YPÄJÄN KUNNAN TIETOSUOJAPOLITIIKKA

Hyväksytty kunnanhallituksessa 16.5.2018
(§ 101, LIITE 19)

Sisällys

JOHDANTO

Kunnallisten palveluiden tuottaminen perustuu tietoon ja sen käsittelyyn. Tietoa on sekä salassa pidettävää että julkista. Lisäksi teknologian kehittyminen on lisännyt henkilötietojen käsittelyä, jolloin tietosuoja ja tietoturva ovat kasvattaneet merkitystään ja tulleet pysyväksi osaksi hyvää hallintotapaa. Puutteellinen tietoturvallisuus voi vaarantaa kunnan ja sen asiakkaiden etuja sekä aiheuttaa lisätyötä ja -kustannuksia. Organisaation menettämä luottamus ja maine on vaikea palauttaa.

Kuntien toimintaan vaikuttavat julkisuus- ja henkilötietolainsäädäntö, jotka säätelevät toiminnan avoimuutta. Julkisuuslaki koskee lähinnä asiakirjatietoja ja niiden käsittelyä, henkilötietolaki henkilötietojen ja -rekistereiden käsittelyä. Vuonna 2018 toukokuussa sovellettava EU:n tietosuoja-asetus (General Data Protection Regulation, GDPR 679/2016) korvaa EU:n jäsenmaata suoraan velvoittavana lainsäädäntönä nykyisen kansallisen henkilötietolain.

Lainsäädäntöuudistusten 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. Tietosuoja-asetus tuo sekä rekisterinpitäjille että henkilötietojen käsittelijöille uusia tehtäviä ja velvollisuuksia.

Uutena asiana rekisterinpitäjälle on tullut osoitusvelvollisuus. Kun vanhan henkilötietolain aikana riitti, että säännöksiä noudatetaan, nyt rekisterinpitäjän on pystyttävä osoittamaan, että asetuksen tietosuojaperiaatteita ja vaatimuksia on noudatettu. Tämä tarkoittaa mm. henkilötietojen käsittelytoimien tarkempaa dokumentointia. Asetus pitää myös sisällään uusia oikeuksia rekisteröidyille.

Tämä asiakirja koostuu kahdesta osasta: ensimmäisessä osassa esitellään Ypäjän kunnan tietosuojaperiaatteet eli tietosuojapolitiikka ja toisessa osassa annetaan ohjeistuksia henkilötietojen käsittelemiseen. Asiakirja koskee henkilötietojen käsittelyä, jossa Ypäjän kunta toimii rekisterinpitäjänä.

Tietosuojapolitiikka sisältää ne henkilötietojen käsittelyyn liittyvät periaatteet, vastuut ja seuraamusjärjestelmän, joita noudatetaan Ypäjän kunnan tietosuojan toteuttamisessa ja kehittämisessä. Tietosuojapolitiikka antaa pohjan ohjeiden ja määräysten soveltamiselle.

Toisen osan ohjeiden tarkoituksena on selventää henkilötietojen käsittelyssä noudatettavia tietosuojaperiaatteita ja täsmentää EU:n tietosuoja-asetuksen edellyttämiä toimenpiteitä.

Tämä asiakirja koskee koko kuntaorganisaatiota ja sen henkilöstöä mukaan lukien kuntakonsernin sekä niitä kunnan sidosryhmien edustajia, jotka toimeksiantojensa puitteissa käsittelevät Ypäjän kunnan omistamaa tai hallinnoimaa tietoa.

KÄSITTEET

Henkilörekisteri

Henkilörekisteri on mikä tahansa jäsenneltyä henkilötietoa sisältävä tietojoukko, josta tiedot ovat saatavilla tietyin perustein. Henkilörekisteri sisältää samaa käyttötarkoitusta varten henkilötietoja. Tietomassa voi olla keskitetty, hajautettu tai jaettu eri perustein. esim. jäsenrekisteri ja käyttäjärekisteri ovat henkilörekistereitä.

Henkilötieto

Henkilötiedolla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja. Tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen, käyttäjätunnuksen tjms. taikka yhden tai useamman hänelle tavanomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella.

Henkilötiedon käsittelijä

Henkilötietojen käsittelijä on se henkilö, viranomainen, virasto tai muu taho, joka käsittelee henkilötietoja rekisterinpitäjän lukuun.

Henkilötietojen käsittely

Henkilötiedon käsittelyllä tarkoitetaan toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietojen kokoelmiin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti, esim. tietojen kerääminen, tallentaminen, järjestäminen, jäsentäminen, säilyttäminen, muokkaaminen tai muuttaminen, haku, kysely, käyttö, tietojen luovuttaminen siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittaminen tai yhdistäminen, rajoittaminen, poistaminen tai tuhoaminen.

