Virtain kaupungin tietoturva- ja tietosuojapolitiikka

Kaupunginhallitus 10.12.2018

Sisällysluettelo

Liitteet

1. TIETOTURVA- JA TIETOSUOJAPOLITIIKAN LÄHTÖKOHDAT

Tietoturva- ja tietosuojapolitiikka velvoittaa Virtain kaupungin henkilöstöä, johtoa, luottamushenkilöitä, viranhaltijoita sekä muita kaupungin tietoja käsitteleviä henkilöitä, kuten konsultteja, alihankkijoita, sidosryhmiä riippumatta siitä, missä muodossa käsiteltävä tieto on. Se tulee huomioida myös kaupungin käyttämien palvelutuottajien ja sidosryhmien toiminnassa. Tämä tietoturva- ja tietosuojapolitiikka korvaa aikaisemman tietoturvapolitiikan, jonka kaupunginhallitus on hyväksynyt 7.12.2015 § 394.

Tietoturvallisuus ja tietosuoja perustuvat lainsäädäntöön, normiohjaukseen ja sopimuksiin. Virtain kaupungin tietoturva- ja tietosuojapolitiikka määrittelee ne ***periaatteet, vastuut, toimintatavat sekä seurannan ja valvonnan***, joita Virtain kaupungin toimintayksiköissä noudatetaan tietoturvan ja tietosuojan toteuttamisessa ja kehittämisessä. Tietoturva- ja tietosuojapolitiikka ***varmistaa yhdenmukaiset käytännöt tietoturvan ja tietosuojan toteuttamiseksi***. Tietoturva- ja tietosuojapolitiikan soveltaminen ei ole sidoksissa tiedon muotoon, käsittely- tai esitystapaan, ja sitä sovelletaan kaikkiin tiedon elinkaaren vaiheisiin. Tietoturva- ja tietosuojapolitiikkaa täydentävät tietoturva- ja tietosuojaperiaatteet sekä tarvittavat erilliset määräykset ja ohjeet.

Tietoturvalla tarkoitetaan tietojen saatavuuden, eheyden ja luottamuksellisuuden turvaamista. Tietoturva käsittää toimet, joilla suojataan tiedot ulkopuolisilta. Tietoturvaan kuuluu muun muassa tietoaineistojen, laitteistojen, ohjelmistojen, tietoliikenteen, tilojen ja toiminnan turvaaminen.

Tietosuojalla tarkoitetaan yksilön (rekisteröidyn) yksityisyyden suojaamista. Tietosuojalla turvataan rekisteröidyn oikeuksia, yksilön tietoja ja luottamusta. Sisäänrakennettu ja oletusarvoinen tietosuoja tarkoittaa sitä, että henkilötietojen suoja otetaan huomioon jo suunniteltaessa toimintaa, jossa käsitellään henkilötietoja.

Tietoturva- ja tietosuojaperiaatteilla ohjataan tietojen suojaamista. Tiedon suojaaminen on oleellinen osa kaupungin kokonaisturvaa ja päivittäistä toimintaa sekä tärkeä osa kaupungin toiminnan ja palveluiden laatua ja varmentamista. Tiedon suojaamisen käytänteet ovat edellytys uuden teknologian turvalliseen käyttämiseen.

Tietoturvalla suojataan Virtain kaupungissa säilytettäviä manuaalisia ja sähköisiä tietoja sekä organisaatioiden, kuntalaisten, rekisteröityjen ja henkilöstön oikeuksia. Tietosuoja kattaa myös vaitiolovelvollisuuden piiriin kuuluvan kirjallisen ja puhutun tiedon käsittelyn.

Virtain kaupunki toteuttaa sisäänrakennetun ja oletusarvoisen tietoturvan ja tietosuojan periaatteita. Tietoturva- ja tietosuojaperiaatteita noudatetaan kaikissa tietojen käsittelyn elinkaaren vaiheissa, ja tätä edistetään tuomalla tietoturva- ja tietosuojasuojaperiaatteet osaksi henkilöstön perehdytystä ja koulutusta. Teknisillä ja organisatorisilla ratkaisuilla varmistetaan, että oletusarvoisesti käsitellään vain käsittelyn kannalta tarpeellisia tietoja.

