Naantalin kaupunki

TIETOSUOJAKÄSIKIRJA

Sisällys

1. Tietosuoja

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 henkilötietojen suojaan.

Henkilötietoja ovat nimen ja henkilötunnuksen lisäksi esimerkiksi osoite, puhelinnumero, sähköpostiosoite, auton rekisterinumero, kiinteistötunnus, 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 voi olla talletettuna esimerkiksi sähköisissä tiedostoissa, tietokannoissa, paperilla, kortistossa, mapeissa tai ääni- ja kuvatallenteella.

Henkilötietojen käsittely tarkoittaa muun muassa tietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakua, kyselyä, käyttöä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne muuten saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista ja tuhoamista. Jo pelkkä henkilötietojen katsominen on henkilötietojen käsittelyä, vaikka tietoja ei muutettaisi mitenkään.

1.1. Pseudonymisointi ja anonymisointi

Pseudonymisointi tarkoittaa henkilötietojen käsittelemistä siten, että henkilötietoja ei voida enää yhdistää tiettyyn henkilöön ilman lisätietoja. Tällaiset lisätiedot täytyy säilyttää huolellisesti erillään henkilötiedoista ja varmistaa, ettei yhdistämistä tunnistettuun tai tunnistettavissa olevaan henkilöön tapahdu. Pseudonymisoidut tiedot ovat yhä henkilötietoja ja niiden käsittelyssä on sovellettava tietosuoja-asetusta.

Anonymisointi tarkoittaa henkilötietojen käsittelemistä siten, että henkilötietoja ei voida enää yhdistää tiettyyn henkilöön edes käyttämällä lisätietoja. Tiedot voidaan esimerkiksi muuttaa tilastolliseen muotoon siten, etteivät henkilöä koskevat tiedot ole enää tunnistettavassa muodossa. Tunnistamisen täyttyy estyä peruuttamattomasti ja siten, että rekisterinpitäjä tai muu ulkopuolinen taho ei voi enää hallussaan olevilla tiedoilla muuttaa tietoja takaisin tunnistettaviksi. Anonymisoidun tiedon käsittely ei ole henkilötietojen käsittelyä eikä se ole tietosuoja-asetuksen soveltamisalan piirissä.

1.2. Mitä eroa on tietosuojalla ja tietoturvalla?

Tietoturva on yksi tietosuojan toteuttamisen keino. Tietoturvan tarkoitus on suojata tietoaineisto (sähköiset ja paperiset) ja tietojärjestelmät. Tietoturva tarkoittaa muun muassa organisatorisia ja teknisiä toimenpiteitä, joilla varmistetaan, että tiedot ovat vain tietoon oikeutettujen käytettävissä (luottamuksellisuus), silloin, kun he niitä tarvitsevat (saatavuus/käytettävyys) ja tietoa ei ole muutettu tahallisesti tai tahattomasti (eheys).

2. Tietosuojalainsäädäntö

EU:n yleistä tietosuoja-asetusta (EU) 2016/679 (General Data Protection Regulation, GDPR) alettiin soveltaa 25.5.2018. Asetus on suoraan sovellettavaa lainsäädäntöä eli sitä ei panna täytäntöön kansalliseen lakiin.

Asetuksen tavoitteena on varmistaa, että ihmisten oikeus henkilötietojen suojaan ja sitä kautta yksityisyyteen toteutuu myös digitaaliaikana. Sääntely pyrkii vastaamaan teknologian nopean kehityksen haasteisiin ja vahvistamaan ihmisten oikeutta valvoa henkilötietojaan. Tavoitteena on myös vahvistaa

säännöt henkilötietojen vapaalle liikkuvuudella EU:n sisällä. Asetus ottaa kantaa henkilötietojen lainmukaiseen käsittelyyn ja kertoo milloin, miten ja kenen toimesta henkilötietoja saa käsitellä.

