Liite 1. Tuusulan tietoturva- ja tietosuojapolitiikka

Käsitteet

Arkisto

Säilytettävien dokumenttien tai tallenteiden kokoelma tai paikka, jossa sitä on tarkoitus säilyttää.

Erityiset (arkaluontoiset) henkilötietoryhmät

Tietosuojalaissa termillä erityiset henkilötietoryhmät tarkoitetaan arkaluonteisia tietoja, joista ilmenee:

- rotu tai etninen alkuperä
- poliittinen mielipide
- uskonnollinen tai filosofinen vakaumus
- ammattiliiton jäsenyys
- terveydentila
- seksuaalinen käyttäytyminen ja suuntautuminen
- geneettinen tai biometrinen informaatio, josta henkilön voi tunnistaa.

Henkilöstöturvallisuus

Henkilöstön luotettavuuteen ja soveltuvuuteen, oikeuksien hallintaan, sijaisjärjestelyihin, henkilöstön suojaamiseen ja työsuhteen sekä työyhdistelmien järjestelyihin liittyvien turvallisuustekijöiden toteuttaminen. Henkilöstöturvallisuuteen kiinnitetään huomiota työsuhteen kaikissa vaiheissa.

Henkilörekisteri

Käyttötarkoituksensa vuoksi yhteenkuuluvista merkinnöistä muodostuva henkilötietoja sisältävä tietojoukko, jota käsitellään osin tai kokonaan tietojärjestelmällä tai joka on teknisesti järjestetty niin, että tiettyä henkilöä koskevat tiedot voidaan löytää helposti ja ilman kohtuuttomia kustannuksia.

Henkilötietojen tietoturvaloukkaus

Henkilötietojen tietoturvaloukkauksella tarkoitetaan tapahtumaa, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu, henkilötietoja luovutetaan luvattomasti tai niihin pääsee käsiksi taho, jolla ei ole käsittelyoikeutta.

Henkilötietojen tietoturvaloukkauksia voivat olla esimerkiksi:

- hävinnyt tiedonsiirtoväline, kuten USB-tikku
- varastettu tietokone
- hakkerointi

- haittaohjelmatartunta
- kyberhyökkäys
- tulipalo datakeskuksessa
- tiliotteen postitus väärälle henkilölle.

Tietoturvaloukkauksesta voi seurata esimerkiksi henkilötietojen valvomiskyvyn menettäminen, identiteettivarkaus tai petos, maineen vahingoittuminen tai pseudonymisoitujen tai salassapitovelvollisuuden alaisten henkilötietojen paljastuminen.

Henkilötieto

Henkilötietoja ovat sellaiset tiedot, joiden perusteella henkilö voidaan tunnistaa suoraan tai välillisesti esimerkiksi yhdistämällä yksittäinen tieto johonkin toiseen tietoon, joka mahdollistaa tunnistamisen. Henkilö voidaan tunnistaa esimerkiksi nimen, henkilötunnuksen tai jonkin hänelle tunnusomaisen tekijän perusteella. Henkilötietoja ovat nimen ja henkilötunnuksen lisäksi esimerkiksi kotiosoite, henkilökortin numero, auton rekisterinumero, potilastiedot tai IP-osoite.

Hyvä tiedonhallintatapa

Huolehtiminen asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen asianmukaisesta saatavuudesta, käytettävyydestä, suojaamisesta, eheydestä ja muista tietojen laatuun vaikuttavista tekijöistä. Julkisuuslain mukaan hyvään tiedonhallintatapaan sisältyy diaarin ja rekisteriselosteiden huolellinen ylläpito, asia-kirjajulkisuuden vaatimat järjestelyt, asianmukainen tietosuoja ja tietoturvallisuus, henkilökunnan koulutus ja informointi näistä seikoista, niitä koskevien ohjeiden noudattamisen valvonta, sekä varautuminen suunniteltujen hallintouudistusten vaikutuksiin asiakirjain julkisuuteen, salassapitoon ja suojaan sekä tietojen laatuun.