Turvallisuudesta huolehditaan tiedon kaikissa olomuodoissa, tiedon koko elinkaaren ajan, mukaan lukien tietojen arkistointi ja suunniteltu hävittäminen. Tiedon elinkaarella tarkoitetaan kaikkia tiedon käsittelyn vaiheita alkaen tiedon keräämisestä tiedon hävittämiseen. Näiden väliin kuuluu esimerkiksi tietojen tallentaminen, järjestäminen, käyttö, siirtäminen, luovuttaminen, säilyttäminen, muuttaminen, yhdistäminen, suojaaminen, poistaminen ja tuhoaminen.

Käyttöoikeuksien ja järjestelmien käytön valvonnan vaatimukset niin tietoturvan kuin tietosuojankin osalta, otetaan huomioon mahdollisimman aikaisessa vaiheessa sovelluksia hankittaessa ja kehitettäessä. Tietoturva- ja tietosuojajärjestelyt pyritään toteuttamaan siten, että turvallisuusloukkausten selvittäminen jälkikäteen on kohtuudella mahdollista.

Tietoturva- ja tietosuojapolitiikka on voimassa toistaiseksi. Asiasisältöä tarkistetaan ja päivitetään tarvittaessa.

2. TIETOTURVA JA TIETOTURVAPERIAATTEET

Tietoturvalla varmistetaan tietojen luottamuksellisuus, eheys, saatavuus ja käytettävyys ja tätä kautta kunnan palvelutuotannon, prosessien ja muiden toimintojen luotettavuus, laatu sekä jatkuvuus. Lähtökohtana tietoturvaa koskevissa päätöksissä ovat viranomaissäädökset sekä hyvä tiedonhallintatapa, että hyvä tiedon käsittelytapa. Tietoturvallisuudesta huolehtiminen on edellytys tietosuojaperiaatteiden toteutumiselle.

Tietoturvaan kuuluvat tietoturvaorganisaatio, tietojenkäsittelijöiden toimintatavat, tietojen turvaamisen menetelmät, välineet ja toimenpiteet, työhön osoitetut resurssit sekä välineistön ja tilojen tietoturvaominaisuudet. Hyväksytyn tietoturva- ja tietosuojapolitiikan mukainen tietoturva tulee sisällyttää luonnollisena osana kaikkeen toimintaan. Tietoturvan kehittäminen ja ylläpito ovat osa toimintayksikön yleistä turvallisuustoimintaa, riskien hallintaa ja sisäistä valvontaa.

Tietoturvatyö on tietoturvan saavuttamiseksi tehtävien toimenpiteiden suunnittelua ja toteuttamista. Tietoturvatyön päämäärä on turvata toimintayksikön toiminnalle tärkeiden tietojärjestelmien ja tietoverkkojen keskeytymätön toiminta, estää tietojen ja tietojärjestelmien joutuminen ulkopuolisille sekä estää niiden valtuudeton käyttö, tahaton tai tahallinen tiedon tuhoutuminen tai vääristyminen sekä minimoida aiheutuvat vahingot. Normaaliajan toiminnan tietojenkäsittelyn turvaamisen lisäksi varaudutaan toiminnan keskeyttäviin uhkatilanteisiin ja niistä toipumiseen.