Tietosuojalaki (1050/2018) tuli voimaan 1.1.2019. Se on henkilötietojen käsittelyyn sovellettava yleislaki, ja siinä on täydennetty ja täsmennetty tietosuoja-asetuksen määräyksiä. Tietosuoja-asetus antaa verrattain vähän liikkumavaraa kansallisille säädöksille, joten *tärkeää onkin lukea ja soveltaa EU:n yleistä tietosuoja-asetusta ja kansallista tietosuojalakia samanaikaisesti.*

3. Tietosuoja-asioiden vastuunjako Naantalin kaupungilla

Hallintosäännön mukaisesti kaupunginhallitus vastaa siitä, että kaupunki täyttää tietosuojalainsäädännön velvoitteet ja valvoo niiden toteuttamista. Palvelualojen johdolla puolestaan on vastuu toiminnan lainmukaisuudesta henkilötietojen käsittelyssä.

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 (tietosuojavaltuutettu) kanssa ja rekisteröityjen (kuntalaiset) oikeuksien toteuttamisen tukeminen. Tietosuojavastaavan yhteystiedot on julkistettava ja ne on ilmoitettava valvontaviranomaiselle. Naantalin kaupunkiin on nimetty vielä erikseen **sosiaali- ja terveydenhuollon tietosuojavastaava**.

Tietoturvapäällikkö (tietohallintopäällikkö) edistää tietoturvallisuuden toteutumista kaupungissa.

Edellä mainitut viranhaltijat muodostavat **tietosuojatyöryhmän**, joka valvoo tietosuojan toteutumista ja kehittää tietosuojatyötä kunnassa. Tietosuojatyöryhmä vastaa vuosittain laadittavan tietotilinpäätöksen koonnista.

Naantalin kaupunki kerää henkilötietoja eri rekistereihin tietojen käyttötarkoituksen mukaan. Rekistereistä laaditaan rekisteriselosteet, joissa on nimetty **rekisterinpitäjä**, joka määrittää henkilötietojen käsittelyn tarkoituksen ja keinot ja **rekisterin yhteyshenkilö**, joka ottaa vastaan tietopyynnöt ja tiedon korjaamisvaatimukset.

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

4. Henkilötietojen käsittelyä koskevat periaatteet

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

1. Lainmukaisuus, kohtuullisuus ja läpinäkyvyys
2. Käyttötarkoitussidonnaisuus
3. Tietojen minimointi
4. Täsmällisyys
5. Säilytyksen rajoittaminen

6. Eheys ja luottamuksellisuus

4.1. Lainmukaisuus, kohtuullisuus ja läpinäkyvyys

Henkilötietojen käsittelylle on aina oltava lain mukainen peruste eikä henkilötietoja saa käyttää väärin. Lisäksi rekisteröidylle tulee kertoa siitä, miten heitä koskevia tietoja kerätään ja käytetään sekä missä määrin henkilötietoja käsitellään.

4.2. Käyttötarkoitussidonnaisuus

Henkilötietojen käsittelyn tarkoitus on suunniteltava ja määriteltävä selkeästi ennen käsittelyn aloittamista. Henkilötietoja saa kerätä vain tiettyä, nimenomaista ja laillista tarkoitusta varten. Kerättyä tietoa ei saa myöhemmin käyttää muuhun tarkoitukseen ilman, että tämä uusi käyttötarkoitus on yhteensopiva alkuperäisen tarkoituksen kanssa.

4.3. Tietojen minimointi

Henkilötietoja ei saa käsitellä turhaan. Henkilötietoja saa käsitellä vain silloin, kun se on tarpeellista käsittelyn tarkoituksen kannalta. Henkilötietojen on oltava asianmukaisia ja olennaisia ja niiden käsittelyn pitää rajoittua vain tarpeelliseen.

4.4. Täsmällisyys

Käsiteltävien henkilötietojen on oltava täsmällisiä ja päivitettyjä. Epätarkat ja virheelliset henkilötiedot on oikaistava tai poistettava viipymättä.