Rekisterinpitäjä

Rekisterinpitäjä on se taho, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Toisin sanoen, rekisterinpitäjä on se henkilö tai organisaatio, jonka käyttöä varten rekisteri perustetaan ja jolla on oikeus määrätä rekisterin käytöstä.

Tietosuoja

Tietosuojalla tarkoitetaan kansalaisten yksityisyyden suojaamista sekä oikeuksien, etujen, vapauksien ja oikeusturvan turvaamista henkilötietoja käsiteltäessä.

Tietosuojavastaava

Nimetty henkilö, jonka tehtävänä on mm. seurata henkilötietojen käsittelyn lainmukaisuutta ja auttaa organisaatiota toteuttamaan lainsäädännön asettamat velvoitteet. Asema on itsenäinen ja riippumaton. Tietosuojavastaava raportoi suoraan rekisterinpitäjän ylimmälle johdolle, joka on päävastuussa henkilötietojen käsittelyn lainmukaisuudesta.

Tietosuojavastaava antaa tietoja ja neuvoja rekisterinpitäjälle ja työntekijöille henkilötietojen käsittelyyn liittyen. Hän seuraa asetuksen noudattamista omassa organisaatiossaan ja hänen vastuulleen kuuluu myös tietosuoja-asioiden kouluttaminen henkilöstölle. Tietosuojavastaava neuvoo vaikutustenarviointeihin liittyen ja toimii yhteyshenkilönä valvontaviranomaiseen päin.

Jokaisen viranomaisen ja julkishallinnon elimen, joka ei ole tuomioistuin, on nimitettävä tietosuojavastaava. Tietosuojavastaava voi olla organisaation henkilöstön jäsen tai hoitaa tehtäviään palvelusopimuksen perusteella. Konserni, samoin kuin useampi viranomainen tai julkishallinnon elin, voi nimittää yhteisen tietosuojavastaavan. Tietosuojavastaava voi tehtävänsä ohella suorittaa muita tehtäviä, mutta nämä tehtävät eivät saa aiheuttaa intressiristiriitoja.

Tietosuojavastaava on otettava asianmukaisesti ja riittävän ajoissa mukaan kaikkien henkilötietojen suojaa koskevien kysymysten käsittelyyn. Hänelle on asetuksen mukaan annettava riittävät resurssit sekä pääsyn henkilötietoihin ja käsittelytoimeen. Hänellä on myös oikeus asetuksen perusteella resursseihin asiantuntemuksen ylläpitämiseksi.

Rekisterinpitäjä tai henkilötietojen käsittelijä ei saa erottaa tai rangaista tietosuojavastaavaa sen vuoksi, että hän on hoitanut tehtäviään tietosuojavastaavana.

Tietoturva

Tietoturvalla tarkoitetaan niitä teknisiä ja hallinnollisia toimenpiteitä, joilla pyritään tietosuojan toteuttamiseen.

OSA I: TIETOSUOJAPOLITIIKKA

Tietosuojan tavoitteet

Yksityisyydensuoja ja henkilötietojen suoja on jokaisen perusoikeus. Ypäjän kunnan tavoitteena on edistää hyvää tietojenkäsittelytapaa sekä varmistaa tietojenkäsittelyn turvallisuus, sekä tehtävien sujuva ja häiriötön toiminta kunnassa. Tietoja käsitellään niin, että kaikki osapuolet voivat luottaa käsittelyn asianmukaisuuteen.

Ypäjän kunta määrittää tarvittavat suojatoimet ottamalla huomioon mm. käytettävissä olevat tilat, tekniikan, toteuttamiskustannukset, käsittelyn luonteen ja laajuuden, asiayhteyden ja tarkoituksen sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat riskit.

Hyvän tietosuojan tason saavuttamiseksi jokaisen tietoa käsittelevän henkilön tulee ymmärtää tietojen käsittelyn periaatteet: mitä tietoa saa käsitellä, missä tarkoituksessa ja milloin tietoa saa käsitellä sekä mitkä ovat rekisteröidyn oikeudet.

Organisaatio ja vastuut

Henkilötietojen käsittelyn lainmukaisuudesta vastaa ensisijaisesti Ypäjän kunnan johto. Vastuu ei riipu siitä, onko joitakin organisaation toimintoja ulkoistettu vai ei. Johdolla on vastuu huolehtia mm. tietoturvatyön riittävästä resursoinnista ja tietosuojan huomioon ottamisesta suunnitelmissa.

Kukin toimialueen johtaja vastaa omalla toimialueellaan tietosuojan lainmukaisuudesta. Lisäksi yksiköiden esimiehet valvovat tietosuojan toteutumista omassa yksikössään. Jokaisen esimiehen tulee huolehtia, että tietosuoja- ja tietoturvaohjeet sekä tietoverkon käyttösäännöt perehdytetään henkilöstölle.