Tietoturvaperiaatteet

- Tietoturva ja tietosuoja ovat Suomen lainsäädännön mukaisesti osa organisaatiomme päivittäistä toimintaa ja koskevat koko toimintaa ja henkilöstöä.
- Asiat pitää tehdä tietoturvallisesti, jolla tarkoitetaan tiedon suojaamista monenlaisilta uhkilta tarkoituksena varmistaa toiminnan jatkuvuus, minimoida toiminnalliset riskit sekä maksimoida toiminnan ja investointien tulos.
- Tietoturva- ja tietosuoja-asiat huomioidaan välineriippumattomasti.
- Paperiset asiakirjat, sähköiset tietovarannot, tietoverkot, tietotekniset laitteet, tietojärjestelmät ja niihin liittyvät palvelut on suojattava sekä normaalioloissa että poikkeusoloissa.
- Tietoturvallisuuden saavuttamiseksi pitää toteuttaa turvamekanismeja, jotka muodostuvat toimintaperiaatteista, prosesseista, organisaatiorakenteista sekä ohjelmisto- ja laitteistotoiminnoista.
- Luottamukselliset, arkaluonteiset ja muut salassa pidettävät asiat kuuluvat vaitiolovelvollisuuden piiriin riippumatta siitä, miten tai mihin niitä on tallennettu tai millä tavalla tiedot on saatu.
- Esimiehen on varmistettava, että tietoturvamääräykset ja ohjeet koulutetaan tai perehdytetään henkilöstölle.
- Tietoturvaan liittyvä ohjaus, valvonta ja seuranta pitää organisoida.

Tietoturvallinen toiminta on tietojen käyttäjien toiminnasta riippuvaista. Tietoturvallisuuden perustana on osaava ja tietoturvaan sitoutunut henkilöstö. Tietojen valtuudeton ja oikeudeton käyttö estetään hyvällä tietojen käsittelyn suunnittelulla sekä ajantasaisella ohjeistuksella, jota henkilöstö noudattaa. Virtain kaupunki velvoittaa jokaisen työntekijän hyväksymään Asiakirjojen, tietojen ja tietojärjestelmien käyttö- ja salassapitositoumuksen palvelussuhteen alkaessa.

3. TIETOSUOJA JA TIETOSUOJAPERIAATTEET

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.

Virtain kaupunki noudattaa asiakkaiden, kuntalaisten, kaupungin henkilöstön ja muiden sidosryhmien henkilötietojen keräämisessä ja käsittelyssä voimassa olevaa lainsäädäntöä. Toukokuusta 2018 lähtien EU:n yleinen tietosuoja-asetus velvoittaa suunnittelemaan ja osoittamaan, että henkilötietojen käsittelyssä noudatetaan lakia ja kaupungin ohjeita. Tietosuojalla turvataan henkilötietojen asianmukainen käsittely koko organisaation toiminnassa, varmistetaan tietojen oikeellisuus ja ennalta ehkäistään henkilötietojen käyttöön liittyviä loukkauksia.

Henkilötiedolla tarkoitetaan kaikenlaisia luonnollista henkilöä taikka hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi.

Rekisteröidyllä tarkoitetaan henkilöä, jonka henkilötietoja kerätään.

Rekisterinpitäjällä tarkoitetaan yhtä tai useampaa henkilöä, yhteisöä, laitosta tai säätiötä, jonka käyttöä varten henkilötietoa kerätään ja jolla on oikeus määrätä henkilötiedon käytöstä tai jonka tehtäväksi henkilötiedon käsittely on lailla säädetty. Kunnissa rekisterinpitäjänä on yleensä lautakunta.

Tietosuojan tavoitteet ja periaatteet

Virtain kaupungin lähtökohtana tietosuojassa on riskilähtöisyys. Virtain kaupunki rekisterinpitäjänä arvioi henkilötietojen käsittelyyn liittyvät riskit ja valitsee arvioidun riskitason mukaan tarvittavat hallintatoimenpiteet. Virtain kaupunki 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. Virtain kaupungin toiminnassa toteutetaan sisäänrakennetun ja oletusarvoisen tietosuojan periaatetta. Tietosuoja otetaan huomioon monipuolisesti perustoiminnan yhteydessä mm. johtamisessa, hankinnoissa, kehitystyössä sekä toimintaprosesseissa. Tietosuoja huomioidaan kaupungin ja eri osapuolten välisissä sopimuksissa. Sopimuksia tehdessä varmistetaan, että sopimusehdoissa varmistutaan tietosuojasäädöksien vaatimuksista. Hankinta- ja ulkoistussopimuksia tekevät vastaavat siitä, että tietoturvan ja tietosuojan taso vastaa myös ostopalveluissa määräyksiä ja ohjeita sekä voimassa olevia säännöksiä sopimuksen tekohetkellä sekä toimeksiannon aikana.

