

IIN KUNNAN HENKILÖTIETOJEN KÄSITTELYOHJE

Kunnanhallitus 27.6.2022
Voimaan 28.6.2022

Sisällys

1 Johdanto	3
2 Rekisterinpitäjä, rekisteri ja rekisteröity.....	3
3 Henkilötietojen käsittely	4
3.1 Mitä on henkilötieto ja henkilötiedon käsittely?	4
3.2 Pääperiaatteet	5
3.3 Erityiset henkilötietoryhmät	6
3.4 Tietojen julkisuus, salassapito ja vaitiolovelvollisuus	6
3.5 Kuka saa käsitellä tietoja ja milloin?	7
3.6 Tietojen luovuttaminen	8
3.7 Miten käsittelen henkilötietoja oikein?	8
4 Rekisterinpitäjän velvollisuudet.....	9
4.1 Tietosuoja-asetuksen noudattaminen	9
4.2 Osoitusvelvollisuus	10
4.3 Tietosuojaseloste ja seloste käsittelytoimista	10
4.4 Tietosuojaloukkauksesta ilmoittaminen viranomaiselle ja rekisteröidylle	10
5 Rekisteröidyn oikeudet.....	11
5.1 Yleistä.....	11
5.2 Tietojen tarkastusoikeus.....	11
5.3 Oikeus tietojen oikaisemiseen	11
5.4 Oikeus tulla unohdetuksi	12
5.5 Oikeus käsittelyn rajoittamiseen.....	12
5.6 Oikeus siirtää tiedot järjestelmästä toiseen	12
5.7 Vastustamisoikeus	12
5.8 Oikeus tehdä valitus viranomaiselle	12
6 Vastuut.....	13

1 Johdanto

EU:n yleisen tietosuoja-asetuksen (GDPR) tarkoituksena on suojella luonnollisen henkilön oikeuksia ja vapauksia henkilötietojen käsittelyssä. Sitä on sovellettu EU-tasoisesti kaikessa henkilötietojen käsittelyssä 25.5.2018 lähtien. Uutena yleislakina toimii kansallinen tietosuojalaki, jossa osittain määritellään, miten tietosuoja-asetusta sovelletaan Suomessa (ns. kansallinen liikkumavara). Tietosuoja-asetus on suoraan kaikissa EU:n jäsenmaissa sovellettavaa oikeutta, eikä sen määräyksiä voida kansallisilla säädöksillä syrjäyttää. Tietosuoja-asetuksen ja tietosuojalain lisäksi henkilötietojen käsittelyä säännellään Suomessa myös useilla erityislaeilla.

Miten tämä koskee kunnan työntekijöitä? On tärkeää, että lainsäädännön mukaiset velvoitteet huomioidaan kaikessa henkilötietojen käsittelyssä. Tietosuoja-asetus antaa rekisteröidylle uusia ja täsmennettyjä oikeuksia ja toisaalta rekisterinpitäjälle ja henkilötietojen käsittelijälle uusia velvollisuuksia. Yksi tärkeimmistä muutoksista on osoitusvelvollisuus. Rekisterinpitäjän tulee pystyä esimerkiksi erilaisin dokumentein, ohjein, prosessikuvauksin osoittamaan, että se on huomionut lainsäädännön asettamat velvollisuudet toiminnassaan.

Tietosuoja-asetuksen myötä myös valvontaviranomaisen (tietosuojavaalautettu) rooli ja oikeudet korostuvat. Henkilötietojen virheellisestä käsittelystä voidaan antaa huomautus, varoitus tai käsittelykielto ja viime kädessä rekisterinpitäjä tai henkilötietojen käsittelijä voidaan velvoittaa maksamaan vahingonkorvauksia rekisteröidylle, mikäli tämän tietoja on käsitelty turhaan, virheellisesti tai jos tiedot päätyvät asiattomien saataville. Julkishallinnon viranomaisille sakkomaksua ei tosin tietosuojalain 24 §:n mukaan voida määrätä.

Organisaatio vastaa siitä, että sen työntekijöillä on käytössään riittävä tuki ja ohjeistus lainsäädännön huomioimiseksi. Työntekijä puolestaan vastaa omalta osaltaan henkilötietojen asianmukaisesta käsittelystä ja tietoturvan ja tietosuojan huomioimisesta arjen työtehtävissä.

Tämä materiaali on tarkoitettu lin kunnan henkilökunnan ja luottamushenkilöiden käyttöön, avuksi henkilötietojen käsittelyyn ja rekisteröidyn oikeuksien toteuttamiseen.

Työntekijällä tarkoitetaan tässä ohjeessa kaikkia kunnan palveluksessa olevia henkilöitä, riippumatta heidän asemastaan. Jokaisen työntekijän ja luottamushenkilön tulisi tutustua tähän ohjeeseen vähintään niiltä osin, kuin ohje koskee heidän toimenkuvaansa. Lisätietoja tietosuoja-asioista saa kunnan tietosuojavaalautavalta.

