen luovutuksesta tiettyyn käyttötarkoitukseen, jotta kaupunki voi näyttää, että sillä on ollut laillinen peruste tietojen luovuttamiselle. Sopimuksessa on kuvattava käsittelyperuste ja käsittelyn sisältö pääpiirteisesti. Sopimuksessa on syytä todeta, että tiedot luovutetaan toiselle rekisterinpitäjälle.

Kaupungin edun mukaista on sopia tietojen luovutuksesta tiettyyn käyttötarkoitukseen, jotta kaupunki voi näyttää, että sillä on ollut laillinen peruste tietojen luovuttamiselle.

17. Julkisuuslain ja tietosuoja-asetuksen suhde

Tietosuojaan liittyvän lainsäädännön lisäksi on huomioitava, että henkilötietojen luovuttamisesta viranomaisen henkilörekisteristä säädetään laissa viranomaisten toiminnan julkisuudesta (julkisuuslaki) (621/1999).

Julkisuuslain mukaisista oikeuksista ja tietopyynnöistä on oma ohjeistuksensa. Julkisuuslain mukaan viranomaisten asiakirjat ovat julkisia, jollei erikseen toisin säädetä. Julkisuuslaissa ja muussa lainsäädännössä on säädetty salassa pidettävät tiedot. Näitä ovat muun muassa sosiaali- ja terveydenhuollon asiakastiedot, oppilashuoltoa koskevia tiedot, henkilön taloudellista asemaa kuvaavat tiedot ja liikesalaisuudet.

Julkisuuslain mukaan viranomaisen henkilörekisteristä saa antaa henkilötietoja sisältävän kopion tai tulosteen tai sen tiedot sähköisessä muodossa, jollei laissa ole toisin erikseen säädetty, jos luovutuksensaajalla on henkilötietojen suojaa koskevien säännösten mukaan oikeus tallettaa ja käyttää sellaisia henkilötietoja. Henkilötietojen suojaa koskevia säännöksiä ovat tietosuoja-asetus ja tietosuojalaki sekä myös erityislait.

Jokaisella on oikeus saada tieto viranomaisen asiakirjasta, joka on julkinen. Esimerkiksi rakennuslupapäätökset ja virkaan ottamispäätökset ovat julkisia, vaikka ne sisältävätkin henkilötietoja. Julkisen asiakirjan sisällöstä annetaan tieto suullisesti tai antamalla asiakirja viranomaisen luona nähtäväksi ja jäljennettäväksi tai kuunneltavaksi tai antamalla siitä kopio tai tuloste. Helsingin kaupungin asiakirjoista voi kysyä kaupungintalolla sijaitsevasta kirjaamosta. Eräissä tapauksissa tieto voidaan antaa myös sähköisesti

Viranomaisen henkilörekisteristä otetun henkilötietoja sisältävän kopion tai tulosteen antamista on rajoitettu lailla. Vastaavien tietojen antamista myös sähköisessä muodossa on rajoitettu lailla. Niitä voidaan julkisilta osin antaa nähtäväksi viranomaisen luona tai antaa tietoja suullisesti kaikille. Sen sijaa kopioita, tulosteita tai tietoja sähköisessä muodossa voidaan pääsääntöisesti antaa vain, jos pyytäjällä on henkilötietojen suojaa koskevien säännösten mukaan oikeus tallettaa ja käyttää sellaisia henkilötietoja.

Jokaisella on oikeus muutamin rajoituksin saada tieto hänestä itsestään viranomaisen asiakirjaan sisältyvistä tiedoista, vaikka tiedot olisivat salassa pidettäviä.

Jos henkilö on asianosaisena jossakin asiassa, hänellä saattaa olla oikeus salassa pidettävän henkilötiedon saantiin silloinkin, kun kyse ei ole hänen omista henkilötiedoistaan.

Jollei viranomainen anna julkisuuslain perusteella pyydettyjä asiakirjoja, viranomaisen tätä koskevasta päätöksestä voi valittaa hallinto-oikeuteen.

Laki viranomaisten toiminnan julkisuudesta (621/1999)

18. Henkilötietojen suoja päätösvalmistelussa

18.1 Henkilötietojen käsittely pöytäkirjassa

Toimielinten, viranhaltijoiden ja luottamushenkilöiden pöytäkirjoihin sisältyy usein henkilötietoja.

Niitä ovat esimerkiksi tiedot asianosaisista, kuten etuuksien, avustuksien tai lupien hakijoista, henkilöstöasioissa tiedot työntekijöistä ja viranhaltijoista ja muutoksenhakua koskevissa asioissa valittajista.

Valmistelijoiden tulee tarkkaan harkita, minkä luonteisia valmisteltavassa asiassa esiintyvät henkilötiedot ovat.