Organisaation tietosuojavastaava toimii tietosuoja-asioissa asiantuntijana ja yhteyshenkilönä. Tietosuojavastaavan tehtävänä on auttaa rekisterinpitäjää saavuttamaan ja ylläpitämään hyvä henkilötietojen käsittelytapa ja tietosuojan taso.

ICT-asiantuntija vastaa teknisen tietoturvan kehittämisestä, tietojärjestelmien toiminnasta, hoidosta ja turvallisuudesta saamiensa resurssien ja toimintavaltuuksien puitteissa.

Jokaisella, joka käsittelee Ypäjän kunnan omistamaa tietoa, on omalta osaltaan henkilökohtainen vastuu kokonaisturvallisuudesta. Jokainen tietoja ja tietojärjestelmiä käyttävä on velvollinen ilmoittamaan havaitsemistaan tietoturvallisuuden puutteista ohjeistetulla tavalla. On syytä muistaa, että parhaimmankin turvallisuusajattelun toteutuminen on henkilöstön käsissä.

Tietosuojan toteuttaminen

Hyvän tietosuojan tason toteuttaminen vaatii organisaation kaikille tasoilla ulottuvia jatkuvia toimia, jolloin taataan organisaation häiriötön toiminta sekä normaali- että häiriötilanteissa. Toteuttaminen tapahtuu erilaisten hallinnollisten ja teknisten toimenpiteiden avulla. Tietosuoja tulee huomioida kaikessa toiminnassa niin manuaalisessa kuin sähköisessä henkilötietojen käsittelyssä sekä puhutussa ja kirjoitetussa tiedossa.

Henkilötietojen käsittelyssä noudatetaan seuraavia yleisessä EU:n tietosuoja-asetuksessa annettuja tietosuojaperiaatteita:

- Henkilötietoja käsitellään **lainmukaisesti, kohtuullisesti** sekä rekisteröidyn kannalta **läpinäkyvästi.** Rekisteröidylle tulee olla läpinäkyvää, miten heitä koskeva tietoja kerätään ja käytetään, sekä missä määrin henkilötietoja käsitellään tai on aikeissa käsitellä.
- Henkilötietojen kerääminen tulee olla **sidonnainen käyttötarkoitukseen** ja tietojen kerääminen tulee tapahtua tiettyä, nimenomaista ja laillista tarkoitusta varten. Kerättyä tietoa ei saa käyttää myöhemmin tarkoitukseen, jolla ei ole sidonnaisuutta kerättyyn käyttötarkoitukseen.
- Henkilötietojen kerääminen tulee rajata ja **minimoida tarpeelliseen tietoon** suhteessa keräämisen tarkoitukseen ja henkilötietojen on oltava asianmukaisia sekä olennaisia.
- Henkilötietojen on oltava **täsmällisiä** ja tarvittaessa päivitettyjä sekä rekisterinpitäjän on kohtuullisen toimenpitein varmistettava, että käsittelyn tarkoituksiin nähden epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä.
- Henkilötiedot on **säilytettävä** muodossa, josta rekisteröity on tunnistettavissa **ainoastaan niin kauan kuin se on tarpeen** tietojen käsittelyä varten. Tietoja voidaan säilyttää kauemmin, mikäli tietoja käsitellään ainoastaan yleisen edun mukaisia arkistointitarkoituksia varten tai tietoja käytetään historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten.
- Henkilötietojen käsittelyssä on varmistettava tietojen asianmukainen turvallisuus ja siten tietojen **eheys ja luottamuksellisuus**. Tietoja tulee suojata luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta, jossa on käytettävä asianmukaisia teknisiä tai organisatorisia toimia.

Lait ja asetukset

Ypäjän kunnan tietosuojan ja tietoturvan käytänteet noudattavat voimassa olevia säädöksiä, määräyksiä, ohjeita ja suosituksia. Tietoturvaratkaisujen tulee noudattaa myös taloudellisia realiteetteja, eivätkä ne saa vaikeuttaa merkittävästi tietojärjestelmien hyötykäyttöä ja asiakaspalvelua. Organisaation omat päätökset, määräykset ja ohjeet eivät saa olla ristiriidassa Ypäjän kunnan tietosuojapolitiikan kanssa.