Tämä ohje perustuu Valtiovarainministeriön Julkisen hallinnon digitaalisen turvallisuuden kehittämisohjelman laatimaan Henkilötietojen käsittelyn yleisohjeeseen.

2 Rekisterinpitäjä, rekisteri ja rekisteröity

Rekisterinpitäjällä tarkoitetaan sitä tahoa, jonka käyttötarkoituksia varten tietoja kerätään. Rekisterinpitäjänä voi toimia luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin. Rekisterinpitäjiä ovat siis niin yksityiset yritykset kuin julkishallinnon toimijatkin.

Rekisteri tarkoittaa rekisteröityjen henkilötiedoista koostuvaa tietojoukkoa, josta tiedot ovat saatavilla tietyin perustein, oli tietojoukko sitten keskitetty, hajautettu tai toiminnallisesti tai maantieteellisesti perustein jaettu. Käytännössä rekisteri voi siis koostua yhdestä tai useammasta, eri paikoissa sijaitsevasta tietolähteestä.

Rekisteröidyllä tarkoitetaan sitä luonnollista henkilöä, jonka tietoja rekisterissä käsitellään. Se on rekisteristä riippuen esimerkiksi asiakas, kansalainen, kuntalainen tai esim. kunnan työntekijä.

3 Henkilötietojen käsittely

3.1 Mitä on henkilötieto ja henkilötiedon käsittely?

Tietosuoja-asetuksen mukaan *henkilötietoa* on kaikki sellainen tieto, josta luonnollinen henkilö eli rekisteröity voidaan suoraan tai epäsuorasti tunnistaa. Tällaisia tunnistetietoja ovat esimerkiksi nimi, henkilötunnus, sijaintitieto, verkkotunnistetieto tai jokin fyysinen, fysiologinen, geneettinen, psyykinen, taloudellinen kulttuurillinen tai sosiaalinen tekijä tai näiden tietojen yhdistelmä. Epäsuora tunnistaminen tarkoittaa sitä, että henkilö voidaan tunnistaa yhdistämällä tietoja useammasta lähteestä, esimerkiksi useammasta tietojärjestelmästä.

Henkilötiedon käsittelyllä puolestaan tarkoitetaan henkilötietoihin tai tietojoukkoihin liittyvää toimintaa, on se sitten automaattista, tietojärjestelmällä sähköisesti tapahtuvaa tai manuaalista käsittelyä, esimerkiksi tulostettujen asiakirjojen mapittamista. Tiedon käsittelyä on tietojen kerääminen, tallentaminen, järjestäminen, jäsentäminen, säilyttäminen, muokkaaminen tai muuttaminen, haku, kysely, käyttö, tietojen luovuttaminen tai asettaminen saataville, tietojen yhteensovittaminen tai yhdistäminen, rajoittaminen, poisto tai tuhoaminen. Tulee huomioida, että myös tiedon katseleminen tai haku sähköisestä järjestelmästä on henkilötietojen käsittelyä.

Henkilötiedon käsittelyä on myös pääsyn mahdollistaminen henkilötietoon esimerkiksi silloin kun henkilötiedon käsittely - palkanlaskenta, tukipalvelut tms. - ulkoistetaan rekisterinpitäjän ulkopuolelle. Käsittelyä on myös pelkästään tietojärjestelmässä tapahtuva, automatisoitu tiedon käsittely, jossa esimerkiksi arvioidaan henkilön piirteitä tai ominaisuuksia.

Henkilötietojen käsittelysäännöt koskevat kaikenlaista henkilötietojen käsittelyä, olivatpa tiedot asiakkaiden, sopimuskumppaneiden tai oman henkilökunnan tietoja.

Henkilötietojen käsittelyn yhteydessä puhutaan usein *pseudonymisoinnin* ja *anonymisoinnin* käsitteistä. Tietoja, joista henkilö on tunnistettavissa vain epäsuorasti, kutsutaan pseudonymisoiduiksi tiedoiksi. On tärkeää huomioida, että pseudonymisoitu tieto on edelleen henkilötieto ja siihen sovelletaan tietosuoja-asetusta. Pseudonymisointi on siis ennen kaikkea tiedon suojaamistoimenpide, jota käytetään esim. tilanteissa, joissa yksilön tiedot korvataan jollain tunnisteella, mutta tunnisteiden avulla tiedot voidaan myöhemmin vielä palauttaa ja yhdistää luonnolliseen henkilöön.

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

Sekä tietojen pseudonymisoinnissa ja anonymisoinnissa tulee huolehtia siitä, että se tehdään sellaisella mallilla ja algoritmilla, johon ei liity haavoittuvuutta tai muuta mahdollisuutta palauttaa alkuperäiset tiedot.

