Nakkilan kunta

Tietosuojapolitiikka

Sisällys

Johdanto

Euroopan unionin yleinen tietosuoja-asetus on tullut voimaan toukokuussa 2016, ja sitä sovelletaan kansallisesti 25.5.2018 alkaen. Asetuksen tavoitteena on varmistaa rekisteröityjen oikeus henkilötietojen suojaan ja yksityisyyteen. Tietosuoja-asetus velvoittaa yritysten ja julkishallinnollisten toimijoiden huolehtimaan rekisterinpidon, henkilötietojen käsittelyn sekä rekisteröidyn henkilön tietojen käsittelyn laillisuudesta ja asianmukaisuudesta.

EU:n tietosuoja-asetus asettaa henkilötietojen käsittelylle uusia vaatimuksia toimintatapojen, tiedon elinkaaren hallinnan ja tietojärjestelmien osalta. Rekisterinpitäjän on suunniteltava toimintansa siten, että henkilötietojen käsittelyä koskevat tiedot on tarvittaessa esitettävissä läpinäkyvässä, helposti ymmärrettävässä ja saatavilla olevassa muodossa. Tietosuojapolitiikka määrittää ne periaatteet, toimintatavat, vastuut, valvonnan ja seuraamusjärjestelmän, joita noudatetaan Nakkilan kunnan tietosuojan toteuttamisessa ja kehittämisessä. Tämä tietosuojapolitiikka koskee henkilötietojen käsittelyä, jossa Nakkilan kunta toimii rekisterinpitäjänä.

EU:n yleinen tietosuoja-asetusta (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016) sovelletaan 25.5.2018 lähtien.

Suomen perustuslain 10 §:ssä henkilötietojen suojaa koskeva säännös on sisällytetty osaksi yksityiselämän suojaa koskevaa perusoikeussäännöstä.

Kansallisesti Suomessa noudatetaan kansallista yleistä tietosuojalakia, jolla täsmennetään ja täydennetään EU:n tietosuoja-asetusta.

EU:n tietosuoja-asetuksen ja kansallisen tietosuojalain lisäksi tietosuojaan liittyen tulee huomioida erityislakeja, esim. tasa-arvolaki ja laki yksityisyyden suojasta työelämässä/työelämän tietosuojalaki.

Nakkilan kunnan palveluiden perustana ovat kuntalaisten tarpeet. Palveluiden tuottaminen perustuu tietoon ja sen käsittelyyn Nakkilan kunnan ja sen konsernin toimintaympäristöissä. Kunnan palvelutuotanto on riippuvainen ICT-teknologiasta ja -palveluiden keskeytyksettömästä ja turvallisesta toiminnasta. Tehokas digitalisointi edellyttää tietoturvallisuuden kaikkien osa-alueiden huomioimisen lisäksi myös tietosuojan huomioimista jo suunnitteluvaiheessa.

Tietosuojassa ei ole kysymys tiedon ”panttaamisesta" tai "pimittämisestä" vaan tietosuojaosaamisella voidaan lisätä organisaation tuottavuutta ja tehokkuutta sekä säästää kustannuksia. EU:n yleisen tietosuoja-asetuksen myötä tietosuojasta, tietosuojatyön organisoinnista ja itse tietosuojatyöstä, sekä koko henkilöstön tietosuojaosaamisesta tulee organisaatioiden operatiivisen toiminnan menestystekijä.

Nakkilan kunnan johto tietosuojatoiminnan omistajana määrittelee tässä politiikassa johtamiseen, palveluihin ja toimintoihin liittyvät tietosuojaperiaatteet, vastuut ja tavoitteet. Politiikka toimii perustana Nakkilan kunnan tietosuojaa koskeville alapolitiikoille ja ohjeille, joiden tehtävänä on tarkentaa politiikassa annettuja määräyksiä ja ohjeistaa niiden soveltamista käytäntöön.

Tietosuojapolitiikka koskee koko kuntaorganisaatiota ja sen henkilöstöä mukaan lukien kuntakonsernin sekä niitä Nakkilan kunnan sidosryhmien edustajia, jotka toimeksiantojensa puitteissa käsittelevät Nakkilan kunnan omistamaa tai hallinnoimaa tietoa. Politiikka kattaa Nakkilan kunnan omistaman tiedon riippumatta sen esitystavasta, muodosta, suojaustasosta tai elinkaaren vaiheesta. Tietosuojapolitiikka liitetään tarvittaessa Nakkilan kunnan toimeksiantosopimuksiin.