4.5. Säilytyksen rajoittaminen

Henkilötietoja saa säilyttää vain niin kauan kuin se on tarpeen tietojen käyttötarkoitusta varten. Rekisterinpitäjän on asetettava määräaika henkilötietojen poistoa tai niiden säilyttämisen tarpeellisuuden määräaikaistarkastelua varten. Kun henkilötietoja ei enää tarvita, ne tulee anonymisoida tai poistaa.

4.6. 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.

5. Henkilötietojen käsittelyn perusteet

5.1. Henkilötietojen käsittelyn on perustuttava lakiin

Henkilötietoja saa käsitellä vain silloin, kun käsittelylle on laista löytyvä peruste. Tietosuoja-asetus määrittelee seuraavat perusteet, joilla henkilötietoja saa käsitellä:

1. Suostumus
2. Sopimus
3. Lakisääteinen velvoite
4. Elintärkeä etu
5. Yleinen etu ja julkinen valta
6. Oikeutettu etu

5.1.1. Suostumus

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

Jotta suostumus on pätevä, sen on oltava

- yksilöity
- tietoinen
- aidosti vapaaehtoinen ja
- yksiselitteinen tahdonilmaisu.

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. Eri käyttötarkoituksia varten on pyydettävä erilliset suostumukset. Uutta käyttötarkoitusta varten on lähtökohtaisesti pyydettävä aina uusi suostumus.

Suostumus tulee 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.

Rekisteröity ei voi antaa suostumustaan siihen, että hänen tietojaan saa käsitellä vapaasti mihin tahansa tarkoituksiin.

5.1.2. 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.

5.1.3. Lakisääteinen velvoite

Naantalin kaupungilla on lakisääteisiä velvoitteita, joiden noudattamiseksi on välttämätöntä kerätä henkilötietoja. Tällaisia velvoitteita ovat esimerkiksi perusopetuksen järjestäminen, sosiaali- ja terveydenhoidon järjestäminen ja pysäköinninvalvonnan järjestäminen. Velvoitteen pitää perustua joko kansalliseen tai Euroopan unionin lainsäädäntöön. Henkilötietoja saa kerätä vain siinä laajuudessa, kun 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 lait.

5.1.4. Elintärkeä etu

Henkilötietojen käsittely on sallittua, kun se on tarpeen rekisteröidyn tai jonkun toisen henkilön elintärkeiden etujen suojaamiseksi. Elintärkeiden etujen suojaaminen sopii käsittelyperusteeksi esimerkiksi tilanteisiin, joissa on kysymys elämästä ja kuolemasta tai uhkista, jotka voisivat johtaa rekisteröidyn tai jonkun toisen loukkaantumiseen tai olla muuten terveydelle vahingollisia.

Henkilötietojen käsittely voi palvella elintärkeää etua esimerkiksi humanitaarisissa hätätilanteissa, kuten luonnonkatastrofeissa tai epidemioissa. Henkilötietojen käsittelyä voidaan tarvita muun muassa silloin, kun halutaan seurata epidemian leviämistä.

Tämä käsittelyperuste on *toissijainen* eli sitä tulee käyttää vain silloin, kun käsittelyllä ei ole muuta ilmeistä käsittelyn oikeusperustetta.

5.1.5. 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, kun 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

5.1.6. Oikeutettu etu

Henkilötietojen käsittely on sallittua silloin, kun se on tarpeen rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi esimerkiksi silloin, kun rekisteröidyn ja rekisterinpitäjän välillä on merkityksellinen ja asianmukainen suhde, kuten asiakkuus- tai palvelusuhde. 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.

Se, milloin etu voidaan katsoa oikeutetuksi, saadaan selville niin kutsutulla tasapainotestillä. Siinä rekisterinpitäjän tai kolmannen osapuolen intressiä punnitaan rekisteröidyn intressejä ja perusoikeuksia vasten.