3.2 Pääperiaatteet

Tietosuoja-asetusta sovelletaan lähtökohtaisesti kaikkeen henkilötietojen käsittelyyn. Henkilötietojen käsittelyyn liittyvää lainsäädäntöä on laajasti myös erityislainsäädännössä, joka luonnollisesti täytyy huomioida varsinaisen tietosuojalainsäädännön - tietosuoja-asetuksen ja tietosuojalain - lisäksi.

Kunnan työntekijöistä ja luottamushenkilöistä sekä yhteistyökumppaneista ja asiakkaista kertyy tietoja rekistereihin niin kunnan lakisääteisten tehtävien hoitamisen kuin sopimusten ja asiakkuussuhteiden tai toimeksiantojen perusteella. Henkilötietoja sisältäviä rekistereitä muodostuu esimerkiksi kunnan varhaiskasvatuksen ja perusopetuksen, työllisyyspalveluiden tai henkilöstön työsuhteiden ja palkanmaksun osalta. Käytännössä henkilötietoja muodostuu lähes kaikilla kunnan toimialoilla.

Rekistereihin saa kerätä tietoa vain tiettyä, nimenomaista ja laillista tarkoitusta varten eli kun tietoa tarvitaan esimerkiksi palvelun toteuttamiseksi ja siihen on olemassa lainmukainen peruste. Käyttötarkoituksen kannalta ylimääräisiä tietoja ei saa kerätä, eikä tietoja saa myöhemminkään käyttää muuhun kuin sitä tarkoitusta varten, johon ne on kerätty. Tietoja tulee käsitellä ja säilyttää asianmukaisesti, rekisteröidyn yksityisyyden suoja ja tietoturva ja -suoja huomioiden. Virheelliset tiedot tulee viipymättä oikaista tai tarvittaessa poistaa kokonaan.

On tärkeää huolehtia siitä, että tietoja säilytetään vain tarpeellisen ajan, käsittelyn tarkoitukset ja lakisääteiset säilytysajat huomioiden. Tiedot tulee arkistoida asianmukaisesti lin kunnan tiedonohjaussuunnitelman mukaisesti. Neuvoja arkistointiin voi kysyä tietopalveluasiantuntijalta.

Tietosuoja-asetus korostaa tietojen avoimuutta ja läpinäkyvyyttä. Rekisteröityä tulee informoida siitä, miten, mitä tarkoituksia varten ja missä määrin häntä koskevia henkilötietoja käsitellään. Lisäksi rekisteröityä tulee tiedottaa henkilötietojen käsittelyyn liittyvistä riskeistä, säännöistä, suojatoimista ja oikeuksista. Tietojen ja viestinnän tulee olla helposti saatavilla ja ymmärrettävissä ja niissä on käytettävä selkeää ja yksinkertaista kieltä.

Henkilötietojen käsittelyn pääperiaatteet:

- henkilötietoja on käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi (lainmukaisuus, kohtuullisuus ja läpinäkyvyys)
- henkilötietoja voi kerätä vain tiettyä, nimenomaista ja laillista tarkoitusta varten, eikä niitä saa käsitellä myöhemmin näiden tarkoitusten kanssa yhteensopimattomalla tavalla (käyttötarkoituSSIDonnaisuus)
- henkilötietojen on oltava asianmukaisia ja olennaisia ja rajoitettuja siihen, mikä on tarpeellista suhteessa niiden käsittelytarkoituksiin (tietojen minimointi)
- henkilötietojen on oltava täsmällisiä ja tarvittaessa päivitettyjä; epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä (täsmällisyysvaatimus)
- henkilötiedot säilytetään muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten (säilytyksen rajoittaminen)
- käsittelyssä huomioidaan henkilötietojen asianmukainen turvallisuus, mukaan lukien suojaaminen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta

häviämiseltä, tuhoutumiselta tai vahingoittumiselta käyttäen asianmukaisia teknisiä tai organisatorisia toimia (tietoturva: eheys ja luottamuksellisuus).

3.3 Erityiset henkilötietoryhmät

Henkilötietoja on erilaisia ja osaa tiedoista tulee käsitellä erityisen huolellisesti. Tietosuoja-asetuksessa on määritelty *erityiset henkilötietoryhmät*, jotka vastaavat pääsääntöisesti aiempia henkilötietolaissa määriteltyjä arkaluonteisia tietoja. Tällaisia tietoja ovat rotu, etninen alkuperä, poliittinen mielipide, uskonnollinen tai filosofinen vakaumus, ammattiliiton jäsenyys, terveyttä koskevat tiedot sekä luonnollisen henkilön seksuaalista käyttäytymistä ja suuntautumista koskevat tiedot. Uusina tietoryhminä ovat geneettiset ja biometriset tiedot.