Virtain kaupungin 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
- henkilötietojen luovuttamisessa huomioidaan tietosuoja-asetuksen, julkisuuslain ja erityslainsäädännön vaatimukset

- varmistetaan tietosuojalainsäädännön vaatimusten toteutumisen koko käsiteltävien henkilötietojen elinkaaren ajan

Virtain kaupungin henkilörekisterit koostuvat tietoryhmistä. Rekisteröidyt henkilöt ja niiden tietoryhmä kuvataan kaupungin tietosuojaselosteissa. Tietosuojaselosteesta rekisteröity saa tiedon hänen tietoihinsa kohdistuvista toimista ja tämä tieto tulee olla rekisteröidyn saatavilla. Tietosuojaselosteet pääsääntöisesti julkaistaan Virtain kaupungin Internet-sivuilla ja hallinnoidaan asianhallintajärjestelmässä.

Virtain kaupunki haluaa toteuttaa sisäänrakennetun ja oletusarvoisen tietosuojan periaatetta ja sisällyttää tietosuojaperiaatteet ja -vaatimukset jo aikaisessa vaiheessa osaksi henkilötietojen käsittelyä. Näin varmistetaan, että käsittely vastaa tietosuoja-asetuksen vaatimuksia. Virtain kaupunki toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet ja menettelyt tietosuojan varmistamiseksi.

Edellä mainittujen toimenpiteiden avulla varmistetaan mm, että:

- oletusarvoisesti kerätään vain henkilötietoja, jotka ovat välttämättömiä käsittelytarkoituksen kannalta
- tietoja ei kerätä eikä säilytetä suurempia määriä eikä kauemmin kuin on välttämätöntä kyseiseen käsittelytarkoitukseen
- henkilötietoja ei oletusarvoisesti saateta rajoittamattoman henkilö määrän saataville
- taataan rekisteröityjen oikeuksien toteutuminen
- taataan henkilötietojen suoja tarvittavin tietoturvakeinoin

Virtain kaupunki voi rekisterinpitäjänä ulkoistaa valitsemansa osan henkilötietojen käsittelystä toimeksisaajalle, henkilötietojen käsittelijälle. Virtain kaupunki valitsee sopimuskumppanikseen vain sellaisia henkilötietojen käsittelijöitä, jotka noudattavat hyvää henkilötietojen käsittelytapaa asianmukaisten teknisten ja organisatoristen toimenpiteiden avulla sekä täyttävät tietosuoja-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.

Virtain kaupungin ja erikseen valitun henkilötietojen käsittelijän välille laaditaan sopimus, joka on kirjallinen. Tietosuoja-asetuksen mukaan sopimuksessa tulee määritellä henkilötietojen käsittelyn kohde, tarkoitus ja kesto sekä sopia käsiteltävät henkilötiedot. Sopimuksen sisältö vaatimuksineen tulee määritellä mahdollisimman tarkasti. Virtain kaupunki ohjeistaa ulkoistettua henkilötietojen käsittelijää kyseistä tarkoitusta varten tehdyllä ohjeistuksella. Samaa ohjeistusta sovelletaan myös kaupungin oman henkilöstön kohdalla.

4. TIETOTURVAN JA TIETOSUOJAN ORGANISOINTI JA VASTUUT

Virtain kaupungin tietoturvaa ja tietosuojaa johtaa ja valvoo **kaupunginhallitus**. Kaupunginjohtaja päättää toimintayksikön kokonaisturvallisuuden eri osa-alueiden kehittämistoiminnan tavoitteista, organisoinnista, resursseista ja toimintavaltuuksista sekä nimeää tietoturvavastaavan. Tietosuojavastaavan nimeää kaupunginhallitus.