*Oikeutettu etu ei käy käsittelyperusteeksi tilanteisiin, joissa viranomaiset käsittelevät tietoja tehtäviensä yhteydessä***.**

5.2. Henkilötietojen käsittely muuhun kuin alkuperäiseen käsittelytarkoitukseen

Henkilötietoja voidaan käsitellä myöhemmin muuhun kuin alkuperäiseen käsittelytarkoitukseen vain, jos käsittely sopii yhteen alkuperäisen tarkoituksen kanssa. Yhteensopivuutta harkittaessa rekisterinpitäjän on otettava huomioon:

- henkilötietojen keräämisen alkuperäisen tarkoituksen ja myöhemmän käsittelyn tarkoituksen väliset yhteydet
- henkilötietojen keräämisen asiayhteys erityisesti rekisteröityjen ja rekisterinpitäjän välisen suhteen osalta
- henkilötietojen luonne
- aiotun myöhemmän käsittelyn mahdolliset seuraukset rekisteröidyille
- asianmukaisten suojatoimien, kuten salaamisen tai pseudonymisoinnin, olemassaolo.

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

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 ja 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 palvelusuhteita ja niihin liittyviä etuja koskevissa asioissa.

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

Digi- ja väestötietovirasto voi tallettaa väestötietojärjestelmään turvakiellon henkilölle, jolla on perusteltu syy epäillä oman tai perheensä turvallisuuden olevan uhattuna. Turvakiellon voi myös peruuttaa.

Turvakielto on poikkeuksellinen turvaamistoimi, jolla rajoitetaan henkilön osoite-, asuinpaikka- ja kotikuntatiedon luovuttamista väestötietojärjestelmästä vain sellaisille viranomaisille, joilla on oikeus turvakiellon alaisten tietojen käsittelyyn. Turvakielto ei ulotu muihin mahdollisiin osoitetiedon sisältäviin henkilörekistereihin.

Naantalin kaupungilla on määritelty erikseen työntekijä, jolle on anottu Digi- ja väestötietovirastosta suorakäyttöoikeudet väestötietojärjestelmään, ja hän voi tarvittaessa katsoa turvakieltohenkilön osoitteen. Hän ei saa luovuttaa tietoja edelleen eikä antaa niitä sivullisen nähtäväksi tai käsiteltäväksi, jollei laissa toisin säädetä. Turvakieltohenkilölle lähetettävät viestien osalta otetaan yhteyttä kaupungin työntekijään, jolla on suorakäyttöoikeudet väestötietojärjestelmään. Hän selvittää turvakieltohenkilön osoitteen ja huolehtii viestien lähettämisestä vastaanottajalle.

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

6. Erityisiä henkilöryhmiä koskeva käsittely

Erityisiin henkilöryhmiin 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.

6.1. 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.

6.2. 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.

7. Rekisteröidyn oikeudet

Rekisteröidyllä henkilöllä on:

- 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

7.1. Oikeus saada pääsy tietoihin

Rekisteröidyllä henkilöllä on oikeus pyytää Naantalin kaupungilta pääsy häntä itseään koskeviin henkilötietoihin. Rekisteröidyllä on oikeus tarkastaa, mitä häntä koskevia henkilötietoja asiakasrekisteriin on tallennettu tai ettei rekisterissä ole häntä koskevia tietoja. Huoltajalla on pääsääntöisesti oikeus tarkastaa myös lastaan koskevat tiedot.

Tarkastuspyyntö tehdään henkilökohtaisesti käynnin yhteydessä tai omakätisellä allekirjoituksella tai vastaavalla tavalla varmennetulla asiakirjalla tai henkilökohtaisesti rekisterinpitäjän luona. Pyyntöä varten on laadittu lomake, joka löytyy Naantalin internetsivuilta
nuutti.naantali.fi/tietosuojajatietoturva/Documents/Rekisteritietojen tarkastuspyynto.pdf
ja toimintayksiköstä. Asiakkaan henkilöllisyys varmennetaan ennen tietojen antamista.