Tietosuojaan liittyvä keskeinen lainsäädäntö:

- EU:n yleinen tietosuoja-asetus (679/2016)
- Suomen perustuslaki (731/1999)
- Hallintolaki (434/2003)
- Hallintolain käyttölaki (586/1996)
- Laki viranomaisten toiminnan julkisuudesta (621/1999)
- Asetus viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999)
- Laki kunnallisesta viranhaltijasta (304/2003)
- Työsopimuslaki (55/2001)
- Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä (VAHTI 7/2009)
- Arkistolaki (831/1994): Asiakirjojen laatiminen, säilyttäminen ja käyttö
- Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003)
- Laki sähköisen viestinnän palveluista (917/2014)
- Rikoslaki (39/1889)
- Vahingonkorvauslaki (412/1974)

Lisäksi

- Hallituksen esitys eduskunnalle laeiksi Euroopan unionin verkko- ja tietoturvadirektiivin täytäntöönpanoon liittyvien lakien muuttamisesta (HE 192/2017 vp.)
- Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista (812/2000)
- Laki potilaan asemasta ja oikeuksista (785/1992)
- Laki terveydenhuollon ammattihenkilöistä (559/1994)

Rikkomukset ja seuraamukset

Jokainen Ypäjän kunnan tietojärjestelmien käyttäjä on velvollinen noudattamaan Ypäjän kunnan tietosuojapolitiikkaa, tietoverkon käyttösääntöjä sekä tietosuoja- ja tietoturvaohjeita. Tietojen käsittelijä on vastuussa mahdollisesta vahingosta, jos se ei ole noudattanut tietosuoja-asetuksessa käsittelijälle nimenomaisesti asetettuja velvoitteita tai rekisterinpitäjän lainmukaista ohjeistusta. Havaitut rikkomukset raportoidaan johdolle ja tietosuojavastaavalle. Rikkomuksen tekijä saatetaan edesvastuuseen ja häntä vastaan ryhdytään rikkomuksen luonteen vaatimiin toimenpiteisiin. Vakaviin tietosuojarikkomuksiin liittyvä sisäinen ja julkinen tiedottaminen hoidetaan tapauskohtaisesti johdon tai johdon valtuuttaman henkilön toimesta.

OSA II: TIETOSUOJA – tietojen käsitteleminen

Henkilötietojen käsittely

Henkilötiedolla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja, ei pelkästään nimeä ja henkilötunnusta vaan myös henkilön ominaisuuksia (ks. Käsitteet).

Henkilötietoja käsiteltäessä tulee toteuttaa kansalaisten yksityiselämän suojaa ja muita perusoikeuksia sekä edistää hyvää tiedonhallintatapaa. Tietoturvanäkökulmasta merkittäviä käsittelyvaiheita ovat tiedon luominen, käyttäminen, muuttaminen, tallettaminen, säilyttäminen, siirtäminen, jakelu, kopioiminen, arkistointi ja hävittäminen eli kaikki henkilötietoihin liittyvät aktiiviset ja passiiviset toimenpiteet.

Henkilötietojen kerääminen

Henkilötietojen käsittely alkaa niiden keräämisestä. Henkilötietoja saa kerätä ja käsitellä vain, jos *jokin* alla olevista perusteista täyttyy. Henkilötietoja ei saa kerätä perusteetta tai mahdollista tulevaa, vielä tunnistamatonta tarvetta varten:

- SUOSTUMUS ja TARKOITUSPERUSTE
  - Rekisteröity on antanut **suostumuksensa** henkilötietojen käsittelyyn yhtä tai useampaa erityistä tarkoitusta varten.
- SOPIMUSPERUSTE
  - Käsittely on tarpeen sellaisen **sopimuksen** täytäntöön panemiseksi, jossa rekisteröity on osapuolena tai sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä.
- LAKISÄÄTEISYYS (legitiimisyysperuste)
  - Käsittely on tarpeen rekisterinpitäjän **lakisääteisen velvoitteen** noudattamiseksi.
- EDUNVALVONTA- ja JULKISOIKEUSPERUSTE
  - Käsittely on tarpeen rekisteröidyn tai toisen luonnollisen **henkilön** elintärkeiden **etujen suojaamiseksi**.
  - Käsittely on tarpeen **yleistä etua** koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan **julkisen vallan** käyttämiseksi.
  - Käsittely on tarpeen **rekisterinpitäjän itsensä** tai **kolmannen osapuolen oikeutettujen etujen** toteuttamiseksi, paitsi milloin henkilötietojen suojaa edellyttävä rekisteröidyn edut tai perusoikeudet ja -vapaudet syrjäyttävät tällaiset edut, erityisesti jos rekisteröity on lapsi.

Iso osa kunnan tietojen keräämisestä perustuu lakisääteisten velvoitteiden hoitamiseen. Jos käsittely ei perustu lakisääteisen velvoitteen hoitamiseen ja rekisteröidyltä kysytään suostumus henkilötietojen käsittelyyn, on rekisteröityä tiedotettava suostumuksen merkityksestä ennen suostumuksen antamista. Suostumus on pätevä vain, kun se on vapaaehtoinen, yksilöity, tietoinen, yksiselitteinen tahdonilmaisu, joka on selkeästi ymmärrettävissä. Suostumus kysytään kirjallisena (suostumuslomakkeella), jolloin pystytään myöhemmin osoittamaan, kuka suostumuksen on antanut, kenelle suostumus on annettu ja mihin tarkoitukseen se on annettu. Jos henkilötietojen käyttötarkoitus muuttuu, tulee tähän kysyä uusi suostumus.