Erityisiin henkilötietoryhmiin liittyviä tietoja saa käsitellä vain tietosuoja-asetuksen määrittelemissä tilanteissa. Tällaisia tilanteita ovat esimerkiksi

- rekisteröidyn antama nimenomainen suostumus
- rekisterinpitäjän tai rekisteröidyn velvoitteiden ja erityisten oikeuksien noudattaminen
- rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaaminen
- käsittely on tarpeen tärkeää yleistä etua koskevasta syystä
- 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
- käsittely on tarpeen yleisen edun mukaisia arkistointitarkoituksia taikka tieteellisiä ja historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten.

Käytännössä kunnat joutuvat aina käsittelemään myös erityisiä henkilötietoja pystyäkseen hoitamaan lakisääteiset tehtävänsä.

3.4 Tietojen julkisuus, salassapito ja vaitiolovelvollisuus

Tärkeimmät organisaation toimintaa koskevat lait ovat

- julkisuuslaki eli laki viranomaisen toiminnan julkisuudesta (621/1999), joka määrittelee, mitkä viranomaisen asiakirjat ovat julkisia ja mitkä asiakirjat ja tiedot salassa pidettäviä
- hallintolaki (434/2003), jossa määritellään hyvän hallinnon perusteet sekä asian käsittelystä ja oikaisuvaatimusmenettelystä.
- kuntalaki (410/2015), jossa säännellään kunnan hallinnon toiminnasta ja talouden järjestämisestä

Pääsääntöisesti kaikki viranomaiselle toimitetut asiakirjat ja tehdyt päätökset ovat julkisia. Valmisteluasiakirjojen osalta organisaatio voi käyttää harkintavaltaa tiedottamisen tai tietojen luovuttamisen osalta. Sisäiset muistiot tai esimerkiksi omat muistiinpanot eivät ole julkisia, eivätkä siten kuulu lainkaan julkisuuslain piiriin.

Salassa pidettäviä asiakirjoja (julkisuuslain 24 §) ei saa näyttää tai luovuttaa eikä niiden sisällöstä saa keskustella ulkopuolisten kanssa. Yleisimmät salassa pidettävät asiat koskevat erityisiä henkilötietoryhmiä, kuten sosiaali- ja terveystietoja ja näihin liittyvää asiakkuutta, oppilashuoltoa tai kunnan liike- ja ammattisalaisuuksia.

Vaitiolovelvollisuus koskee paitsi salassa pidettävää asiakirjaa, myös muuta tietoa, jonka henkilö - virkamies, työntekijä, harjoittelija, luottamushenkilö jne. - saa tietoonsa työtehtäviä hoitaessaan. Jokainen lin kunnan työntekijä ja luottamushenkilö on velvollinen noudattamaan lakia ja olemaan paljastamatta salassa pidettävää tietoa palveluksessa oloaikanaan tai sen jälkeen. Vaitiolovelvollisuudesta säädetään mm. julkisuuslaissa ja sen rikkomisesta on määritelty rangaistus rikoslaissa.

Aina, kun käsittelet luottamuksellisia tietoja, huomioi

- ettei tällaisia tietoja sisältäviä tulosteita jää muiden näkyviin
- tiedon tallennuspaikka, ettet erehdyksessä tallenna tietoa väärään paikkaan
- sähköpostiosoitteen tarkistus, ettei tieto joudu väärälle henkilölle
- ettet keskustele asiasta niin, että tietoa paljastuu ulkopuolisille

3.5 Kuka saa käsitellä tietoja ja milloin?

Henkilötietojen käsittelylle täytyy lähtökohtaisesti olla aina jokin peruste. Julkisella sektorilla se on yleensä lakisääteinen oikeus tai velvollisuus käsitellä tietoja. Henkilötietoja ei saa kerätä ilman syytä, vaikka tiedot olisivat vapaasti saatavilla esimerkiksi internetistä. Tietoja ei myöskään saa katsella esimerkiksi tietojärjestelmistä tai tulosteilta muuten vain, ilman asiallista syytä. Salassa pidettäviä tietoja ei lähtökohtaisesti saa käsitellä lainkaan, elleivät työtehtävät sitä edellytä. Niistä ei myöskään tule keskustella ulkopuolisten kanssa.

Ellei tietojen käsittely perustu lainmukaiseen oikeuteen tai velvollisuuteen tai esimerkiksi rekisteröidyn kanssa tehtävään sopimukseen, tulee henkilötietojen käsittelyyn pyytää suostumus. Rekisteröity saa koska tahansa peruuttaa suostumuksensa, ja peruuttamisen tulee olla yhtä helppoa kuin suostumuksen antamisenkin.