Tietoturvavastaava vastaa toimintayksikön tietoturvatyön kokonaisuudesta toimintayksikön johdolta saamiensa resurssien ja toimintavaltuuksien puitteissa. Tietoturvavastaavan valtuudet ja velvollisuudet on määritelty erikseen. Hän vastaa myös tietoturva-asioista tiedottamisesta toimintayksikön ulkopuolelle ja toimintayksikössä yleisellä tasolla. Tietoturvavastaava vastaa toimintayksikön tietoturvallisuustason määrittelystä ja arvioinnista ja raportoinnista sekä muusta hallinnollisesta tietoturvasta. Hän vastaa tietoturvan kehittämissuunnitelmien tekemisestä, toteutuksen valvonnasta, tietoturvatietouden edistämisestä ja tietoturvallisesta toimintatavasta toimintayksikössä ja sen ostamissa palveluissa sekä raportoinnista johdolle.

Tietosuojavastaavan tehtävänä on toimia rekisterinpitäjän erityisasiantuntijana henkilötietojen hyvän käsittelytavan ja mahdollisimman korkeatasoinen tietosuojan saavuttamiseksi. Hänen tehtävänään on tukea henkilökuntaa tietosuoja-asioissa ja auttaa toteuttamaan rekisterinpitäjälle määrätyt Tietosuoja-asetuksen ja tietosuojalain mukaiset velvoitteet.

Toimintayksikön keskeisten toimintojen turvanäkemyksiä edustaa **tietoturvaryhmä**, jonka asettaa kaupunginjohtaja. Tietoturvaryhmälle on nimetty puheenjohtaja ja sihteeri. Ryhmän jäsenet vastaavat oman vastuualueensa tietoturvaprosessin asioiden valmistelusta. Tietoturvaryhmä käsittelee tietoturvan linjaukset ja ohjeet ennen kuin ne esitellään johdolle hyväksyttäväksi. Virtain kaupungin tietoturvaryhmään kuuluvat hallintojohtaja, tietohallintopäällikkö, tietosuojavastaava ja asianhallintasihteeri.

Tietosuojatyöryhmä koostuu tietoturvatyöryhmästä ja toimialojen yhteyshenkilöistä, jotka toimivat tietoturva- ja tietosuoja-asioiden yhteyshenkilönä oman toimialansa ja tietoturvatyöryhmän välillä. Toimialan osastopäällikkö nimeää jäsenen tietosuojatyöryhmään, joka raportoi tietosuojatyöryhmälle yksikön aikaansaannoksista ja tekemisistä.

Jokaisella tietojärjestelmällä on **omistajayksikkö ja vastuuhenkilö**. Tietojärjestelmän vastuuhenkilön (osastopäällikkö) velvollisuuksiin kuuluu tietojärjestelmän toimintaan, tietosuojaan ja turvallisuuteen asetettavien vaatimusten (esim. kriittisyyden, jatkuvuussuunnittelun ja varmuuskopiointimenettelyn) määrittely sekä käyttöoikeuksien myöntäminen) ja valvonta. Tietoturva- ja tietosuoja-asioiden ohjeistamisesta, tiedottamisesta ja valvonnasta omassa yksikössään vastaa **yksikön esimies**. Yksikön esimies vastaa myös tietosuojan toteutumisen valvonnasta, tiedon omistajien määrittämisestä johtamisjärjestelmän vastuiden mukaisesti, oman yksikkönsä tietosuojakoulutukseen osallistumisen huolehtimisesta ja vastaa, että yksiköllä on sen oman toiminnan erityisvaatimukset huomioiden tarkennetut tietosuojatavoitteet ja periaatteet.