Arkaluonteinen henkilötieto eli erityisiin henkilötietoryhmiin kuuluva tieto

Erityisiä henkilötietoryhmiä koskevia tietoja, eli arkaluonteisia henkilötietoja ei saa lähtökohtaisesti lainkaan käsitellä. Näitä tietoja ovat muun muassa rotuun tai etniseen alkuperään, poliittiseen mielipiteeseen, uskonnolliseen tai filosofiseen vakaumukseen tai ammattiliiton jäsenyyteen liittyvät tiedot. Lisäksi geneettisiä tai biometrisiä tietoja, joista henkilö voidaan yksiselitteisesti tunnistaa, terveyttä koskevia tietoja tai luonnollisen henkilön seksuaalista käyttäytymistä ja suuntautumista koskevia tietoja ei lähtökohtaisesti saa käsitellä.

Erityisiä henkilötietoryhmiä koskevia tietoja käsitellään
a) suostumuksen perusteella,
b) henkilön elintärkeiden etujen suojaamiseksi tai
c) jos käsittely on tarpeen yleistä etua koskevasta syystä lainsäädännön nojalla.

Alle 16-vuotiaiden lasten henkilötietojen käsittely ei ole sallittua ilman vanhemman suostumusta. (Kansallisessa lainsäädännössä eli uudistettavassa henkilötietolaissa on vielä mahdollisuus soveltaa alempaa ikärajaa, joka voi alimmillaan olla 13 vuotta [tilanne toukokuu 2018]).

Henkilörekisteri ja henkilötietojen elinkaari

Henkilötiedoista syntynyt henkilörekisteri on mikä tahansa henkilötietoluettelo, joka voi olla niin paperilla, taulukkolaskentaohjelmassa, tekstitiedostossa, tietojärjestelmässä, sähköpostissa tai arkistossa. Kunnan ja sen henkilöstön tulee tietää, mitä henkilörekistereitä heidän käytössään on, sillä tietosuoja-asetus määrää kaikki tietovarannot kartoitettavaksi ja kuvattavaksi. Henkilörekisterit tulee kuvata tietosuojaselosteissa (ks. Rekisteröidyn oikeudet).

Henkilörekisteriin tulee tallentaa vain rekisterin käyttötarkoituksen ja muun hallintotoiminnan kannalta tarpeellisia tietoja. Henkilötietoja saa käyttää ainoastaan siihen tarkoitukseen, mihin ne on kerätty. Tiedot tai koko henkilörekisteri on hävitettävä, jos se ei ole enää tarpeellinen. Henkilötietoja ei saa säilyttää ’varmuuden vuoksi’. Poikkeuksen muodostavat lakisääteiset rekisterit. Henkilötietojen säilyttämisen ja käytön aikarajat määritellään arkistonmuodostussuunnitelmassa.

Henkilötietojen käsittelijän tulee käyttää luotettavia tietolähteitä eikä henkilörekisteriin saa tallettaa tarpeettomia, puutteellisia tai vanhentuneita henkilötietoja. Tällaiset tiedot on poistettava rekisteristä.

Käyttöoikeudet, vaitiolo- ja salassapitovelvollisuus

Henkilötietoja saavat käsitellä vain ne henkilöt, joilla on siihen tehtäviensä vuoksi oikeus. Yksiköiden esimiehet päättävät kenelle tietojärjestelmien käyttöoikeuksia annetaan. Käyttöoikeudet tulee rajata henkilön työtehtävien mukaisesti. Käyttöoikeuksia myöntäessä ja muuttaessa tulee jäädä merkintä (loki tai dokumentti), jolloin käyttöoikeuksia voidaan tarvittaessa selvittää myös jälkikäteen.

Henkilötietoja käsittelevät kunnan palveluksessa olevat henkilöt tai ulkopuoliset työn suorittajat eivät saa ilmaista sivullisille tietoja toisen henkilön ominaisuuksista, henkilökohtaisista oloista tai taloudellisesta asemasta, joita he ovat saaneet tietoonsa henkilötietojen käsittelyyn liittyviä toimenpiteitä suorittaessaan tai muutoin.

Henkilötietoja käsittelevät henkilöt velvoitetaan vaitiolovelvollisuuteen työ- tai muilla sopimuksilla, ja velvoituksen on oltava voimassa työ-, sopimus- tai toimeksiantosuhteen päätyttyäkin. Henkilötietojen oikeudeton käsittely on rangaistava teko.