Henkilötietoja saa käsitellä esimerkiksi seuraavissa tilanteissa

- siihen on olemassa rekisteröidyn suostumus
- käsittely on tarpeen organisaation lakisääteisten velvoitteiden noudattamiseksi
- käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi (esimerkiksi tutkimuskäyttö tai organisaation ei-lakisääteinen tehtävä).
- rekisteröity on tehnyt sopimuksen, johon käsittely perustuu; käsittely voi olla tarpeen esimerkiksi sopimuksen täytäntöön panemiseksi tai sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi tai
- käsittely on tarpeen rekisterinpitäjän oikeutettujen etujen toteuttamiseksi.

Huomaa, ettet voi vapaasti keskustella rekisteröityjen – olivatpa he kansalaisia, kuntalaisia, asiakkaita tai henkilöstöön kuuluvia – henkilötiedoista kollegoidenkaan kanssa tai näyttää heihin liittyviä tai muuten salassa pidettäviä tietoja tietojärjestelmästä sillä perusteella, että molempia osapuolia koskevat salassapitosäännöt, mukaan lukien vaitiolovelvollisuus.

Henkilötietojen käsittelylle, esimerkiksi tietojen katselulle, tulee aina löytyä myös henkilötietoja käsittelevän työntekijän työrooliin perustuva oikeus.

3.6 Tietojen luovuttaminen

Tietosuoja-asetus sääntelee tietojen luovuttamisesta tai siirtoa rekisterinpitäjältä toiselle tai rekisterinpitäjältä henkilötietojen käsitteijätaholle eli esimerkiksi ulkoistustilanteissa sille yritykselle, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Virallisten asiakirjojen julkisuudesta ja tietojen luovuttamisesta esimerkiksi viranomaistaholta toiselle säännellään edelleen kansallisessa lainsäädännössä – eli julkisuuslaissa ja eri alojen erityislaeissa.

Tietojen luovutuksessa on huomioitava, että luovuttaja vastaa aina luovutusten laillisuudesta. On siis syytä pohtia, missä tilanteissa ja mihin tarkoituksiin tietoja luovutetaan. Tiedon luovutukset tulee aina dokumentoida, eikä ilman kirjallista pyyntöä tietoja ole syytä luovuttaa, ellei kyseisestä tarkoituksesta ja luovutuksensaajasta voida olla täysin varmoja.

Tietojen luovuttaja vastaa siitä, että:

- tiedon pyytäjällä on oikeus saada tiedot
- tietojen luovutukset tehdään tarvittaessa suojatusti turvasähköpostilla, kirjepostilla tai paikan päällä organisaatiossa siten, että pyytäjän henkilöllisyys varmistetaan

Mikäli et ole täysin varma siitä, voiko tietoa luovuttaa, on syytä kääntyä esimiehen tai tietosuojavastaavan puoleen.

3.7 Miten käsittelen henkilötietoja oikein?

Henkilötietojen käsittelyssä pienilläkin asioilla on suuri merkitys. Tärkeintä on huomioida arjen työtehtävissä toimenpiteet, joilla tietoa pyritään suojaamaan sivullisilta, käsiteltiinpä henkilötietoja sitten sähköisesti tietojärjestelmissä, paperilla, kuvina tai keskusteluissa. Huomioi aina, etteivät ulkopuoliset pääse kuulemaan tai näkemään käsittelemiäsi tietoja.

Oikeudet verkkolevyille tai erilaisiin tietojärjestelmiin myönnetään henkilökohtaisesti ja työtehtäväperusteisesti. Tietojärjestelmissä toimitaan aina henkilökohtaisilla tunnuksilla ja omaan työrooliin kuuluvilla oikeustasoilla. Toisten henkilöiden tunnuksia ei saa käyttää, eikä omia tunnuksia saa lainata tai luovuttaa toiselle. Tämä on myös oikeusturvakysymys;

useimpien tietojärjestelmien käyttöä valvotaan yhä laajemmin, jotta voidaan tarvittaessa jälkikäteen todentaa, kuka henkilötietoja on katsonut tai muuten käsitellyt.

Ole erityisen huolellinen lähettäessäsi sähköpostia myös organisaation sisällä - varsinkin jos sähköposti sisältää henkilötietoa tai erityisiin henkilötietoryhmiin kuuluvaa tietoa. Tarkista aina, että vastaanottaja on varmasti oikea eikä nimikaima organisaation sisältä tai ulkopuolelta. Erityisiin henkilötietoryhmiin kuuluvaa tietoa ei saa lähettää organisaation ulkopuolelle salaamattomana, vaan on käytettävä turvasähköpostia. Esimiesten tulee pyytää alaisilleen turvasähköpostin käyttöoikeuksia matalalla kynnyksellä, koska hyvin monissa tehtävissä joutuu nykyään käsittelemään salasta vaativia henkilötietoja.

