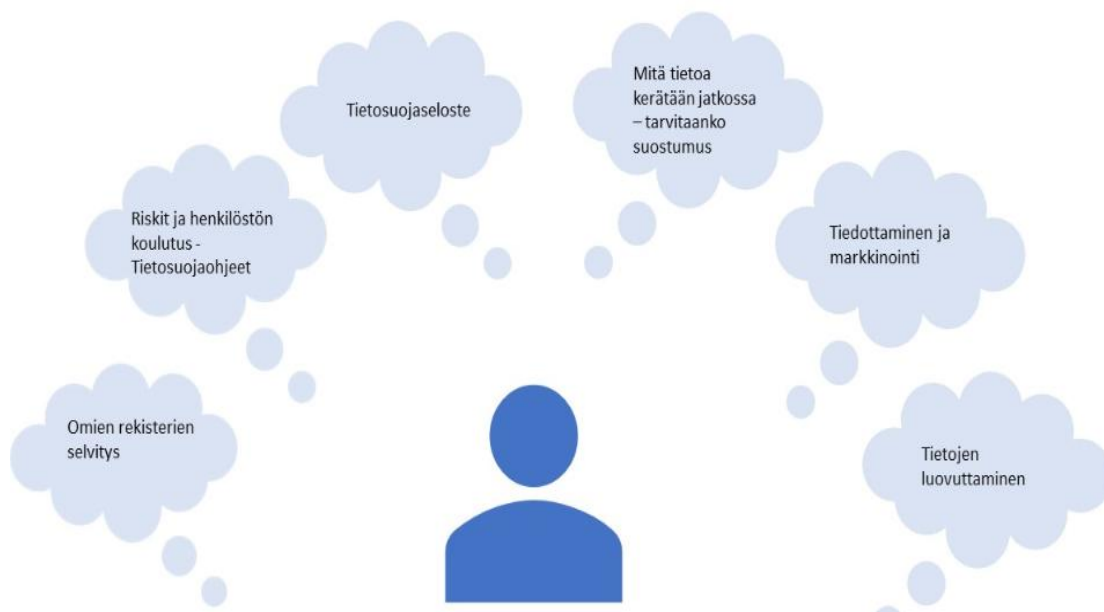


Tampereen ympäristökuntien tietosuojapolitiikka



Hämeenkyrö-Kangasala-Lempäälä-Nokia-Orivesi-Pirkkala-Vesilahti-Ylöjärvi

Kunnanhallitus 14.5.2018

Tampereen ympäristökuntien tietosuojapolitiikka

Johdanto

Tietosuojapolitiikka määrittää ne periaatteet, toimintatavat, vastuut, valvonnan ja seuraamusjärjestelmän, joita noudatetaan Hämeenkyrön kunnan tietosuojan toteuttamisessa ja kehittämisessä. Tämä tietosuojapolitiikka koskee henkilötietojen käsittelyä, jossa Hämeenkyrön kunta toimii rekisterinpitäjänä.

Hämeenkyrön kunnan palveluiden perustana ovat kuntalaisten tarpeet. Palveluiden tuottaminen perustuu tietoon ja sen käsittelyyn Hämeenkyrön kunnan ja sen konsernin toimintaympäristöissä. Kunnan palvelutuotanto on riippuvainen ICT-teknologiasta ja -palveluiden keskeytyksettömästä ja turvallisesta toiminnasta.

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.

Hämeenkyrön kunnan johto tietosuojatoiminnan omistajana määrittelee tässä politiikassa johtamiseen, palveluihin ja toimintoihin liittyvät tietosuojaperiaatteet, vastuut ja tavoitteet. Poliitiikka toimii perustana Hämeenkyrön kunnan tietosuoja 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 Hämeenkyrön kunnan sidosryhmien edustajia, jotka toimeksiantojensa puitteissa käsittelevät Hämeenkyrön kunnan omistamaa tai hallinnoimaa tietoa. Poliitiikka kattaa Hämeenkyrön kunnan omistaman tiedon riippumatta sen esitystavasta, muodosta, suojaustasosta tai elinkaaren vaiheesta.