Tietosuojan määritelmä

Oikeus henkilötietojen suojaan on jokaiselle kuuluva perusoikeus. Viranomaisen asiakirjat ovat lähtökohtaisesti julkisia (Perustuslaki § 12), jollei sitä julkisuuslaissa tai muussa laissa erikseen toisin säädetä. Julkisuuden ja avoimuuden ohella oikeus yksityisyyden ja henkilötietojen suojaan (Perustuslaki § 10) on jokaiselle kuuluva perusoikeus. Henkilötietojen suojasta säädetään erikseen.

Tämä tarkoittaa, että henkilötietojen käsittelyn on yhtäältä oltava asianmukaista ja toisaalta sen on aina tapahduttava tiettyä tarkoitusta varten ja asianomaisen henkilön suostumuksella tai muun laissa säädetyn oikeuttavan perusteen nojalla. Henkilötietojen suojalla tarkoitetaan myös jokaiselle turvattua oikeutta tutustua niihin tietoihin, joita hänestä on kerätty ja tarvittaessa myös saada hänestä kerätyt tiedot muutetuiksi tai poistetuiksi, mikäli tietojen oikaisu on tarpeen.

Tietosuojan tavoitteet ja periaatteet

Nakkilan kunnan lähtökohtana tietosuojassa on riskilähtöisyys. Nakkilan kunta rekisterinpitäjänä arvioi henkilötietojen käsittelyyn liittyvät riskit ja valitsee arvioidun riskitason mukaan tarvittavat hallintatoimenpiteet. Tietosuojariskien hallinta on osa Nakkilan kunnan riskienhallintaprosessia, jolloin erityisesti merkittävän tason riskit raportoidaan johdolle saakka. Riskilähtöisyys ohjaa organisaation henkilötietojen käsittelyä ja on erittäin tärkeä osa rekisterinpitäjän osoitusvelvollisuuden toteuttamista.

Nakkilan kunta toteuttaa riskilähtöisen toimintaperiaatteen varmistamiseksi tietosuojan vaikutustenarviointeja sellaisten henkilötietojen käsittelytoimille, joiden suunnitteluvaiheessa on todennäköistä, että käsittelytoimiin liittyy yksilöiden oikeuksien ja vapauksien kannalta merkittäviä riskejä. Vaikutustenarvioinnin tuloksia käytetään niiden hallintakeinojen määrittelemisessä, joilla pyritään pienentämään henkilötietojen käsittelyn riskitasoa. Samalla varmistetaan tietosuoja-asetuksen vaatimusten toteutuminen.

Nakkilan kunnan toiminnassa toteutetaan sisäänrakennetun ja oletusarvoisen tietosuojan periaatetta. Tietosuoja otetaan huomioon monipuolisesti perustoiminnan yhteydessä mm. johtamisessa, hankinnoissa, kehitystyössä sekä toimintaprosesseissa. Tietosuojan oikeanlainen toteutuminen varmistetaan myös käyttämällä tilannekohtaisesti parhaita mahdollisia teknisiä ja organisatorisia riskiarvioon perustuvia ratkaisuja.

Nakkilan kunnan tavoitteena on huolehtia tietosuoja-asetuksen mukaisten rekisteröityjen oikeuksien toteutumisesta dokumentoimalla ja ohjeistamalla henkilötietojen käsittelyn käytänteet sekä huolehtimalla käyttäjäkoulutuksesta toteuttaakseen laadukasta ja lainmukaista henkilötietojen käsittelyä.

Henkilötietojen käsittely toteutetaan noudattamalla alla lueteltuja periaatteita:

- henkilötietoja käsitellään lainmukaisesti, asianmukaisesti sekä läpinäkyvästi
- henkilötietoja käsitellään suunnitellun käyttötarkoituksen mukaisesti
- henkilötietoja kerätään käyttötarkoituksen mukainen määrä, ei enempää
- henkilötietojen käsittely toteutetaan täsmällisesti
- henkilötietoja säilytetään käyttötarkoituksen kannalta tarkoituksenmukainen aika
- henkilötietojen käsittelyssä toteutetaan henkilötietojen eheyden ja luottamuksellisuuden periaatetta

Tietosuojan toteutuminen

EU:n tietosuoja-asetus velvoittaa rekisterinpitäjän arvioimaan henkilötietojen käsittelyn prosesseja koko henkilötiedon elinkaaren ajan. Henkilörekistereistä laadituissa tietosuojaselosteissa ja tietosuojan hallintamallissa kuvataan, miten henkilötietoja sisältäviä tietovarantoja ylläpidetään, millaisia tietovirtoja henkilötiedoista muodostuu ja mikä on näiden tietojen elinkaari. Arkaluonteisia tietoja ei kerätä, tallenneta tai käsitellä tarpeettomasti.

