9.8.2019

Kouvolan kaupungin digitaalisen turvallisuuden politiikka ja tietosuojapolitiikka

LIITE 1 Terminologia

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

Hallinnollinen sakko: Valvontaviranomaisen rekisterinpitäjälle tai henkilötietojen käsittelijälle määräämä sakko tietosuoja-asetuksen vaatimusten laiminlyönnistä. Suuruus määräytyy rikkomuksen luonteen perusteella ja on enimmäismäärältään 20 milj. € tai 4% yrityksen edeltävän tilikauden kokonaisliikevaihdosta. Vaikka sakkoa ei kansallisen lain esitöiden mukaan ole tarkoitus kohdistaa suoraan julkiseen toimijaan (kaupunkiin), voivat sen vaikutukset kohdistua kaupunkiin henkilötietojen käsittelijöiden kanssa solmittujen sopimusten vahingonkorvauspykälien kautta.

Hallinnolliset seuraamukset: Valvontaviranomaisen määräämät seuraamukset koskien tietosuoja-asetuksen vaatimusten laiminlyöntejä. Koskee sekä julkisia että yksityisiä toimijoita.

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 eheys ja luottamuksellisuus: Tietojen säilyttäminen muuttumattomina ja turvallisesti siten, että niihin pääsevät käsiksi vain sellaiset henkilöt, joiden työtehtävien hoitamiseksi tiedot ovat välttämättömiä. Luottamuksellisuus varmistetaan joko lainsäädännön tai sopimusten kautta.

Henkilötietojen erityiset tietoryhmät, arkaluonteiset henkilötiedot: Tiedot, joista ilmenee rotu tai etninen alkuperä, poliittinen mielipide, 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 minimointi: Henkilötietoja tulee kerätä ainoastaan siinä määrin, kuin se on välttämätöntä kyseessä olevan tehtävän hoitamiseksi.

Henkilötietojen tietoturvaloukkaus: Tahallinen tai tahaton tapahtuma, 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.

IRT: Incident Responsible Team. Selvitystyöryhmä, joka kokoontuu laajojen tietoturvapoikkeamien selvityksen yhteydessä. Koordinoi poikkeaman selvitystyötä.

Kyberturvallisuus: Kyberturvallisuudessa tunnistetaan, ehkäistään ja varaudutaan (yhteiskunnalle ja organisaatiolle) merkittävien ICT-toimintojen häiriöihin. Se yhdistää laaja-alaisesti riskienhallinnan, tietoturvallisuuden, tietosuojan, jatkuvuuden hallinnan, sekä varautumis- ja toipumissuunnittelun kokonaisuuksia.

Lapsen henkilötietojen käsittely: Lähtökohtaisesti alle 16-vuotiaiden lasten henkilötietojen käsittely ei ole sallittua ilman vanhemman suostumusta. Jäsenvaltioilla on mahdollisuus soveltaa alempaa ikärajaa, joka voi alimmillaan olla 13 vuotta. Erityislainsäädännössä voidaan soveltaa myös muita ikärajoja. Suomessa ikärajaksi on kaavailtu 13-vuoden ikää.

Käyttötarkoitussidonnaisuus: Henkilötietoja voidaan kerätä ja niitä voidaan käsitellä vain rekisterin ilmoitetun käyttötarkoituksen ja oikeusperusteen mukaisesti.

Osoitusvelvollisuus: Osoitusvelvollisuuden (accountability) avulla organisaation tulee kyetä näyttämään, että se on huolehtinut seuraavista henkilötietojen käsittelyn osa-alueista:

- lainmukaisuus, kohtuullisuus ja läpinäkyvyys
- käyttötarkoitussidonnaisuus
- tietojen minimointi
- täsmällisyys
- säilytyksen rajoittaminen ja
- eheys ja luottamuksellisuus.

Profilointi: Mikä tahansa henkilötietojen automaattinen käsittely, jossa arvioidaan kyseisen henkilön henkilökohtaisia ominaisuuksia henkilön tietoja käyttäen. Erityisesti analysoidaan tai ennakoidaan työsuoritukseen, taloudelliseen tilanteeseen, terveyteen, henkilökohtaisiin mieltymyksiin tai kiinnostuksen kohteisiin, luotettavuuteen tai käyttäytymiseen sekä sijaintiin tai liikkeisiin liittyviä asioita. Profilointia käytetään lukuisissa sosiaalisen median palveluissa ja osassa päätelaitteita käytössä olevissa sovelluksissa.

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.

Rekisteriseloste, tietosuojaseloste: Tietosuoja-asetuksen vaatimusten mukainen informointidokumentti, joka rekisterinpitäjän tulee laatia ja pitää yleisesti saatavilla. Sen tulee kuvata henkilötietojen käsittely tiiviisti esitetyssä, avoimessa ja helposti ymmärrettävässä muodossa.

Rekisteröity: Henkilö, jonka henkilötietoja käsitellään.

