



Nurmijärven kunnan tietosuojapolitiikka

11.6.2018

Tietosuoja on henkilötietojen suoja

Tietosuoja tarkoittaa henkilötietojen suojaamista ja niiden asiallista käsittelyä. Henkilötiedolla tarkoitetaan kaikenlaisia luonnollista henkilöä takka hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi. EU:n tietosuoja-asetus, jota sovelletaan kansallisesti 25.5.2018 alkaen, asettaa entistä tiukemmat vaatimukset henkilötietojen käsittelylle, ja niihin kuuluu osoitusvelvollisuus. Rekisterinpitäjällä on velvollisuus osoittaa, miten se käsittelee henkilötietoja ja miten yksityisyyden suoja turvataan.

Tietosuojapolitiikassa määritellään henkilötietojen käsittelyn ja suojaamisen yleiset periaatteet kunnassa, ja ne muodostavat samalla perusteet osoittamisvelvollisuudelle. Periaatteita noudattamalla tavoitellaan luottamusta: Nurmijärven kunnassa henkilötietoja käsitellään tavalla, johon kuntalaiset ja muut rekisteröidyt sekä yhteistyökumppanit voivat luottaa. Tämä vaatii sitä, että periaatteet ovat riittävän selkeät ja konkreettiset, ja että rekisteröidyillä on saatavilla riittävästi informaatiota tietosuojan toteutumisesta Nurmijärven kunnassa. Tietosuojapolitiikkaa täydentävät henkilötietojen käsittelyä koskevat käytännön ohjeet, jotka julkaistaan kunnan intranetissä.

Tietosuoja liittyy läheisesti tietoturvaan, eli tietojen saatavuuden, eheyden ja luottamuksellisuuden varmistamiseen. Tietoturvaan kuuluu muun muassa tietoaineistojen, laitteistojen, ohjelmistojen, tietoliikenteen ja toiminnan turvaaminen. Siihen liittyvät periaatteet on kuvattu kunnan tietoturvapoliitikassa ja tietoturvaohjeissa. Tietosuojapolitiikka täydentää niitä henkilötietojen turvallisen käsittelyn osalta.

Tietosuojaperiaatteet ja rekisteröidyn oikeudet

Tietojen käsittelylle kunnassa tulee aina olla selkeä **peruste** (laki, suostumus, sopimus tai yleinen/oikeutettu etu). Suurin osa kunnan tehtävistä on lakisääteisiä. Mikäli tietojen käsittely perustuu muuhun kuin lakiin, tulee peruste selvittää huolellisesti ja tarvittaessa pyytää käsittelyyn rekisteröidyn suostumus. Tietoja käytetään vain niille alun perin määriteltyyn käyttötarkoitukseen.

Aina henkilötietoja käsiteltäessä noudatetaan **tietojen minimointia**. Se tarkoittaa, että henkilötietoja ei lähtökohtaisesti koskaan kerätä enempää kuin kyseisen tehtävän hoitamiseksi on perusteltua. Tietoja ei myöskään säilytetä kauemmin kuin kyseisen tehtävän hoitaminen edellyttää.

Sisäänrakennettu ja oletusarvoinen tietosuoja tarkoittaa sitä, että henkilötietojen suoja otetaan huomioon jo toimintaa suunniteltaessa. Aina kun suunnitellaan uutta toimintaa, hankintaa tai toimintatavan muutosta, johon sisältyy henkilötietojen käsittelyä, on arvioitava toiminnan vaikutuksia tietosuojan näkökulmasta, ja siitä on informoitava tietosuojavastaavaa.



Tietosuojan toteutumista tarkastellaan **riskilähtöisesti**. Huomio kiinnitetään ensisijaisesti sellaisiin rekistereihin ja järjestelmiin, joissa havaitaan korkea riskitaso. Tällaisia ovat etenkin järjestelmät, joissa käsitellään erityisiä tietoja (esim. arkaluontoisia henkilötietoja tai alaikäisten tietoja) ja suuria tietomassoja, ja järjestelmät, joiden tietosuojassa mahdollisesti havaitaan puutteita.

Tietosuojan lähtökohtana on **rekisteröidyn oikeuksien** toteutuminen. Henkilötietojen käsittelyn tulee perustua avoimuuteen, mitä toteutetaan mm. kertomalla tietosuojasta ja henkilötietojen käsittelystä kunnan www-sivuilla riittävän informatiivisesti (mm. tietosuojaselosteet). Jos tietojen kerääminen perustuu suostumukseen, se pyydetään aina erikseen. Rekisteröidyllä on oikeus omien tietojensa tarkastamiseen ja mahdollisten virheellisten tietojen oikaisemiseen, ja tietojen tarkastuspyynnön tekemiseen on saatavilla lomake kunnan www-sivuilla.