Organisaatiossa jokainen toimintayksikön **työntekijä**, **tietoja käsittelevä**, **tietojärjestelmien** tai **tietoverkkojen ylläpitäjä ja käyttäjä** ovat omalta osaltaan vastuussa tietoturvan ja tietosuojan toteuttamisesta sekä tietoturva- ja tietosuojaohjeiden noudattamisesta. Jokainen henkilö on velvollinen tietoturvaan ja tietosuojaan liittyvien uhkien ja poikkeamien raportoimisesta esimiehelleen, tietoturvavastaavalle tai tietosuojavastaavalle.

5. TIETOTURVAN JA TIETOSUOJAN TOTEUTTAMINEN

Tietoturvan ja tietosuojan toteuttamisen perusta on tämä kaupunginhallituksen hyväksymä kirjallinen tietoturva- ja tietosuojapolitiikka, joka annetaan tiedoksi jokaiselle Virtain kaupungin työntekijälle.

Toimintayksikön tietoturva- ja tietosuojaperiaatteet perustuvat kansainvälisiin, kansallisiin, yleisiin ja toimialakohtaista tietoturvaa ja tietosuojaa, henkilörekistereitä, hyvää tiedonhallintatapaa ja tiedon laatua ohjaaviin, velvoittaviin säädöksiin, ohjeisiin ja standardeihin. Lainsäädännön ja ohjeistuksen muutokset otetaan huomioon toimintayksikön tietoturvan ja tietosuojan kehittämisessä.

Tietoturvan toteuttaminen ja ylläpito kuvataan yksityiskohtaisesti tietoturvaperiaatteissa. Tietoturvan toteutuksen tulee perustua niihin vaatimuksiin, joita toiminta ja palvelut sekä kunkin tiedon ja tietojärjestelmän turvallisuusluokka asettavat tietojenkäsittelyn varmuudelle, käytettävyydelle, salassapidolle, laadulle ja toiminnan jatkuvuudelle sekä toimintaan kohdistuvien riskien arvioinnille.

Tietoturvan tavoitteiden saavuttaminen on jatkuva prosessi, joka tapahtuu hallinnollisten ja teknisten ratkaisujen avulla. Ne kuvataan tietoturvasuunnitelmassa ja tarvittaessa käyttöympäristöille ja yksiköille laadituissa erillisissä tietoturvan kehittämissuunnitelmissa.

Käyttäjien toimintaa ohjataan tietoturvasuunnitelmaan sisältyvillä käyttösäännöillä sekä vahvistetuilla ja saatavilla olevilla toimintaohjeilla sekä tietoturvakoulutuksella. Jokainen käyttäjä allekirjoittaa käyttäjän tietosuojaohjeen ja sitoumuksen saadessaan oikeuden tehtäviensä mukaiseen tietojärjestelmien ja tietoaineistojen käyttöön.

6. TIETOTURVAN JA TIETOSUOJAN SEURANTA JA VALVONTA

Virtain kaupungin työntekijöiden, tietojärjestelmien käyttäjien ja ylläpitäjien tulee ilmoittaa havaitsemastaan tietoturvan tai tietosuojan puutteesta, tietoturvaan tai tietosuojaan liittyvästä väärinkäytöksestä tai epäilemästään tietoturva- ja tietosuojarikkomuksesta esimiehelleen, tietoturvavastaavalle tai tietosuojavastaavalle.

Yksikön esimiehen tehtävänä on valvoa tietoturvan ja tietosuojan toteutumista omassa yksikössään. Tietoturvavastaavan tehtävänä on seurata ja valvoa Virtain kaupungin tietojärjestelmien tietoturvan toteutumista ja ryhtyä toimenpiteisiin havaittujen tietoturvan heikkouksien korjaamiseksi.