OHJEITA:

- Selvitä itsellesi tietojen ja asiakirjojen luokittelu ja siihen liittyvät käyttöä, luovutusta ja käsittelyä koskevat säännöt ja rajoitukset.
- Mikäli laadit salassa pidettävää asiakirjaa, vastaat tehtäviesi mukaisesti myös sen luokittelusta ja merkinnästä. Osa salassa pidettävästä aineistosta kuuluu turvaluokittelun piiriin.
- Käsittele tietoja huolellisesti käsittely- tai tallennusvälineestä riippumatta.
- Muista, että voit käyttää ja käsitellä käyttöösi saamiasi salassa pidettäviä ja arkaluonteisia tietoja vain työtehtäviesi hoitamisessa. Esimerkiksi henkilörekisterin tietojen käyttötarkoituksen vastainen käyttö on lainvastaista. Huomioi myös, että tietojärjestelmien käyttöä valvotaan.
- Varo antamasta viattomankin oloisten keskustelujen ja lomakkeiden yhteydessä tietoa salassa pidettävistä ja yksityisyyden suojan piiriin kuuluvista tiedoista.

- Kaikki ovat vaitiolovelvollisia toisten viesteistä, jotka on työtehtävissään vahingossa saanut tietoonsa.
- Tukahduta juorut.

Tietosuojaseloste

Henkilörekistereistä tulee olla laadittuna tietosuojaseloste (ent. ’rekisteriseloste’), joka kertoo mm. mitä henkilötietoja rekisteri sisältää, mitkä ovat käsittelyn tarkoitukset, mistä tiedot on saatu ja minne tietoja luovutetaan. Tietosuojaselostetta käytetään kansalaisten perusoikeuksien, yleisen tiedonsaantioikeuden toteuttamiseksi ja rekisteröidyn informoimiseksi.

Ennen henkilötietojen keräämistä rekisteröitävälle on ilmoitettava tietosuojaselosteessa seuraavat tiedot:

1) rekisterinpitäjän ja
2) tietosuojavastaavan yhteystiedot,
3) rekisterin yhteyshenkilö,
4) rekisterin nimi,
5) henkilötietojen käsittelyn tarkoitus ja oikeusperusta,
6) rekisterin tietosisältö,
7) säännönmukaiset tietolähteet,
8) säännönmukaiset tietojen luovutukset ja
9) tietojen siirto EU:n ulkopuolelle,
10) rekisterin suojauksen periaatteet,
11) henkilötietojen säilytysaika tai säilytysajan määräytymisperusteet sekä
12) rekisteröidyn oikeudet ja miten rekisteröidyt voivat niitä käyttää,
13) oikeus peruuttaa suostumus milloin tahansa,
14) oikeus tehdä valitus valvontaviranomaiselle.

Tietosuojaseloste on pidettävä jokaisen nähtävänä asianosaisessa toimintayksikössä. Seloste on pidettävä jatkuvasti ajan tasalla.

Tietosuojaselosteen jäljennös toimitetaan kunnan tietosuojavastaavalle, joka ylläpitää luetteloa Ypäjän kunnan henkilötietoja sisältävistä rekistereistä.

Rekisteröidyn oikeudet

Rekisteröidyllä on oikeus pyytää hänen henkilötietojensa käsittelyä koskevat tiedot. Tiedot on pystyttävä esittämään mahdollisimman helposti ymmärrettävässä ja tiiviissä muodossa. Näitä tietoja ovat ainakin tietosuojaselosteet, tarkastusoikeuden kohteena olevat tiedot, tiedot henkilötietojen korjaamisesta, poistamisesta, rajoittamisesta, siirrosta, tiedot käsittelyn tai profiloinnin vastustamisesta ja ilmoitukset tietoturvaloukkauksista.

Rekisteröidyn oikeus saada tietoja

Rekisteröidyllä on kohtuullisin väliajoin oikeus saada pääsy henkilötietoihin, joita hänestä on kerätty sekä tietoihin hänen henkilötietojen käsittelyyn liittyen. Kaikilla rekisteröidyillä on siis oikeus tietää ja saada ilmoitus erityisesti henkilötietojen käsittelyn tarkoituksista, käsittelyajasta, henkilötietojen vastaanottajista, käsiteltävien henkilötietojen automaattisen käsittelyn logiikasta sekä kyseisen käsittelyn mahdollisista seurauksista. Lisäksi rekisteröidyillä on oikeus saada tietoa omista oikeuksistaan suhteessa rekisterinpitäjään. Tietopyyntöjä tehdään lomakkeilla, joita saa Ypäjän kunnalta.

Rekisteröidylle on annettava tiedot ilman aiheetonta viivytystä ja viimeistään yhden **kuukauden (1 kk) kuluessa** pyynnön vastaanottamisesta. Määräaikaa voidaan tietyin edellytyksin jatkaa. Tietoja antaessa

on huomioitava, että jos tietopyyntö koskee lisäksi myös viranomaisen asiakirjaa, tulee noudatettavaksi julkisuuslain mukaiset lyhyemmät määräajat (14 pv).