Suojattavaa tietoa ovat esimerkiksi paperitulosteet, usb-tikut, CD- ja DVD-levyt, valokuvat jne. - jotka sisältävät sellaista henkilötietoa, josta henkilö voidaan yksilöidä. Tietosuojattava materiaali tulee käsitellä, kerätä, varastoida ja hävittää niin, ettei tietosuoja vaarannu - älä siis jätä henkilötietoja sisältävää materiaalia pöydille muiden nähtäväksi, älä varastoi sitä esimerkiksi pahvilaatikoihin myöhemmin hävitettäväksi tai heitä tulosteita tavalliseen roska-astiaan tai paperinkeräykseen. Kunnan eri toimipisteissä on käytössä lukollisia tietosuoja-asäiliöitä, joiden avulla asiakirjat hävitetään tietoturvallisesti. Lisätietoa voi kysyä tietopalveluasiantuntijalta.

Esimerkkejä hyvistä toimintatavoista:

- lukitse työasemasi aina kun poistut työpisteeltä hetkeksikin (Windows-näppäin + kirjain L)
- suojaa tarvittaessa näytön tiedot käyttämällä näytönsuojakalvoa
- huomioi tietosuoja myös työmatkoilla ja etätyössä; estä ulkopuolisten pääsy näkemään näytölläsi olevia tietoja; esim. näytönsuojakalvokaan ei auta, jos junassa takanasi istuu utelias ihminen
- pidättäydy keskustelemasta luottamuksellisista tai salassa pidettävistä asioista edes muiden työkavereiden kanssa
- henkilötietoja sisältävät tulosteet kuuluvat tietosuojattavan jätteen astiaan, ei tavalliseen paperinkeräykseen tai roska-astiaan eikä niitä saa varastoida myöhemmin hävitettäväksi
- älä tallenna henkilötietoja sisältävää materiaalia suojaamattomille tikuille tai muille ulkoisille lisämuisteille. Työaseman omalla verkkolevylläsi tiedot ovat turvassa, vaikka joku varastaisi työaseman.
- huomioi, että työajan ulkopuolellakin sinua koskee vaitiolovelvollisuus - älä puhu työasioista ulkopuolisten kuullen.

4 Rekisterinpitäjän velvollisuudet

4.1 Tietosuoja-asetuksen noudattaminen

Rekisterinpitäjän tulee toteuttaa asianmukaiset tekniset ja organisatoriset toimenpiteet, joilla varmistetaan, että asetuksessa säädetyt vaatimukset täyttyvät. Velvoite on laaja: rekisterinpitäjän tulee mm. huolehtia siitä, että

- käsittelyssä huomioidaan sertifiointit, salaukset ja esimerkiksi tietojärjestelmien auditoinnit tai lokitietojen kerääminen tarvittaessa sekä huolehtia tarvittaessa tietojen pseudonymisoinnista ja anonymisoinnista
- edellä mainittuja käsittelyperiaatteita noudatetaan toiminnassa
- tietosuoja huomioidaan jo kehitettäessä ja otettaessa käyttöön uusia tuotteita, palveluja ja sovelluksia
- tarvittavat ohjeet, prosessit, koulutukset on dokumentoitu riittävän tarkalla tasolla, jotta henkilökunnan on mahdollista huomioida tietosuoja työtehtävissään.

4.2 Osoitusvelvollisuus

Erittäin tärkeä uusi velvollisuus on osoitusvelvollisuus. Organisaation tulee pystyä pyydettäessä osoittamaan, että henkilötietojen käsittelyä koskevia periaatteita on noudatettu. Tämä edellyttää henkilötietojen käsittelytoimien, ohjeiden, koulutusten ja prosessien dokumentointia riittävän tarkalla tasolla, jotta tietosuojaviranomaiset pystyvät todentamaan tarvittaessa henkilötietojen käsittelyn lainmukaisuuden kunnan eri toiminnoissa.

4.3 Tietosuojaseloste ja seloste käsittelytoimista

Tietosuojaselosteiden laatiminen kaikista organisaation rekisteristä on yksi osoitusvelvollisuutta toteuttava dokumentti. Mitä keskeisempi rekisteri on kyseessä ja mitä arkaluonteisempaa tietoa (erityisiä henkilötietoryhmiä) rekisterissä käsitellään, sitä huolellisemmin tietosuojaseloste on täytettävä. Tietosuojaseloste tulee pitää julkisesti saatavilla. Iin kunnan tietosuojaselosteet löytyvät kunnan nettisivuilta. Lisäksi organisaatio ylläpitää selostetta organisaation vastuulla olevista käsittelytoimista. Seloste käsittelytoimista dokumentti on tarkoitettu vain sisäiseen ja tietosuojaviranomaisten käyttöön.