Esityslistan sisältämät henkilötiedot

Esityslistat sisältävät henkilötietoja. Niiden sisältämiä henkilötietoja voidaan julkaista yleisessä tietoverkossa vain, kun kysymys on kuntalaisten tiedonsaannin kannalta välttämättömistä tiedoista, jotka eivät ole salassa pidettäviä. Näitä ovat esittelijän ja valmistelijan tiedot sekä tapauskohtaisen harkinnan perusteella välttämättömiksi katsotut muut henkilötiedot.

Pöytäkirjan julkaiseminen yleisessä tietoverkossa

Pöytäkirja siihen liitettyine oikaisuvaatimusohjeineen tai valitusosoituksineen pidetään tarkastamisen jälkeen nähtävänä yleisessä tietoverkossa, jollei salassapitoa koskevista säännöksistä muuta johdu. Jos asia on kokonaan salassa pidettävä, pöytäkirjassa julkaistaan ainoastaan maininta salassa pidettävän asian käsittelystä. Jos vain osa tiedoista on salassa pidettäviä, jätetään julkaisematta salassa pidettävät tiedot. Tietosuoja-asetuksen mukaisiin erityisiin henkilötietoryhmiin kuuluvat tiedot ovat kansallisen lainsäädännön nojalla lähtökohtaisesti salassa pidettäviä tietoja.

Henkilötunnus ei ole salassa pidettävä tieto, mutta koska sitä saa käsitellä vain tietyillä perusteilla, ei henkilötunnusta saa julkaista yleisessä tietoverkossa.

Tietoverkossa julkaistavassa pöytäkirjassa saa julkaista ainoastaan julkiset ja tiedonsaannin kannalta välttämättömät henkilötiedot. Tietoverkossa julkaistavassa pöytäkirjassa tulee kuitenkin aina olla päätöksentekoon liittyvät olennaiset tiedot sekä ne tiedot, jotka ovat tarpeellisia esimerkiksi oikaisuvaatimuksen tai valituksen tekemiseksi. Jos henkilötieto on päätöksentekoon liittyvä olennainen tieto tai tarpeellinen oikaisuvaatimuksen tai valituksen tekemiseksi, on se tiedonsaannin kannalta välttämätön henkilötieto, joka on julkaistava tietoverkossa.

Sen sijaan mitä tahansa julkisiakaan henkilötietoja ei saa viedä yleiseen tietoverkkoon. On olemassa tietotyyppejä, jotka verkkoon laitettaessa altistavat asianosaisen erilaisille riskeille. Tällaisia tietoja voivat olla esimerkiksi osoite, puhelinnumero, sähköpostiosoite, pankkitilin numero tai tieto perheenjäsenistä. Edellä mainittujen henkilötietojen julkaiseminen on yleensä myös tarpeetonta kuntalaisen tiedonsaannin kannalta.

Sen sijaan esimerkiksi viranhaltijan valintaa koskevissa päätöksissä joidenkin henkilötietojen kuten nimitiedon ja mahdollisesti ammattia tai koulutusta koskevan tiedon julkaiseminen voi olla välttämätöntä asian arvioimiseksi muutoksenhaun kannalta. Kunnalliset viranhaltijat hoitavat tehtäviä, joissa käytetään julkista valtaa. Virkavalinnan osalta voidaankin pitää kunnallisen tiedotusintressin näkökulmasta perusteltuna julkaista valitun henkilön nimi päätöksessä.

Valmistelijoiden tulee tarkkaan harkita, minkä luonteisia valmisteltavassa asiassa esiintyvät henkilötiedot ovat.

Päätöksentekijän ja valmistelijan henkilötiedot

Myös päätöksentekijän, esittelijän ja valmistelijan nimi ja yhteystiedot ovat henkilötietoja. Hallintolain mukaan kirjallisesta päätöksestä on käytävä selvästi ilmi päätöksen tehnyt viranomainen ja ne asianosaiset, joihin päätös välittömästi kohdistuu sekä sen henkilön nimi ja yhteystiedot, jolta asianosainen voi pyytää tarvittaessa lisätietoja päätöksestä. Tämä vuoksi myös yleisessä tietover-

kossa julkaistussa päätöksessä on välttämätöntä julkaista päätöksentekijän ja valmistelijan nimet ja tarvittavat yhteystiedot. Asianosaisen henkilötietojen, kuten nimen, julkaisemisen osalta on kaikkien tietojen osalta harkittava, onko kyseessä päätöksentekoon liittyvä olennainen tieto, kuten oikaisuvaatimuksen tai valituksen tekemiseksi tarpeellinen tieto.

Henkilötietojen poistaminen päätöksestä oikaisu- tai valitusajan jälkeen

Kuntalain mukaan pöytäkirjan sisältämät henkilötiedot on poistettava tietoverkosta oikaisuvaatimus- tai valitusajan päättyessä. Erityistä huomiota tulee kiinnittää siihen, että henkilötiedot kokonaisuudessaan poistetaan päätöksestä oikaisuvaatimus- tai valitusajan päättyessä. Henkilötiedoilla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan henkilöön liittyviä tietoja, joten henkilötietojen suoja on harvoin toteutettavissa ainoastaan henkilön nimen poistamisella. Myös muut henkilöön liittyvät tiedot, kuten virkavalinnassa kuvaukset henkilön työhistoriasta ja ansioista, on poistettava päätöksestä muutoksenhakuajan jälkeen.