Tietosuojaperiaatteet koskevat kaikkia henkilötietoja riippumatta niiden tallennusmuodosta. Niitä noudatetaan koko tiedon elinkaaren ajan, tietojen keräämisestä niiden arkistointiin tai hävittämiseen saakka.

Kunta rekisterinpitäjänä

Tietosuojaperiaatteet koskevat kaikkea henkilötietojen käsittelyä. Erityisesti huomiota kiinnitetään henkilörekistereihin. Henkilörekisteri on jäseneltyä henkilötietoa sisältävä tietojoukko, josta tiedot ovat saatavilla tietyin perustein. Kunnan henkilörekistereistä pidetään yllä luetteloa. Kunnan www-sivuilla tulee olla saatavilla tietosuojaselosteet, joista käy ilmi kunkin rekisterin tietosisältö, tietojen käsittelyn periaatteet, tietojen mahdolliset luovutukset, yhteyshenkilö ja muut tarvittavat tiedot.

Ylätasolla kunta on rekisterinpitäjä, eli kunta viranomaisena määrittelee henkilötietojen käsittelyn tarkoituksen ja keinot. Hallintosäännön mukaan kunnanhallitus nimeää kunnan rekisterinpitäjät. Niitä ovat tehtäviensä mukaisesti eri lautakunnat. Esimerkiksi hallintoa ja henkilöstöä koskevissa rekistereissä rekisterinpitäjä on pääsääntöisesti Nurmijärven kunnan kunnanhallitus. Toimielimiä informoidaan niiden vastuualueeseen kuuluvista henkilörekistereistä antamalla niille tiedoksi tietosuojaselosteet. Rekistereille määritellään myös vastuu- ja yhteyshenkilöt, jotka ovat kunnan työntekijöitä.

Kunnan ollessa rekisterinpitäjä vastuu tietosuojan toteutumisesta on viime kädessä kunnalla, vaikka joku muu käsittelee henkilötietoja kunnan lukuun. Ulkoisia henkilötietojen käsittelijöitä ovat esimerkiksi tietojärjestelmätoimittajat, kun tietoja käsitellään heidän ylläpitämässään käyttöympäristössä, ja eräät muut ostopalveluiden tuottajat. Hankinta- ja ulkoistussopimuksia tekevät vastaavat siitä, että tietoturvan ja tietosuojan taso vastaa myös ostopalveluissa ohjeita ja voimassa olevia säädöksiä. Sopimuksia tehdessä varmistetaan, että sopimusehdoissa on riittävästi määritelty tietosuojan toteuttaminen ja osapuolten vastuut.

Tietosuojan organisointi ja vastuut

Tietosuojan toteutumisesta kunnassa on viime kädessä vastuussa kunnanhallitus, joka myös hyväksyy tietosuojapolitiikan. Tietosuojan toteutumisesta käytännössä on vastuussa jokainen kunnan työntekijä osaltaan. Esimiesten tehtävä on informoida alaisiaan, ja tietojärjestelmien



omistajien ja pääkäyttäjien on kiinnitettävä jatkuvaa huomiota tietosuojan toteutumiseen omissa järjestelmissään.

Tietosuojavastaava on erityisasiantuntija, jonka tehtävä on toimia rekisterinpitäjän tukena ja auttaa rekisterinpitäjää lakisääteisten velvoitteiden toteuttamisessa. Tietosuojavastaavan tehtäviin kuuluu myös asiantuntija-avun antaminen sekä organisaation henkilöstölle että johdolle tietosuojaan (henkilötietojen käsittelyyn) liittyvissä kysymyksissä. Tietosuojavastaavan tulee myös toimia organisaatiossa henkilötietojen käsittelyä valvovana tahona sekä yhdyssiteenä valvontaviranomaisiin.

Tietosuojatyön eteenpäin viemiseen osallistuu ja sitä valvoo tietosuojatyöryhmä, jonka puheenjohtajana toimii hallintojohtaja ja sihteerinä tietosuojavastaava. Ryhmässä on edustus kaikilta kunnan toimialoilta, ja se toimii projektiluontoisesti vuoden 2018. Sen jälkeen päätetään, sulautuuko se kunnan tietoturvatyöryhmään vai jatkaako se toimintaansa itsenäisenä.