4.4 Tietosuojaloukkauksesta ilmoittaminen viranomaiselle ja rekisteröidylle

Henkilötietojen tietoturvaloukkauksella tarkoitetaan tilannetta, jonka seurauksena on siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen tai pääsy tietoihin. Tietomurtojen lisäksi tämä tarkoittaa siis myös esimerkiksi tilanteita, joissa henkilötietoa päätyy vahingossa ulkopuolisten saataville, esimerkiksi

- henkilötietoja sisältävää materiaalia katoaa tai joutuu hukkaan
- henkilötietoja sisältävä muistitikku tai muu tallennusväline katoaa tai joutuu hukkaan
- työasema varastetaan
- henkilötietoja sisältäviä asiakirjoja löytyy varastoituna julkisista valvomattomista tiloista
- henkilötietoja sisältäviä aineistoja päätyy erehdyksessä julkisille verkkosivuille
- henkilötietoja sisältäviä dokumentteja tulostetaan erehdyksessä väärälle tulostimelle
- henkilötietoja sisältäviä asiakirjoja lähetetään väärälle ihmiselle.

Henkilötietojen tietoturvaloukkauksesta tulee pääsääntöisesti aina ilmoittaa tietosuojaviranomaisille ja tietyin edellytyksin myös rekisteröidylle itselleen. Kaikista ilmoittamisista päättää organisaation tietosuojavastaava yhdessä tietohallinnon tietoturvasiantuntijoiden ja kyseisen rekisterin omistajan kanssa. Henkilötietojen tietoturvaloukkauksista on lin kunnassa laadittu tarkempi ohje, joka ohjeistaa toimintatavan tietoturvaloukkaustilanteessa. Ohje löytyy intrasta ja Dynastysta.

Jotta voimme toteuttaa ilmoitusvelvollisuutemme, on erittäin tärkeää, että jokainen kunnan työntekijä ilmoittaa välittömästi tietoonsa tulleista henkilötietojen tietoturvaloukkauksista esimiehelleen sekä tietosuojavastaavalle.

5 Rekisteröidyn oikeudet

5.1 Yleistä

Tietosuoja-asetus takaa rekisteröidylle, eli henkilölle, jonka tietoja käsitellään, erilaisia oikeuksia. Oikeuksia sovelletaan eri tavalla riippuen henkilötietojen käsittelyperusteesta. Henkilöllä on mm. oikeus tietää, käsitelläänkö hänen henkilötietojaan ja mitä henkilötietoja käsitellään sekä pyytää itseään koskevat tiedot. Henkilöllä on myös oikeus vaatia virheelliset henkilötiedot oikaistavaksi. Rekisteröidyn oikeuksista ohjeistetaan tarkemmin lin kunnan tietosuoja- ja tietoturvapoliittikkaa ohjaavassa asiakirjassa.

5.2 Tietojen tarkastusoikeus

Henkilöllä on oikeus tietää, käsitelläänkö hänen henkilötietojaan vai ei, ja mitä henkilötietoja hänestä on tallennettu. Organisaatio toimittaa rekisteröidyn pyynnöstä tiedot mahdollisimman pian ilman aiheetonta viivytystä. Määräaika tietojen toimittamiseksi tai tietopyyntöön liittyvien lisätietojen antamiseksi on kuukausi pyynnön vastaanottamisesta. Mikäli tietopyyntö on poikkeuksellisen monimutkainen ja laaja, määräaika voidaan jatkaa kahdella kuukaudella.

Rekisteröidyn tiedot toimitetaan lähtökohtaisesti maksutta. Jos jäljennöksiä pyydetään useampia, organisaatio voi kuitenkin periä niistä hallinnollisiin kustannuksiin perustuvan kohtuullisen maksun. Mikäli tietopyyntö on ilmeisen perusteeton ja kohtuuton, erityisesti jos tietopyyntöjä esitetään toistuvasti, organisaatio voi periä tietojen toimittamisesta aiheutuneet hallinnolliset kustannukset tai kieltäytyä kokonaan toimittamasta tietoja. Tällaisessa tapauksessa organisaatio osoittaa pyynnön ilmeisen perusteettomuuden tai kohtuuttomuuden.

Mikäli organisaatio ei toimita tietoja, annetaan asiasta kirjallinen todistus. Samassa yhteydessä kerrotaan oikeudesta oikeussuojakeinoihin, esimerkiksi mahdollisuudesta tehdä valitus valvontaviranomaiselle.

5.3 Oikeus tietojen oikaisemiseen

Henkilöllä on oikeus vaatia, että häntä koskevat virheelliset, epätarkat tai puutteelliset henkilötiedot oikaistaan tai täydennetään ilman aiheetonta viivytystä. Lisäksi henkilöllä on oikeus vaatia, että tarpeettomat henkilötiedot poistetaan. Tarpeettomuutta ja virheellisyyttä arvioidaan tietojen tallennushetken mukaan.