Tämä politiikka liitetään tarvittaessa Hämeenkyrön kunnan toimeksiantosopimuksiin.

Tietosuojan määritelmä

Oikeus henkilötietojen suojaan on jokaiselle kuuluva perusoikeus. 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

Hämeenkyrön kunnan lähtökohtana tietosuojassa on riskilähtöisyys. Hämeenkyrön kunta rekisterinpitäjänä arvioi henkilötietojen käsittelyyn liittyvät riskit ja valitsee arvioidun riskitason mukaan tarvittavat hallintatoimenpiteet. Riskilähtöisyys ohjaa organisaation henkilötietojen käsittelyä ja on erittäin tärkeä osa rekisterinpitäjän osoitusvelvollisuuden toteuttamista.

Hämeenkyrön 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. Hämeenkyrön 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.

Hämeenkyrön kunnan tavoitteena on huolehtia tietosuojaa-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 toteuttaminen

Hämeenkyrön kunta haluaa toteuttaa sisäänrakennetun ja oletusarvoisen tietosuojan periaatetta ja sisällyttää tietosuojaperiaatteet ja -vaatimukset jo aikaisessa vaiheessa osaksi henkilötietojen käsittelyä. Näin varmistetaan, että käsittely vastaa tietosuojaa-asetuksen vaatimuksia. Hämeenkyrön kunta toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet ja menettelyt tietosuojan varmistamiseksi. Edellä mainittujen toimenpiteiden avulla varmistetaan mm, että:

1. oletusarvoisesti kerätään vain henkilötietoja, jotka ovat välttämättömiä käsittelytarkoituksen kannalta
2. tietoja ei kerätä eikä säilytetä suurempia määriä eikä kauemmin kuin on välttämätöntä kyseiseen käsittelytarkoitukseen
3. henkilötietoja ei oletusarvoisesti saateta rajoittamattoman henkilömäärän saataville
4. taataan rekisteröityjen oikeuksien toteutuminen
5. taataan henkilötietojen suoja tarvittavin tietoturvakeinoin

Hämeenkyrön kunnan järjestelmä- ja sovelluskehitysprosesseissa on mukana työvaiheet, joissa analysoidaan henkilötietojen käyttötarkoituksiin sovellettavat tietosuojavaatimukset. Sovellettavat tietosuojavaatimukset vaihtelevat kerättävien henkilötietojen ja tietojen käyttötarkoituksen mukaan. Tietosuojavaatimuksia ovat toimialakohtaiset lait esimerkiksi terveydenhuollossa sekä käsiteltäessä työntekijöiden henkilötietoja työnantajan roolissa. Tekninen toteutus suunnitellaan siten, että se vastaa käsittelyn riskitasoa. Riskitason perusteella valitaan tilanteeseen sopivat hallintakeinot riskitason hallitsemiseksi ja vaatimustenmukaisuuden saavuttamiseksi. Hallintakeinojen valinnassa huomioidaan parhaat mahdolliset käytännöt tietoturvan suhteen.

Hämeenkyrön kunta voi rekisterinpitäjänä ulkoistaa valitsemansa osan henkilötietojen käsittelystä toimeksisaajalle, henkilötietojen käsittelijälle. Hämeenkyrön kunta valitsee sopimuskumppanikseen vain sellaisia henkilötietojen käsittelijöitä, jotka noudattavat hyvää henkilötietojen käsittelytapaa asianmukaisten teknisten ja organisatoristen toimenpiteiden avulla sekä täyttävät tietosuojaa-asetuksen vaatimukset ja pystyvät huolehtimaan rekisteröidyn oikeuksien toteutumisesta. Henkilötietojen käsittelyä sisältävien hankintojen kohdalla tietosuojaan liittyvät näkökohdat huomioidaan jo hankinnan suunnitteluvaiheessa ja saatetaan ne osaksi tarjouspyyntöä.