Riskien arviointi: Tietoturvaloukkauksen tai henkilötietojen tietoturvaloukkauksen aiheuttaman tietoihin tai henkilötietoihin kohdistuvien uhkien ja haavoittuvuuksien arvottaminen vakavuuden ja todennäköisyyden perusteella. Tietosuoja-asetuksen mukainen riskien arviointi on tehtävä rekisteröidyn näkökulmasta.

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 säilytetä suurempia määriä eikä kauemmin kuin on tarpeellista kyseiseen tarkoitukseen
- henkilötietoja ei oletusarvoisesti saateta rajoittamattoman henkilömäärän saataville
- taataan rekisteröityjen oikeuksien toteutuminen

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

Säilytyksen rajoittaminen: Henkilötietojen säilyttämiselle lainsäädännössä, muussa viranomaisten ohjeistuksessa tai arkistonmuodostamissuunnitelmassa (toiminnanohjaussuunitelmassa) asetettu määräaika, jonka jälkeen tiedot on tuhottava. Vaihtoehtoisesti kyseeseen voi tulla lainmukainen peruste, jos säilyttämisen rajoittamisesta poiketaan.

Tiedollinen itsemääräämisoikeus: Rekisteröidyn oikeus henkilötietojaan kohtaan. Näihin oikeuksiin kuuluvat asetuksen mukaisesti mm. pääsy tietoihin, tietojen oikaiseminen ja poistaminen, oikeus rajoittaa käsittelyä ja oikeus siirtää tiedot järjestelmästä toiseen. Tiedolliseen itsemääräämisoikeuteen kuuluu keskeisesti oikeus saada tietoa henkilötietojen käsittelystä.

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

Tietoturvaloukkaus: Tahallinen tai tahaton tapahtuma, jonka seurauksena organisaation omistamaa tai hallinnoimaa tietoa on joutunut valtuudettoman henkilön käyttöön, tai joku on tahallaan tai tahattomasti estänyt organisaation tietojen käsittelyn organisaatiolle ominaisella tavalla ja sen omistamilla tai hallinnoimilla tietojenkäsittelylaitteilla.

Tietoturvapoikkeama: Tahallinen tai tahaton tapahtuma tai olotila, jonka seurauksena organisaation vastuulla olevien tietojen ja palvelujen eheys, luottamuksellisuus tai tarkoituksenmukainen käytettävyystaso on tai saattaa olla vaarantunut. Katso myös kohta henkilötietojen tietoturvaloukkaus ja tietoturvaloukkaus.

Tietosuojan sertifiointimekanismit: Tietosuojaa koskevia sertifiointimekanismeja, tietosuojasinettejä ja -merkkejä kannustetaan ottamaan käyttöön erityisesti Euroopan Unionin tasolla. Niiden tarkoitus on osoittaa, että rekisterinpitäjä ja/tai käsittelijä, jolle sertifikaatti, sinetti tai merkki on myönnetty, noudattaa hyvää tietojenkäsittelytapaa ja asetuksen vaatimuksia. Euroopan tietosuojaneuvosto tulee kokoamaan kaikki saataville tulevat sertifiointimekanismit julkisesti nähtäville.

Tietosuojapolitiikka: Johdon hyväksymä näkemys tietosuojan päämääristä, periaatteista ja toteutuksesta.

Tietosuojavastaava: Tietosuoja-asetuksen määrittelemä rooli organisaatiossa, jonka rekisterinpitäjän ja henkilötiedon käsittelijän on nimettävä määritellyissä tilanteissa. Asetus määrittelee myös tietosuojavastaavan aseman ja toimenkuvan.

Tietotilinpäätös: Organisaation laatima vapaaehtoinen raportti, joka antaa kokonaiskuvan organisaation tietojenkäsittelyn nykytilasta. Raportti on tarkoitettu johdon työkaluksi ja lisäämään sidosryhmien luottamusta siihen, että organisaatio noudattaa hyvää ja sääntelyn mukaista

tietojenkäsittelytapaa henkilötietojen käsittelyssä. Raportin informaatio on tärkeää myös tietosuojavastaavien työlle. Tietotilinpäätöstä voidaan käyttää yhtenä keinona tietosuoja-asetuksen osoitusvelvollisuuden toteuttamisessa.

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

Turvallisuussitoumus: Turvallisuussitoumuksella tarkoitetaan käyttäjien työasemille avautuvaa tietoturvasitoumusta.

Vaikutustenarviointi (DPIA): Suunniteltujen henkilötietojen käsittelytoimien vaikutusten arviointi tietosuojaan ja yksilön vapauksiin liittyen. Jos käsittely todennäköisesti aiheuttaa yksilön oikeuksien ja vapauksien kannalta suuren riskin, rekisterinpitäjän on ennen käsittelytoimien aloittamista toteutettava tietosuojan vaikutustenarviointi ja määriteltävä toimenpiteet, joilla riskiä voidaan hallita. Arviointi on tehtävä yhteistyössä tietosuojavastaavien kanssa.