Rekisteröidyn pyynnön perusteella toimitetut tiedot ja rekisterinpitäjän toimet rekisteröiden oikeuksien toteuttamiseksi ovat pääsääntöisesti **maksuttomia.** Pyydetyt tiedot pitää ensisijaisesti luovuttaa sähköisessä muodossa. Ennen tietojen luovuttamista, rekisteröidyn henkilöllisyys tulee varmistaa. Tunnettu henkilöys ei riitä.

Oikeus tietojen oikaisemiseen ja oikeus tulla unohdetuksi

Rekisteröidyllä on oikeus vaatia, että rekisterinpitäjä oikaisee ilman aiheetonta viivytystä rekisteröityä koskevat epätarkat ja virheelliset henkilötiedot. Ottaen huomioon tarkoitukset, joihin tietoja käsiteltiin, rekisteröidyllä on oikeus saada puutteelliset henkilötiedot täydennettyä, esim. toimittamalla rekisterinpitäjälle lisäselvitystä.

Rekisteröidyllä on myös oikeus vaatia, että rekisterinpitäjä poistaa rekisteröityä koskevat henkilötiedot, kun tietoja ei enää tarvita. On huomioitava, että tämä oikeus ei koske lakisääteistä rekisteriä. Tietojen poistaminen niistä ei ole mahdollista lakisääteisten tehtävien suorittamiseen liittyvän käsittelyn yhteydessä.

Oikeus käsittelyn rajoittamiseen ja vastustamisoikeus

Rekisteröidyllä on oikeus pyytää henkilötietojensa rajoittamista muun muassa, kun henkilötiedot eivät pidä enää paikkaansa tai henkilötietojen käsittely rikkoo lainsäädäntöä. Käsittelyn rajoittaminen tarkoittaa esim. tietojen siirtämistä toiseen käsittelyjärjestelmään tai käyttäjien pääsyn estämistä valittuihin henkilötietoihin.

Rekisteröidyllä on oikeus vastustaa käsittelyä suoramarkkinointitarkoituksissa ja eräissä muissa tietosuoja-asetuksessa mainituissa tilanteissa, jolloin hänen henkilötietojaan ei saa enää käsitellä ko. tarkoituksissa. Vastustusoikeus ei koske lakisääteisiä rekistereitä.

Oikeus siirtää tiedot järjestelmästä toiseen

Rekisteröidyllä on oikeus saada häntä koskevat henkilötiedot yleisesti käytössä olevassa siirtomuodossa (esim. muistitikulla) ja hänellä on oikeus toimittaa tiedot toiselle rekisterinpitäjälle. Eri rekisterinpitäjien järjestelmien ei tarvitse olla yhteensopivia. Siirto-oikeutta sovelletaan kunnassa niihin rekistereihin, jotka on kerätty vapaaehtoisten tehtävien hoitamiseen. Siirto-oikeutta ei ole, kun kyse on yleistä etua koskevan tehtävän suorittamisesta tai julkisen vallan käyttämisestä.

Ypäjän kunnalla on kirjallinen suunnitelma tietopyyntöjen käsittelemiseksi. Suunnitelma pitää sisällään vastuut ja toimenpiteet, joita noudatetaan tietopyynnön käsittelyssä.

Tietoturvaloukkauksesta ilmoittaminen

Henkilötietojen tietoturvaloukkauksen sattuessa Ypäjän kunnalla on velvollisuus ilmoittaa tietoturvaloukkauksista tietosuojaviranomaiselle ja rekisteröidylle. Tietoturvaloukkauksella tarkoitetaan loukkausta, jonka seurauksena on henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin.

Henkilötietojen käsittelijän on ilmoitettava tietoturvaloukkauksista kunnan tietosuojavastaavalle ilman aiheetonta viivytystä loukkauksen tietoonsa saatuaan. Loukkausta koskeva ilmoitus tehdään valvontaviranomaiselle (tietosuojavaltuutetulle) mahdollisuuksien mukaan 72 tunnin kuluessa loukkauksen ilmitulosta, riippumatta siitä, onko loukkaus tapahtunut omassa vai ulkopuolisen käsittelijän toiminnassa.

Rekisteröidylle henkilötietojen tietoturvaloukkauksesta ilmoitetaan ilman aiheetonta viivytystä. Ilmoituksen voi tehdä lomakkeella ”Tietoturvapoikkeamasta ilmoittaminen rekisteröidylle”. Rekisteröidylle suunnattavassa ilmoituksessa tulee kertoa vähintään seuraavassa listatut kohdat.