Ellei organisaatio hyväksy oikaisupyyntöä, annetaan asiasta kirjallinen todistus, jossa mainitaan ne syyt, joihin perustuen vaatimusta ei ole hyväksytty. Samoin tiedotetaan oikeudesta oikeussuojakeinoihin, esimerkiksi mahdollisuudesta tehdä valitus valvontaviranomaiselle.

5.4 Oikeus tulla unohdetuksi

Henkilöllä on vain tietyissä poikkeustapauksissa oikeus saada henkilötietonsa kokonaan poistettua organisaation rekistereistä (oikeus tulla unohdetuksi). Tällaista oikeutta ei kuitenkaan ole niissä tapauksissa, kun henkilötietojen käsittely on tarpeellista lakisääteisen velvoitteen noudattamiseksi tai organisaatiolle kuuluvan julkisen vallan käyttämistä varten. Tietojen säilyttämisessä ja poistamisessa noudatetaan organisaation tiedonohjaus- ja arkistonmuodostussuunnitelmia sekä lainsäädännön velvoittamia tietojen säilytysaikoja.

5.5 Oikeus käsittelyn rajoittamiseen

Henkilöllä voi tietyissä tilanteissa olla oikeus pyytää henkilötietojensa käsittelyn rajoittamista siksi aikaa, kunnes hänen tietonsa on asianmukaisesti tarkistettu ja korjattu tai täydennetty. Rekisteröidyllä on oikeus pyytää henkilötietojensa rajoittamista muun muassa, kun henkilötiedot eivät pidä enää paikkaansa tai henkilötietojen käsittely rikkoo lainsäädäntöä.

5.6 Oikeus siirtää tiedot järjestelmästä toiseen

Oikeus ei koske sellaista henkilötiedon käsittelyä, joka on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi. Näin ollen pääsääntöisesti oikeutta ei sovelleta kunnan henkilörekistereihin liittyen.

5.7 Vastustamisoikeus

Henkilöllä on oikeus henkilökohtaiseen, erityiseen tilanteeseensa perustuen milloin tahansa vastustaa henkilötietojensa käsittelyä silloinkin, kun käsittely perustuu yleistä etua koskevan tehtävän suorittamiseksi tai organisaatiolle kuuluvan julkisen vallan käyttämistä. Tässä tapauksessa tietoja voidaan käsitellä edelleen vain, jos käsittelyyn on olemassa huomattavan tärkeä ja perusteltu syy, joka voidaan osoittaa. Vastustusoikeus ei koske lakisääteisiä rekistereitä.

5.8 Oikeus tehdä valitus viranomaiselle

Henkilöllä on oikeus tehdä valitus erityisesti vakinaisen asuin- tai työpaikkansa sijainnin mukaiselle valvontaviranomaiselle, jos hän katsoo, että henkilötietojen käsittelyssä rikotaan EU:n yleistä tietosuojasetusta (EU) 2016/679. Tämän lisäksi henkilöllä on oikeus käyttää muita hallinnollisia muutoksenhakekeinoja sekä oikeussuojakeinoja.

Henkilöllä on oikeus myös nostaa kanne rekisterinpitäjää tai henkilötietojen käsittelijä-organisaatiota vastaan, jos hän katsoo oikeuksiaan loukatun sen takia, ettei hänen henkilötietojensa käsittelyssä ole noudatettu tietosuojasetusta.

- Oikeus saada tietoa henkilötietojen käsittelystä
- Oikeus tietojen oikaisuun
- Oikeus vastustaa automaattista päätöksentekoa
- Oikeus saada kopio käsiteltävistä henkilötiedoista
- Oikeus saada tieto henkilötietojen tietoturvaloukkauksesta
- Oikeus tietojen poistoon, ellei poistolle ole lakisääteistä estettä

6 Vastuut

Iin kunta vastaa rekisterinpitäjänä siitä, että sen toiminnassa noudatetaan tietosuoja-asetusta, tietosuojalakia sekä muuta henkilötietojen käsittelyyn liittyvää erityislainsäädäntöä. Toimialat huolehtivat oman toimialansa asia- ja lainsäädäntöosaamisesta ja kouluttavat ja ohjeistavat henkilöstön paitsi organisaation yhteisiin, myös toimialaansa koskeviin tarkempiin henkilötietojen käsittelyohjeisiin.

Jokaisen kunnan työntekijän tulee osallistua työssään tarvitsemiinsa koulutuksiin, perehtyä ohjeisiin ja noudattaa niitä sekä huomioida tietoturva ja tietosuoja työtehtävissään. Myös luottamushenkilöiden on noudatettava samoja henkilötietojen käsittelyperiaatteita aina kun he joutuvat luottamustointaan hoitaessaan tekemisiin henkilötietojen kanssa.