18.2 Kunnallinen tiedotusintressi

Kuntalain mukaan kunnan toiminnasta on tiedotettava asukkaille, palvelujen käyttäjille, järjestöille ja muille yhteisöille. Kunnan tulee antaa riittävästi tietoja järjestämistään palveluista, taloudesta, valmistelussa olevista asioista, niitä koskevista suunnitelmista, asioiden käsittelystä, tehdyistä päätöksistä ja päätösten vaikutuksista. Kunnan on tiedotettava, millä tavoin päätösten valmisteluun voi osallistua ja vaikuttaa sekä huolehdittava siitä, että toimielinten käsittelyyn tulevien asioiden valmistelusta annetaan esityslistan valmistuttua yleisen tiedonsaannin kannalta tarpeellisia tietoja yleisessä tietoverkossa. Kunnan on verkkoviestinnässään huolehdittava, että salassa pidettäviä tietoja ei viedä yleiseen tietoverkkoon ja että yksityisyyden suoja henkilötietojen käsittelyssä toteutuu.

Tietosuojalain mukaan henkilötietoja saa käsitellä yleistä etua koskevan tehtävän suorittamiseksi, jos käsittely on tarpeen ja oikeasuhtaista viranomaisen toiminnassa yleisen edun mukaisen tehtävän suorittamiseksi.

Henkilötietojen pitäminen tietoverkossa muutoksenhakuajan päättymisen jälkeen tulee perustua kunnan omaan tiedottamisintressiin eli tietosuojalain ja kuntalain säännöksiin.

Kaupunginhallitus on 17.6.2013 viestinnän ohjeissa linjannut siitä, että Helsingissä kunnallisen viranomaisen pöytäkirjat julkaistaan yleisessä tietoverkossa pysyvästi kunnallista päätöksentekoa koskevan tiedonsaannin helpottamiseksi.

Kuntalain mukaista kunnallista tiedotusvelvollisuutta on Helsingissä toteutettu jättämällä muutoksenhakuajan jälkeenkin pöytäkirjoihin kuntalaisen tiedonsaannin kannalta merkittävät tiedot, kuten päätöksentekijän nimi, lisätiedonantajan eli valmistelijan nimi sekä tapauskohtaisen harkinnan mukaan esim. erityisen merkittävissä virkavalinnoissa valituksi tulleen johtotason viranhaltijan nimi. Myös esimerkiksi tietyn asian valmistelua koskevan työryhmän perustamista koskeva päätös voi sisältää kaupungin työntekijöiden nimiä, jotka ovat kuntalaisten tiedonsaannin ja vaikutusmahdollisuuksien turvaamiseksi perusteltua pitää saatavilla yleisessä tietoverkossa.

Kaupungin tulee kussakin yksittäisessä asiassa punnita, onko olemassa sellainen tiedotusintressi, että se oikeuttaa kyseisten henkilötietojen julkaisemisen ja käsittelyn kunnan verkkosivulla. Tämä edellyttää sen arvioimista, onko kyseisten henkilötietojen julkaisu avoimessa tietoverkossa tarpeellista yleisen edun mukaisen kunnallista päätöksentekoa koskevan tiedonsaannin kannalta. Samalla on arvioitava, onko yleisessä tietoverkossa julkaiseminen oikeasuhtaista, kun huomioidaan siitä aiheutuva haitta henkilötietojen ja yksityisyyden suojalle.

Hallintolaki (434/2003): 44 §

Kuntalaki (410/2015): 140 §, 29 §

Tietosuojalaki 1050/2018: 4 § 1 mom. 2 kohta

Julkaisija:
Helsingin kaupunki
kaupunginkanslia

Työryhmä:
Tietosuojatyöryhmä

Lisätietoja
hel.fi/tietosuoja
tietosuoja@hel.fi

Taitto:
Aste Helsinki Oy, Lea Hult

Kuvat: Helsinki Material Bank

kansi	Jussi Ratilainen
s. 4	Jussi Hellsten
s. 6	Eetu Ahanen
s. 8	Jussi Ratilainen
s. 11	Jussi Hellsten
s. 18	Kuvatoimisto Kuvio Oy
s. 31	Carl Bergman/Duotone
s. 32	Super Otus
s. 38	Yiping Feng and Ling Ouyang
s. 43	Julia Kivelä
s. 46	Mikael Ahlfors/KEKSI
s. 54	Mikael Ahlfors/KEKSI
s. 57	Tuomas Uusheimo
s. 62	Aleksi Poutanen
s. 64	Paul Masukowitz Photography

Helsinki