- Tietosuojavastaavan nimi ja yhteystiedot tai muu yhteystieto, josta rekisteröidyt voivat halutessaan kysyä lisätietoja.
- Selkeä ja yksinkertainen kuvaus tapahtuneesta.
- Tiedot siitä, millaisia vaikutuksia henkilötietojen tietoturvaloukkauksella voi todennäköisesti olla rekisteröidylle.
- Kuvaus niistä toimenpiteistä, joita rekisterinpitäjä aikoo toteuttaa tai jotka se on jo toteuttanut haittavaikutusten lieventämiseksi ja tilanteen ratkaisemiseksi riittävän yleisellä tasolla.

ilmoitusta ei kuitenkaan tarvitse tehdä, jos tietoturvaloukkauksesta ei todennäköisesti aiheudu riskiä rekisteröidyn oikeuksille. Kuitenkin myös mahdollisesta vakavasta lähellä-piti-tilanteesta olisi hyvä ilmoittaa tietosuojavastaavalle, jolloin tiedot voidaan tilastoida ja tietoturvaa voidaan kehittää.

Ypäjän kunnalla on kirjallinen suunnitelma tietosuojaloukkausten varalle. Suunnitelma pitää sisällään vastuut ja toimenpiteet, joita noudatetaan tietosuojaloukkauksen tapahtuessa.

Sopimusvaatimukset, kun henkilötietojen käsittelyä ulkoistetaan

Toimeksiantosuhteissa, annettaessa palveluita ulkopuolisen hoidettaviksi, laaditaan toimeksiannosta kirjallinen sopimus. Sopimuksessa vahvistetaan mm. käsittelyn kohde ja kesto, käsittelyn luonne ja tarkoitus, henkilötietojen tyyppi ja rekisteröityjen ryhmät ja rekisterinpitäjän velvollisuudet ja oikeudet. Toimeksiantotehtävää suorittavaa koskevat huolellisuusvelvoite, kielto käyttää saatuja tietoja ulkopuolisiin tarkoituksiin ja velvollisuus suojata saadut tiedot.
Kuntaliitto, Hansel, KL-Kuntahankinnat Oy ja Julkisten hankintojen neuvontayksikkö ovat tehneet ohjeen ”Tietosuoja-asetuksen huomioiminen kilpailutettaessa julkisia hankintoja”. Ohjeessa on myös valmiita lausekkeita sopimusehtoihin.

Seuraamukset ja hallinnolliset sanktiot

Tietosuoja-asetuksen mukaan henkilöllä, jolle on aiheutunut tietosuoja-asetuksen rikkomisen vuoksi vahinkoa, on oikeus saada täysi korvaus vahingosta joko rekisterinpitäjältä tai henkilötietojen käsittelijältä. Rekisterinpitäjällä on lähtökohtaisesti päävastuu ja henkilötietojen käsittelijän vastuu toissijaista. Käsittelijä on vastuussa vahingosta vain, jos se ei ole noudattanut tietosuoja-asetuksessa käsittelijälle nimenomaisesti asetettuja velvoitteita tai jos se ei ole noudattanut rekisterinpitäjän ohjeistusta.

Lisäksi mikäli henkilötietoja ei käsitellä lainmukaisesti ja tietosuoja-asetusta rikotaan, voi rekisterinpitäjä saada huomautuksen, varoituksen, henkilötietojen käsittelykiellon tai muun sanktion. Hallinnollisen sanktion määräämisestä päättää tietosuoja-asetuksen nojalla perustettu valvontaviranomainen.

SOVELTAMINEN

Tämä Ypäjän kunnan tietosuojapolitiikka annetaan tiedoksi jokaiselle uudelle ja vanhalle työntekijälle ja tietojärjestelmien käyttäjälle. Lisäksi henkilökunnalle annetaan säännöllistä tietoturva- ja tietosuojakoulutusta ja on laadittu erillinen tietoturva- ja tietosuojaohjeistus.

Tietosuojapolitiikkaa ja tietoturvaohjeita noudatetaan kaikessa toiminnassa ja ne koskevat kaikkia organisaation palveluksessa olevia henkilöitä, luottamushenkilöstöä sekä organisaation ulkopuolisia yhteistyökumppaneita.

Tämä tietosuojapolitiikka on voimassa toistaiseksi ja voimassaolo jatkuu, ellei sitä nimenomaisesti kumota.

LÄHTEET

EU-tietosuojan kokonaisuudistus, VAHTI-raportti 1/2016, Julkisen hallinnon ICT,
Valtionvarainministeriö 2016

Henkilöstön tietoturvaohje, VAHTI 4/2013, Valtionhallinnon tietoturvallisuuden johtoryhmä,
Valtionvarainministeriö 2013

Henkilöstön tietoturvaohjeet, Perusturvaosasto
Isonkyrön kunta 2011

Miten valmistautua EU:n tietosuoja-asetukseen?, Selvityksiä ja ohjeita 4/2017,
Tietosuoja-valtuutetun toimisto, Oikeusministeriö 2017

Tietoturvapolitiikka, malliesimerkki
Sosiaali- ja terveysministeriö 2010

Yleinen tietosuoja-asetus, Yleiskirje 14/2017, Ida Sulin 29.5.2017
Kuntaliitto 2017