7. TIETOTURVA- JA TIETOSUOJAKOULUTUS JA OHJEISTUS

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

Liite 1. Lakiluettelo

Tietosuojaan liittyvää lainsäädäntöä

Perustuslaki (731/1999)
Kuntalaki (410/2015)
Hallintolaki (434/2003)
Arkistolaki (831/1994)
Asetus viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999)
Laki viranomaisen toiminnan julkisuudesta (621/1999)
Henkilötietolaki (523/1999)
Euroopan unionin yleinen tietosuoja-asetus luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (EU 679/2016)
Euroopan parlamentin ja neuvoston direktiivi, luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta (EU 680/2016)
Laki yksityisyyden suojasta työelämässä (759/2004)
Laki kunnallisesta viranhaltijasta (304/2003)
Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista (617/2009)
Laki väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista (661/2009)
Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004)
Laki julkisista hankinnoista ja käyttöoikeussopimuksista (1397/2016)
Rikoslaki (39/1889)
Työsopimuslaki (55/2001)
Valmiuslaki (1552/2011)
Tietoyhteiskuntakaari (917/2014)
Tekijänoikeuslaki (404/1961)

Lukiolaki (629/1998)
Perusopetuslaki (628/1998)
Oppilas- ja opiskelijahuoltolaki (1287/2013)

Kansanterveyslaki (66/1972)
Laki potilaan asemasta ja oikeuksista (785/1992)
Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista (812/2000)
Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007)
Laki sosiaali- ja terveydenhuollon palvelusetelistä (569/2009)
Laki sähköisestä lääkemääräyksestä (61/2007)
Laki terveydenhuollon ammattihenkilöstä (559/1994)
Sosiaalihuoltolaki (1301/2014), sosiaalihuoltolain (710/1982) 2 luku, 25, 26, 26 a, 27 d, 27 e ja 40 § sekä 5 ja 8 luku jäävät voimaan
Sosiaali- ja terveysministeriön asetus potilasasiakirjoista (298/2009)
Terveydenhuoltolaki (1326/2010)

Liite 2. Keskeiset käsitteet

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

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

Tietosuojapolitiikka
Johdon hyväksymä näkemys tietosuojan päämääristä, periaatteista ja toteutuksesta.

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.

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

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

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.

Tietosuojavastaava
Tietosuoja-asetuksen määrittelemä rooli, jonka rekisterinpitäjän ja henkilötiedon käsittelijän on nimettävä määritellyissä tilanteissa:

- jos tietojenkäsittelyä suorittaa viranomainen tai julkishallinnon elin (muu kuin tuomioistuin),
- ydintehtävät muodostuvat käsittelytoimista, jotka edellyttävät rekisteröityjen säännöllistä ja järjestelmällistä seurantaa laajassa mitassa, tai
- ydintehtävät muodostuvat käsittelytoimista, jotka kohdistuvat henkilötietojen erityisiin tietoryhmiin, rikostuomioihin tai rikoksia koskeviin tietoihin.

Asetus määrittelee myös tietosuojavastaavan aseman ja toimenkuvan.

Hallinnollinen sakko
Valvontaviranomainen voi määrätä rekisterinpitäjälle tai henkilötietojen käsittelijälle sakon tietosuoja-asetuksen vaatimusten laiminlyönnistä. Sakon suuruus määräytyy rikkomuksen luonteen perusteella. Sakon enimmäismäärä on 20 milj. € tai 4% yrityksen edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta.

Hallinnolliset seuraamukset
Valvontaviranomaisen määräämät seuraamukset koskien tietosuoja-asetuksen vaatimusten laiminlyöntejä.

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

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.

Rekisteriseloste, tietosuojaseloste
Dokumentti, joka rekisterinpitäjän tulee laatia ja pitää yleisesti saatavilla. Sen tulee kuvata henkilötietojen käsittely tiiviisti esitetyssä, avoimessa ja helposti ymmärrettävässä muodossa.

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 (accountability) toteuttamisessa.

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.

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

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 henkilö määrän saataville taataan rekisteröityjen oikeuksien toteutuminen
- Tietosuoja-asetuksen vaatimusten toteutuminen tulee taata määrittelyvaiheesta aina koko käsiteltävien henkilötietojen elinkaaren loppuun.