Jatkuvuuden hallinta

Organisaation prosessi, jolla tunnistetaan toiminnan uhat ja arvioidaan niiden vaikutukset organisaatiossa ja sen toimijaverkostossa sekä luodaan toimintatapa vakavien häiriötilanteiden hallinnalle.

Jatkuvuussuunnittelu

Varautuminen toiminnan häiriöihin ja keskeytyksiin niin, että toimintaa voidaan jatkaa ja häiriöiden haittavaikutuksia rajoittaa. Jatkuvuussuunnittelu on jatkuva prosessi ja osa riskienhallintaa. Työnä jatkuvuussuunnittelu on kriittisen toiminnon (esim. palvelun tai toiminnon omistajan) vastuulla olevaa työtä. Jatkuvuussuunnittelun tuotoksena syntyy kriittisten ja tärkeimpien toimintaprosessien jatkuvuus-suunnitelma, jossa kuvataan toimintojen ja niitä mahdollistavan tietojenkäsittelyn ja tiedonsiirron turvaaminen niin, että ne voivat jatkua kriisien, katastrofien, onnettomuuksien, toimintaolosuhteiden merkittävien muutosten ja häiriöiden aikana sekä niiden jälkeen. Kaikki ne toimenpiteet, jotka tulee tehdä kriittisen toimintaprosessin jatkuvuuden turvaamiseksi.

Järjestelmän omistaja

Nimetty taho, jolla on valta tai valtuudet sekä vastuu päättää järjestelmästä.

Käyttäjätunnus

Tunnistamista varten annettu käyttäjätilin yksilöivä tunniste.

Käyttöturvallisuus

Sisältää kunnan päivittäisten toimintojen ja rutiinien turvaamiseksi tehtävät suojaustoimenpiteet, kuten salasanojen hallinnoinnin ja tietojärjestelmien valvonnan.

Laitteistoturvallisuus

Laitteistojen käytettävyyden, toiminnan, ylläpidon sekä laitteiden ja tarvikkeiden saatavuuden turvaavat toimenpiteet. Laitteiston elinkaarta turvataan laitteistoturvallisuudella, johon kuuluvat asennuksen, takuun ja ylläpidon lisäksi erilaiset tukipalvelut ja -sopimukset sekä laitteiston turvallinen poisto elinkaaren lopussa.

Luottamuksellisuus

Tietojen säilyminen luottamuksellisina (ettei kukaan sivullinen saa tietoa) ja tietoihin, tietojenkäsittelyyn ja tietoliikenteeseen kohdistuvien oikeuksien säilyminen vaarantumiselta ja loukkaukselta.

Ohjelmistoturvallisuus

Käyttöjärjestelmiin, varus- ja työkaluohjelmistoihin sekä muihin ohjelmistoihin kohdistuvat turvatoimet. Näitä ovat esim. ohjelmistojen tunnistamis-, eristämis-, pääsynvalvonta- ja varmistusmenettelyt, tarkkailu- ja paljastustoimet, lokimenettelyt ja laadunvarmistus.

Oikeellisuus

Virheettömyys, yhtäpitävyys todellisen asiaintilan kanssa.

Rekisterinpitäjä

Rekisterinpitäjällä tarkoitetaan yhtä tai useampaa henkilöä, yhteisöä. laitosta tai säätiötä, jonka käyttöä varten henkilörekisteri perustetaan ja jolla on oikeus määrätä sen käytöstä, tai jonka tehtäväksi rekisterinpito on lailla säädetty.

Riski

Todennäköisyys, että uhka toteutuu aiheuttaen tietyn menetyksen tai vahingon. Uhkaan liittyvän vahingon rahallinen arvo tai odotusarvo.

Riski voi olla myös mahdollisuus menettää päämääräksi asetettu seikka.