Asiakkaalla on oikeus tutustua ja nähdä itseään koskevat asiakastiedot ja pyynnöstä saada kopiot niistä kirjallisena. Pääsääntöisesti tarkastusoikeus toteutetaan siinä yksikössä, jossa tiedot ovat syntyneet. Kun rekisteröity pyytää omia tietojaan, tiedot toimitetaan hänelle ilman aiheetonta viivytystä ja joka tapauksessa kuukauden kuluessa pyynnön vastaanottamisesta. Jos pyyntöjä on monta tai ne ovat monimutkaisia, määräaikaa voidaan tarvittaessa jatkaa enintään kahdella kuukaudella. Jos määräaikaa jatketaan, kaupunki ilmoittaa tietojen pyytäjälle asiasta kuukauden kuluessa pyynnön vastaanottamisesta. Määräajan jatkaminen on perusteltava.

Tarkastusoikeus voidaan evätä ainoastaan poikkeustapauksissa. Epäämisperusteena voi olla esimerkiksi, että tiedon antaminen saattaisi aiheuttaa vakavaa vaaraa asiakkaan terveydelle tai hoidolle taikka jonkun muun oikeuksille. Jos tarkastusoikeus evätään, asiakkaalle annetaan kirjallinen kieltäytymistodistus, jossa mainitaan kieltäytymisen syyt. Asiakkaalla on oikeus saattaa asia tietosuojavaltuutetun ratkaistavaksi. Ulkopuolisella ei ole tarkastusoikeutta, vaikka häntä koskevia tietoja voi olla tallennettuna asiakasta koskeviin tietoihin.

Tarkastusoikeus on maksutonta kerran vuoden aikana toteutettuna.

7.2. Oikeus tiedon oikaisemiseen

Rekisteröidyllä henkilöllä on oikeus pyytää Naantalin kaupungilta häntä itseään koskevien epätarkkojen ja virheellisten henkilötietojen oikaisemista ilman aiheetonta viivytystä. Muutokset tehdään siten, että rekisteriin jää näkyviin tiedot tehdystä korjauksesta, tekijästä ja korjauspäivämäärästä ja alkuperäinen merkintä on mahdollista nähdä jälkikäteen. Pyyntöä varten on laadittu lomake, joka löytyy Naantalin internetsivuilta http://nuutti.naantali.fi/tietosuojajatietoturva/Documents/Rekisteritietojen korjaamisvaatimus.pdf ja toimintayksiköstä. Asiakkaan tulee pyynnössään yksilöidä ja perustella tarkasti, mitä tietoa vaaditaan korjattavaksi ja mikä on asiakkaan mielestä oikea tieto ja millä tavalla korjaus pyydetään tekemään. Asiakkaan henkilöllisyys varmennetaan ennen tietojen oikaisemista.

Jos tarkastusoikeus evätään, asiakkaalle annetaan kirjallinen kieltäytymistodistus, jossa mainitaan kieltäytymisen syyt. Asiakkaalla on oikeus saattaa asia tietosuojavaltuutetun ratkaistavaksi.

7.3. Oikeus tietojen poistamiseen

Rekisteröidyllä henkilöllä on oikeus pyytää Naantalin kaupungilta häntä itseään koskevien tietojen poistamista ilman aiheetonta viivytystä. Oikeus tunnetaan myös nimellä oikeus tulla unohdetuksi.

Tätä oikeutta ei ole, jos tietojen käsittely on tarpeen

- sananvapautta ja tiedonvälityksen vapautta koskevan oikeuden käyttämiseksi
- rekisterinpitäjään sovellettavaan unionin oikeuteen tai jäsenvaltion lainsäädäntöön perustuvan, käsittelyä edellyttävän lakisääteisen velvoitteen noudattamiseksi tai jos käsittely tapahtuu yleistä etua koskevan tehtävän suorittamista tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämistä varten
- kansanterveyteen liittyvää yleistä etua koskevista syistä
- yleisen edun mukaisia arkistointitarkoituksia tai tieteellisiä tai historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten, jos oikeus saada tiedot poistetuksi todennäköisesti estää kyseisen käsittelyn tai vaikeuttaa sitä suuresti
- oikeudellisen vaateen laatimiseksi, esittämiseksi tai puolustamiseksi.