Rekisteröityjen tietopyyntöprosessi

Hämeenkyrön kunnassa määritellään toimintaprosessi ja ohje liittyen toimintaan rekisteröityjen käyttäessä oikeuttaan saada pääsy henkilötietoihinsa. Tämän prosessin mukaista toimintatapaa noudatetaan niissä tapauksissa, joissa rekisteröidyt haluavat saada nähtäväkseen omia rekistereissä olevia henkilötietojaan.

Henkilöstön tietosuojakoulutus

Hämeenkyrön kunta huolehtii henkilöstön riittävästä tietosuojasaamisesta henkilöstökoulutuksien ja informaation välittämisen kautta. Myös organisaatioon tulevat uudet työntekijät perehdytetään tietosuoja-asioihin järjestelmällisesti. Erityisesti tämä korostuu niissä rooleissa, joissa käsitellään henkilötietoja ja toteutetaan rekisteröityjen oikeuksien toteuttamisprosesseja.

Toiminta tietosuojapoikkeamatilanteissa sekä ilmoitusvelvollisuus

Hämeenkyrön kunnassa määritellään toimintaprosessi ja ohje liittyen toimintaan tietosuojaloukkausten tapahtuessa. Kunnan toiminta kriisitilanteissa perustuu lakisääteiseen valmiussuunnitteluun. Kunnan palveluista vastaavat palvelu- ja vastuualueet sekä yksiköt ja liikelaitokset, laativat kukin omat suunnitelmansa kriisien varalle.

Keskeisiä käsitteitä

Anonymisointi

Henkilötiedon tunnistettavuuden poistaminen siten, että yhdistäminen rekisteröityyn ei enää ole mahdollista.

Hallinnollinen sakko

Valvontaviranomainen voi määrätä rekisterinpitäjälle tai henkilötietojen käsittelijälle sakon tietosuoja-asetuksen vaatimusten laiminlyönnistä. Sakon suuruus määräytyy rikkomuksen luonteen perusteella.

Hallinnolliset seuraamukset

Valvontaviranomaisen määräämät seuraamukset koskien tietosuoja-asetuksen vaatimusten laiminlyöntejä.

Henkilötieto

Kaikki tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyvät tiedot (esim. nimi, henkilötunnus, kuva, biometrinen tai geneettinen tieto). Tunnistettavissa olevana pidetään henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, sijaintitiedon, verkkotunnistetietojen tai yhden tai useamman henkilölle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella.

Henkilötietojen erityiset tietoryhmät, arkaluonteiset henkilötiedot

Tiedot, joista ilmenee rotu tai etninen alkuperä, poliittisia mielipiteitä, uskonnollinen tai filosofinen vakaumus, ammattiliiton jäsenyys, geneettisiä tietoja, terveyttä koskevia tietoja, tai seksuaaliseen käyttäytymiseen liittyviä tietoja. Erityisiä tietoryhmiä koskeva käsittely on erikseen säänneltyä.

Henkilötietojen käsittelijä

Luonnollinen tai oikeushenkilö, viranomainen, virasto tai muu elin, joka käsittelee henkilötietoja rekisterinpitäjän toimeksiannosta.

Henkilötietojen käsittely

Kaikenlaiset toiminnot, joita kohdistetaan henkilötietoihin joko automaattista tietojenkäsittelyä hyödyntäen tai manuaalisesti. Käsittelyä ovat esimerkiksi henkilötietojen kerääminen, tallentaminen, järjestäminen, jäsentäminen, säilyttäminen, muokkaaminen, haku, käyttö, luovuttaminen, levittäminen tai saattaminen muutoin saataville, yhteensovittaminen, yhdistäminen, rajoittaminen, poistaminen ja hävittäminen.

Henkilötietojen tietoturvaloukkaus

Tietoturvaloukkaus, jonka seurauksena on henkilötietojen lainvastainen käsittely. Loukkauksesta seuraa siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen tai saanti.

Lapsen henkilötietojen käsittely

Alle 16-vuotiaiden lasten henkilötietojen käsittely ei ole sallittua ilman vanhemman suostumusta. Jäsenvaltioilla on mahdollisuus soveltaa alemmaa ikärajaa, joka voi alimmillaan olla 13 vuotta.