Nakkilan kunta toteuttaa ja sisällyttää tietosuojaperiaatteet ja -vaatimukset jo aikaisessa vaiheessa osaksi henkilötietojen käsittelyä. Näin varmistetaan, että käsittely vastaa tietosuoja-asetuksen vaatimuksia. Kunta toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet ja menettelyt tietosuojan varmistamiseksi ja rekisteröityjen oikeuksien toteutumiseksi. Toimintaperiaatteilla ja ohjeistuksella varmistetaan, että:

- kerätään vain henkilötietoja, jotka ovat välttämättömiä käsittelytarkoituksen kannalta
- henkilötietoja ei säilytetä kauemmin kuin on välttämätöntä kyseisessä käsittelytarkoituksessa
- henkilötietoja ei saateta rajoittamattoman henkilömäärän saataville

Tietosuojan toteuttamisessa kunta haluaa varmistaa tietosuojalainsäädännön vaatimusten toteutumisen koko käsiteltävien henkilötietojen elinkaaren ajan.

Nakkilan kunta huolehtii henkilöstön riittävästä tietosuojaosaamisesta henkilöstökoulutuksien ja informaation välittämisen kautta. Tietosuojavastaava koordinoi koulutusta.

Uudet työntekijät perehdytetään tietosuoja-asioihin. Erityisesti tämä korostuu niissä rooleissa, joissa käsitellään arkaluonteisia henkilötietoja.

Henkilörekisterit, tietovarannot ja tietoturva

Kunnan tulee tunnistaa ja määritellä kaikki hallitsemansa henkilörekisterit ja tietovarannot omassa toiminnassaan.

Henkilötietojen käsittely edellyttää käsittelyn lainmukaisuuden varmistamista. EU:n tietosuoja-asetuksen artiklassa 6 on kerrottu henkilötietojen käsittelyn edellytykset. Kaikille kerätyille henkilötiedoille tulisi olla lainmukainen perustelu. Henkilötietojen käsittelyn lainvoimaisuus tulisi aina arvioida miettien, mihin käyttötarkoitukseen henkilötietoja tarvitaan ja onko käyttötarkoitukseen lainmukainen käsittelyoikeus.

EU:n tietosuoja-asetus velvoittaa rekisterinpitäjän arvioimaan vaikutukset rekisteröidylle, mikäli hänen henkilötietoihinsa päästäisiin lainvastaisesti, henkilötiedot muuttuisivat tahtomatta tai henkilö- tiedot katoaisivat. Lisäksi rekisterinpitäjä arvioi henkilötietojen käsittelyn laajuuden (rekisteröityjen määrä) ja luonteen sekä arvioi, minkälaisia teknisiä ja organisatorisia suojatoimia henkilötietojen suojaamiseen tarvitaan. Mitä arkaluontoisempia tietoja tietojärjestelmässä on, sitä vahvempia tieto- turvaratkaisuja ja muita suojatoimia toteutetaan.

Rekisterinpitäjä on vastuullinen koko rekisterin, ei pelkästään sovelluksen, tietoturvasta. Rekisterin- pitäjän tulee arvioida sovelluksen lisäksi esim. mahdollisen paperiarkiston tietoturva ja rekisteriin liittyvien prosessien tietoturva.

Rekisterinpitäjä on vastuussa sovellusten ja ohjelmistoympäristöjen käyttöoikeuksien hallinnasta.

Rekisteröidyn tietopyyntöprosessi

Henkilötietoja käsitellään rekisteröidyn kannalta läpinäkyvästi. Nakkilan kunnassa on määritetty toimintaprosessi ja ohje liittyen toimintaan rekisteröityjen käyttäessä oikeuttaan päästä omiin henkilötietoihinsa. Toimintatapaa noudatetaan niissä tapauksissa, joissa rekisteröidyt haluavat saada nähtäväkseen omia rekistereissä olevia henkilötietojaan. Tietopyyntö osoitetaan kirjaamoon tietosuojavastaavalle erillisellä tietopyyntölomakkeella.

Toiminta tietoturva ja tietosuojapoikkematilanteissa sekä ilmoitusvelvollisuus

Henkilötietojen tietoturvaloukkauksen sattuessa kunnalla on rekisterinpitäjänä ilmoitusvelvollisuus valvontaviranomaisen sekä rekisteröidyn suuntaan. Valvontaviranomaiselle tehdään ilmoitus tietosuoja-asetuksen mukaisesti 72 tunnin kuluessa siitä, kun henkilötietojen tietoturvaloukkaus on tullut ilmi. Kunnassa on määritetty toimintaprosessi tietoturva- ja suojaloukkausten varalle. Henkilötietojen tietoturvaloukkaus ilmoitetaan rekisteröidylle ilman aiheetonta viivytystä. Tietosuojavastaava vastaa tietosuojapoikkeaman ilmoitusvelvollisuudesta.