Kun ei ole kysymys edellä mainituista tilanteista, rekisterinpitäjällä on velvollisuus poistaa henkilötiedot ilman aiheetonta viivytystä, jos

- henkilötietoja ei enää tarvita niihin tarkoituksiin, joita varten ne kerättiin tai joita varten niitä muutoin käsiteltiin
- rekisteröity peruuttaa suostumuksen, johon käsittely on perustunut, eikä käsittelyyn ole muuta laillista perustetta
- rekisteröity vastustaa henkilötietojensa käsittelyä suoramarkkinoinnin tarkoituksiin tai käyttää vastustamisoikeuttaan muutoin, eikä käsittelyyn ole olemassa perusteltua syytä
- henkilötietoja on käsitelty lainvastaisesti
- henkilötiedot on poistettava unionin oikeuteen tai jäsenvaltion lainsäädäntöön perustuvan rekisterinpitäjään sovellettavan lakisääteisen velvoitteen noudattamiseksi
- henkilötiedot on kerätty tietoyhteiskunnan palvelujen tarjoamisen yhteydessä.

Rekisterinpitäjän on mahdollisuuksien mukaan ilmoitettava henkilötietojen poistamisesta jokaiselle vastaanottajalle, jolle henkilötietoja on luovutettu. Rekisterinpitäjän on ilmoitettava rekisteröidylle näistä vastaanottajista, jos rekisteröity sitä pyytää.

7.4. Oikeus käsittelyn rajoittamiseen

Rekisteröidyllä henkilöllä on oikeus pyytää Naantalin kaupungilta häntä itseään koskevien tietojen käsittelyn rajoittamista.

Oikeus on olemassa seuraavissa tilanteissa:

- Rekisteröity kiistää henkilötietojen paikkansapitävyyden. Tällöin käsittelyä rajoitetaan ajaksi, jonka kuluessa rekisterinpitäjä voi varmistaa niiden paikkansapitävyyden.
- Käsittely on lainvastaista, mutta rekisteröity vastustaa henkilötietojen poistamista ja vaatii sen sijaan niiden käytön rajoittamista.
- Rekisterinpitäjä ei enää tarvitse kyseisiä henkilötietoja käsittelyn tarkoituksiin, mutta rekisteröity tarvitsee niitä oikeudellisen vaateen laatimiseksi, esittämiseksi tai puolustamiseksi.
- Rekisteröity on vastustanut henkilötietojen käsittelyä muuhun kuin suoramarkkinointitarkoitukseen, ja odotetaan sen todentamista, syrjäyttävätkö rekisterinpitäjän edut rekisteröidyn edut.

Jos Naantalin 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.

7.5. Oikeus siirtää tiedot järjestelmästä toiseen

Rekisteröidyllä henkilöllä on oikeus siirtää häntä itseään koskevat tiedot järjestelmästä toiseen.

Oikeutta sovelletaan

- ainoastaan henkilötietojen automaattiseen käsittelyyn
- kun henkilötiedot koskevat rekisteröityä ja ovat hänen toimittamiaan
- kun henkilötietojen käsittely perustuu suostumukseen tai sopimukseen
- kun tietojen siirto ei vaikuta haitallisesti kolmansien osapuolten oikeuksiin ja vapauksiin.

Naantalin 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, siirto-oikeuteen kuuluu myös tietojen siirtäminen suoraan rekisterinpitäjältä toiselle edellyttäen, että se on teknisesti mahdollista. Ennen tietojen luovuttamista toiselle rekisterinpitäjälle, Naantalin kaupungin on varmistettava, että toinen rekisterinpitäjä toimii rekisteröidyn puolesta. Naantalin 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.

7.6. Vastustamisoikeus

Rekisteröidyllä henkilöllä on tietyissä tilanteissa oikeus vastustaa henkilötietojensa käsittelyä eli pyytää, että niitä ei käsiteltäisi ollenkaan.