Valtakunnallisella tasolla henkilötietojen käsittelyä ohjaava, neuvova ja valvova viranomainen on tietosuojavaltuutettu. Tietosuojavaltuutettu käyttää päätösvaltaa tarkastusoikeuden toteuttamista ja tiedon korjaamista koskeissa asioissa sekä antaa ratkaisuja rekisterinpidon lainmukaisuudesta ja rekisteröityjen oikeuksien toteutumisesta. Mahdollisista tietoturvapoikkeamista ilmoitetaan säädösten edellyttämällä tavalla tietosuojavaltuutetulle ja rekisteröidyille itselleen.

Tietojärjestelmien turvallinen käyttö ja henkilöstön osaamisen varmistaminen

Kunnan sisäisiä henkilötietojen käsittelijöitä ovat kaikki henkilötietoja työssään käsittelevät henkilöt. Heiltä vaaditaan osaamista ja sitoutumista. Tietojärjestelmien käyttöoikeuksien saamiseksi työntekijältä edellytetään tietoturva- ja tietosuojasitoumuksen allekirjoittamista. Osaamisen varmistamiseksi koko henkilöstöltä edellytetään Navisec-tietoturva- ja tietosuojakoulutuksen suorittamista. Esimiehet ovat vastuussa alaistensa tietosuojaosaamisesta, ja testin suorittaminen tarkistetaan vuosittain kehityskeskustelujen yhteydessä. Lisäksi järjestetään vuosittain tietosuojakoulutusta kohdennetuille henkilöstöryhmille. Toimialat huolehtivat omaan toimintaansa liittyvän lisäohjeistuksen riittävydestä yhteistyössä tietosuojavastaavan kanssa. Tietosuoja-asioista informoidaan myös luottamushenkilöitä.

Kunnassa käytettäviltä tietojärjestelmiltä, joissa käsitellään henkilötietoja, edellytetään käyttäjäkohtaista tunnistautumista ja tehtävien mukaan määriteltyjä käyttöoikeuksia. Henkilötietoja tulee päästä käsittelemään vain niiden, joilla siihen on työtehtäviensä vuoksi perusteltu oikeus. Järjestelmien pääkäyttäjien tulee valvoa käyttöoikeuksien tarkoituksenmukaisuutta ja ajantasaisuutta. Erityisesti silloin, kun järjestelmässä käsitellään arkaluontoisia henkilötietoja, siinä tulee olla myös lokiseuranta, josta on nähtävissä, kuka tietoja on käynyt katsomassa ja mahdollisesti muuttamassa. Henkilötietojen säilyttämiseen tai käsittelyyn muualla kuin tietojärjestelmissä (verkkolevyt, paperi jne.) on oltava selkeä peruste, ja tietojen riittävästä suojaamisesta oikeudettomalta käytöltä on huolehdittava.

Henkilötietoja ei säilytetä kauempaa kuin niiden käyttötarkoituksen vuoksi on välttämätöntä. Joissakin tapauksissa tietojen säilytysaika on arkistoinnin normien vuoksi pidempi, ja tietojen säilyttäminen perustellussa arkistointitarkoituksessa on mahdollista. Tietojärjestelmiltä edellytetään tiedon elinkaaren huomiointia, mikä tarkoittaa tietosuoja- ja tietoturvanäkökulmasta erityisesti tarpeettomien tietojen poistumista määritellyn ajan jälkeen.



Tietojen luovuttaminen

Luovutuksia voidaan tehdä vain säädösten hyväksymiin tarkoituksiin (tietosuoja-asetus ja -laki, julkisuuslaki, erityislainsäädäntö). Luovutuksen mahdollisuudesta on kerrottava rekisteröidylle. Luovutuksen saajilta edellytetään sitoutumista säädösten mukaiseen henkilötietojen käsittelyyn, mukaan lukien tietojen tuhoaminen käyttötarpeen päätyttyä.

Yhteystiedot

Tietosuoja-asioissa ensisijainen yhteyshenkilö on kunnan tietosuojavastaava, joka on tarvittaessa yhteydessä tietosuojavaltuutettuun ja muihin tahoihin. Rekisterikohtaiset yhteyshenkilöt on nimetty tietosuojaselosteissa.

Tietosuojaperiaatteiden päivittäminen

Tietosuojaperiaatteet ovat tämän hetken käytäntömme mukaiset. Periaatteita päivitetään säännöllisesti. Suurempiin muutoksiin tarvitaan kunnanhallituksen hyväksyntä.