Pseudonymisointi

Henkilötietojen käsittelemistä niin, että tietoja ei voida enää suoraan yhdistää tiettyyn rekisteröityyn käyttämättä lisätietoja. Tällaiset lisätiedot tulee säilyttää erillään ja niihin sovelletaan teknisiä ja organisatorisia toimenpiteitä, joilla varmistetaan, ettei tällaista yhdistämistä tunnistettuun tai tunnistettavissa olevaan henkilöön tapahdu.

Rekisterinpitäjä

Luonnollinen tai oikeushenkilö, julkinen viranomainen, virasto tai muu elin, joka yksin tai yhteistyössä muiden kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.

Rekisteröity

Henkilö, jonka henkilötietoja käsitellään.

Rekisteriseloste, tietosuojaseloste

Dokumentti, joka rekisterinpitäjän tulee laatia ja pitää yleisesti saatavilla. Sen tulee kuvata henkilötietojen käsittely tiiviisti esitetystä, avoimesta ja helposti ymmärrettävässä muodossa.

Sisäänrakennettu ja oletusarvoinen tietosuoja

Tietosuojaperiaatteiden sisällyttäminen aikaisessa vaiheessa henkilötietojen käsittelyn osaksi. Periaatteiden huomioiminen käsittelytapojen määrittelyn ja itse käsittelyn yhteydessä, siten että varmistetaan käsittelyn vastaavuus tietosuoja-asetuksen vaatimusten kanssa.

Rekisterinpitäjän tulee toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet ja menettelyt, jotta mm.

- oletusarvoisesti kerätään vain henkilötietoja, jotka ovat välttämättömiä ja tarpeellisia käsittelytarkoituksen kannalta
- tietoja ei kerätä eikä säilyttää suurempia määriä eikä kauemmin kuin on tarpeellista kyseiseen tarkoitukseen
- henkilötietoja ei oletusarvoisesti saateta rajoittamattoman henkilö määrän saataville
- taataan rekisteröityjen oikeuksien toteutuminen

Tietosuoja-asetuksen vaatimusten toteutuminen tulee taata määrittelyvaiheesta aina koko käsiteltävien henkilö-tietojen elinkaaren loppuun.

Tietosuoja

Tietosuojalla tarkoitetaan toimenpiteitä, joiden tarkoituksena on suojata henkilön yksityisyys henkilötietojen käsittelyssä.

Tietosuojapolitiikka

Johdon hyväksymä näkemys tietosuojan päämääristä, periaatteista ja toteutuksesta.

Tietotilinpäätös

Tietotilinpäätös on organisaation laatima vapaaehtoinen raportti, joka antaa kokonaiskuvan organisaation tietojenkäsittelyn nykytilasta. Raportti on tarkoitettu johdon työkaluksi ja lisäämään sidosryhmien luottamusta siihen, että organisaatio noudattaa hyvää sääntelyn mukaista tietojenkäsittelytapaa henkilötietojen käsittelyssä. Tietotilinpäätöstä voidaan käyttää yhtenä keinona tietosuoja-asetuksen osoitusvelvollisuuden toteuttamisessa.

Tietoturva

Järjestelyt, joilla pyritään varmistamaan tiedon käytettävyys, eheys ja luottamuksellisuus. Tietoturvallisuus on riskienhallintaa ja osa yrittäjästä.

Vaikutustenarviointi

Suunniteltujen henkilötietojen käsittelytoimien vaikutusten arviointi tietosuojaan ja yksilön vapauksiin. Jos käsittely todennäköisesti aiheuttaa yksilön oikeuksien ja vapauksien kannalta suuren riskin, rekisterinpitäjän on ennen käsittelytoimien aloittamista toteutettava tietosuojan vaikutustenarviointi ja määriteltävä toimenpiteitä, joilla riskiä voidaan hallita. Valvontaviranomainen tulee julkaisemaan luettelon käsittelytoimista, jotka vaativat vaikutustenarvioinnin laatimisen.