Kun tietoja käsitellään yleistä etua koskevan tehtävän suorittamiseksi, rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi tai rekisterinpitäjän tai kolmannen osapuolten oikeutettujen etujen toteuttamiseksi, rekisteröity voi vastustaa käsittelyä henkilökohtaiseen erityiseen tilanteeseensa liittyvällä perusteella.

Tällöin tietojen käsittely on lopetettava, paitsi jos

- rekisterinpitäjä voi osoittaa, että käsittelyyn on olemassa huomattavan tärkeä ja perusteltu syy, joka syrjäyttää rekisteröidyn edut, oikeudet ja vapaudet, tai
- käsittely on tarpeen oikeusvaateen laatimiseksi, esittämiseksi tai puolustamiseksi.

7.7. Oikeus riitauttaa automaattinen yksittäispäätös

Rekisteröidyllä henkilöllä on oikeus vaatia, että häntä koskevat päätökset tekee ihminen.

Rekisteröidyllä on oikeus olla joutumatta sellaisen päätöksen kohteeksi, joka perustuu pelkästään automaattiseen käsittelyyn, kuten profilointiin, ja jolla on häntä koskevia oikeusvaikutuksia tai joka vaikuttaa häneen vastaavalla tavalla merkittävästi.

7.8. Oikeus tehdä valitus valitusviranomaiselle

Henkilöllä, jonka henkilötietoja on Naantalin 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.

8. Rekisterinpitäjän velvollisuudet

8.1. Rekisteröidyn informointi

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

8.2. Rekisteriselosteet

Henkilötietoja kerätään eri rekistereihin tietojen käyttötarkoituksen 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

Palvelualojen tietosuojan vastuuhenkilöt huolehtivat rekisteriselosteiden laatimisesta. Selosteet tehdään kaupungin rekisteriselostepohjalle.

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.

Palvelualojen 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.

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.

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.

Perusohjeistus tietosuojasta ja –turvasta on Naantalin kaupungilla toteutettu verkkokoulutuksena. Kaikkien Naantalin kaupungin palveluksessa olevien tulee suorittaa tietosuojaan ja tietoturvaan liittyvät koulutusosiot. Koulutukset uusitaan säännöllisesti. Verkkokoulutuksien suorittamista seurataan

raportoinnilla esimiehille. Palvelualat perehdyttävät henkilötietoja käsittelevän henkilökuntansa tietosuoja-asetuksen mukaiseen toimintaan sekä valvovat sen noudattamista.

8.5. Osoitusvelvollisuus

Osoitusvelvollisuus on tietosuoja-asetuksessa säädetty velvoite, jonka mukaan rekisterinpitäjä vastaa ja sen on pystyttävä osoittamaan, että tietosuoja-asetuksen henkilötietojen käsittelyä koskevia periaatteita on noudatettu.
Naantalin kaupunki toteuttaa osoitusvelvollisuutta tuottamalla muun muassa seuraavia dokumentteja ja sisältöä:

- 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
- 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.

9. Tietoturva

Kukin palveluala 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.

9.1. 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.

9.2. Tietoturvan ohjeet toimittajalle

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

Yleisiin ohjeisiin tulee lisätä ainakin toimittajayrityksen tiedot, erityisesti yhteystiedot palveluseurantaa varten. 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 Naantalin ja palvelutoimittajan välillä, millaisia tietoliikenne-, palomuuri-, haittaohjelma- tai päivitysjärjestelyjä vaaditaan, miten tiedot tulee hävittää ja kuinka pidetään käyttökirjanpitoa tietojen käsittelystä (lokeja).

9.3. 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 muututtua niitä ei enää tarvita. Kaikkien käyttäjätunnusten ajanmukaisuus tulee määräajoin tarkastaa.

10. Tietoturvaloukkauksista ilmoittaminen

10.1. 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.