Riskienhallinta

Järjestelmällinen toiminta riskien rajoittamiseksi niin, että ne ovat optimisuhteessa riskien rajoittamisen kustannuksiin samalla kun organisaation toiminnalle asetetut tavoitteet voidaan saavuttaa. Riskien hallinta on jokaisen hallinnon tehtävää suorittavan henkilön vastuulla. Erikseen

organisoitu riskienhallintatoiminto tukee hallinnon johtamista. Riskienhallinnan vaiheita ovat riskianalyysi, riskienhallintamenetelmän valinta, päätös riskien poistamisesta, alentamisesta tai pitämisestä omalla vastuulla, sekä riskienhallinnan organisointi.

Salassa pidettävä tieto

Laissa salassa pidettäväksi säädetty asiakirja tai tieto. Suomessa salassapitoa koskevia säädöksiä on muun muassa julkisuuslain 22 ja 24 §:ssä.

Salaus

Tiedon, esimerkiksi toiselle henkilölle lähetettävän viestin käsittely niin, että ulkopuolinen ei saisi haltuunsa tietoa, viestiä tai sen sisältämää informaatiota. Salakirjoittaa: Käyttää menetelmää tiedon esityksen muuttamiseksi sellaiseksi, että tiedon alkuperäinen sisältö on mahdollista saada selville vain samaa tai soveltuvaa käänteistä menetelmää käyttäen. Salakirjoittaminen tapahtuu salausavainta käyttäen tietyn salausalgoritmin mukaisesti.

Tietosuojan hallintamalli

Tietosuojan hallintamallilla tarkoitetaan niitä toimenpiteitä, joita organisaatiossa tehdään EU:n tietosuoja-asetuksesta tulevan rekisterinpitäjän osoitusvelvollisuuden todentamiseksi. Esimerkiksi tietosuojavastaavan nimeäminen, tietosuojatyöhön liittyvien vastuiden jakaminen, tietosuojatyön dokumentoiminen ja henkilöstön kouluttaminen ovat osa tietosuojan hallintamallia.

Tietoturvapoikkeama

Haitallinen tapahtuma, tahallinen tai tahaton tapahtuma tai olotila, jonka seurauksena kunnan vastuulla olevien tietojen ja palvelujen eheys, luottamuksellisuus tai tarkoituksenmukainen käytettävyystaso on tai saattaa olla vaarantunut.

Toipumissuunnittelu

Toipumissuunnitelman laatimiseksi ja ylläpitämiseksi tehtävät toimenpiteet. Toipumissuunnitelma on jatkuvuussuunnitelman tai varautumissuunnitelman osa, joka sisältää ohjeet katastrofista toipumiseen, toiminnan jatkamisesta ja paluusta normaaliin toimintaan. Määrittelee tärkeille tietojärjestelmille varajärjestelyvaatimukset, vastuut ja toimet valmiuden luomiseksi sekä antaa ohjeet toiminnasta poikkeustilanteissa. Suunnitelma ei sisällä vain vaatimuksia vaan konkreettisia sovittuja toimenpiteitä / menettelytapoja / teknisiä vararatkaisuja.

Valvontaviranomainen

Valvontaviranomaisella tarkoitetaan EU:n tietosuoja-asetuksessa säädettyä kansallista valvontaviranomaista, joka valvoo henkilötietojen käsittelyn lainmukaisuutta ja ihmisten tietosuojaoikeuksien toteutumista. Suomessa valvontaviranomaisen tehtävistä vastaa Tietosuojavaltuutetun toimisto.

Varautuminen

Toiminta, jonka tarkoituksena on luoda ja ylläpitää kunnan riittävä valmius oman toiminnan jatkumiseen normaaliolojen vakavien häiriötilanteiden ja poikkeusolojen varalta. Varautuminen käsittää suunnittelun sekä tarvittavat etukäteisvalmistelut.

Verkkourkinta

Käyttäjän manipuloinnin muoto, jossa pyritään sähköpostin tai WWW-sivun välityksellä saamaan luottamuksellista tietoa.