10.2. Kaikki tietoturvaloukkaukset on dokumentoitava

Dokumentoi kaikki henkilötietojen tietoturvaloukkaukset sekä niiden vaikutukset ja toteutetut korjaavat toimet riippumatta siitä, mitä toimenpiteitä tietoturvaloukkauksesta lopulta seuraa.

10.3. Tietoturvaloukkauksesta ilmoittaminen tietosuojavaltuutetulle

Henkilötietojen tietoturvaloukkauksesta täytyy ilmoittaa tietosuojavaltuutetulle, jos loukkauksesta voi aiheutua riski luonnollisten henkilöiden oikeuksille ja vapauksille.

Henkilötietojen tietoturvaloukkauksesta on ilmoitettava tietosuojavaltuutetun toimistolle ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa siitä, kun rekisterinpitäjä on tullut tietoiseksi tietoturvaloukkauksesta. Jos ilmoitusta ei tehdä 72 tunnin kuluessa, rekisterinpitäjän on toimitettava tietosuojavaltuutetun toimistolle perusteltu selitys.

10.4. Henkilötietojen tietoturvaloukkauksesta ilmoittaminen rekisteröidylle

Henkilötietojen tietoturvaloukkauksesta on ilmoitettava rekisteröidylle, jos se todennäköisesti aiheuttaa korkean riskin tämän oikeuksille ja vapauksille. Rekisterinpitäjän on tällöin ilmoitettava tapahtuneesta tietoturvaloukkauksesta rekisteröidylle ilman aiheetonta viivytystä, mutta tuntimääräistä aikarajaa ei ole määritelty.

Rekisteröidylle on ilmoitettava:

- selkeä ja yksinkertainen kuvaus tapahtuneesta henkilötietojen tietoturvaloukkauksesta
- tietosuojavastaavan nimi ja yhteystiedot tai muu yhteyspiste, josta voi saada lisätietoa
- henkilötietojen tietoturvaloukkauksen todennäköiset seuraukset
- toimenpiteet, joita rekisterinpitäjä on ehdottanut tai jotka se on toteuttanut henkilötietojen tieto-

turvaloukkauksen johdosta, tarvittaessa myös toimenpiteet mahdollisten haittavaikutusten lieventämiseksi

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

Jos rekisterinpitäjä ei ole vielä ilmoittanut henkilötietojen tietoturvaloukkauksesta rekisteröidylle, valvontaviranomainen voi vaatia ilmoituksen tekemistä.

- 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

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

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.

11. Tietosuojaa koskeva vaikutustenarviointi

11.1. Mikä on vaikutustenarviointi ja mitä se sisältää?

Tietosuojaa koskevan vaikutuksenarvioinnin 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.

11.2. 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

11.3. 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.

11.4. Vaikutustenarvioinnin tekemisen vastuut

Rekisterinpitäjä tekee vaikutustenarvioinnin yhdessä henkilötietojen käsittelijöiden kanssa. Vastuu vaikutustenarvioinnin tekemisestä on sillä palvelualalla, 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.

11.5. 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.

11.6. Vaikutustenarvioinnin tekeminen

12. Tietosuojalainsäädännön rikkomisen seuraamukset

12.1. 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.

12.2. 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.

12.3. 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.

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

12.4. 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.

13. Sopimukset ja hankinnat

13.1. Tietosuoja-asetuksen vaikutus sopimusehtoihin

Arvioitaessa tietosuoja-asetuksen asettamia velvoitteita sopimusehtojen kannalta, lähtökohdaksi on otettava asetuksen 28 artiklan 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.

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 sekä huomioitava tietosuojavaatimukset järjestelmälle tai palvelulle asetettavissa vaatimuksissa.

13.2. 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

14. Henkilötietojen suoja päätösvalmistelussa

14.1. 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.

14.1.1. Esityslista 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.

14.1.2. 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.

14.1.3. 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 tietoverkossa 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.

14.1.4. Henkilötietojen poistaminen päätöksestä oikaisu- ja 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.

14.2. 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.

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.