TIETOSUOJAPOLITIIKKA

Turun kaupunki

Konsernihallinto
Tietosuojavastaava
7.1.2019

Sisällysluettelo

1. Johdanto

Tietosuojapolitiikka määrittää ne periaatteet, toimintatavat, vastuut, valvonnan ja seuraamusjärjestelmän, joita noudatetaan Turun kaupungin tietosuojan toteuttamisessa ja kehittämisessä. Tämä tietosuojapolitiikka koskee henkilötietojen käsittelyä, jossa Turun kaupunki, sen organisaatioyksikkö, lautakunta tai muu taho toimii rekisterinpitäjänä.

Turun kaupungin palveluiden perustana ovat kaupungin asukkaiden tarpeet. Palveluiden tuottaminen perustuu tietoon ja sen käsittelyyn organisaation ja sen konsernin toimintaympäristöissä. Kaupungin palvelutuotanto on riippuvainen ICT-teknologiasta ja -palveluiden keskeytyksettömästä ja turvallisesta toiminnasta. Organisaation toiminta kriisitilanteissa perustuu lakisääteiseen valmiussuunnitteluun. Henkilötietojen käsittelyn suunnittelussa ja ohjaamisessa tulee varautua niin pieneen, keskisuureen, kuin suureen toimintahäiriöön sekä soveltuvin osin poikkeusoloihin. Erityisesti huolellista ennakkovalmistelua edellyttävät tilanteet, joissa henkilötietojen käsittelyä ohjataan sopimuksilla.

Tietoturvallisuus ja tietosuoja on huomioitava kaikessa tietojen käsittelyssä jo suunnitteluvaiheessa. Turun kaupungin johto tietosuoja- ja tietoturvaturvatoiminnan omistajana määrittelee tässä politiikassa johtamiseen, palveluihin ja toimintoihin liittyvät tietosuojaperiaatteet, vastuut ja tavoitteet. Politiikka toimii perustana organisaation tietosuojaa koskeville toimintaohjeille, joiden tehtävänä on tarkentaa politiikassa annettuja määräyksiä ja ohjeistaa niiden soveltamista käytäntöön. Tietoturvatoiminnan periaatteet on määritelty kaupungin riskienhallinnan ja sisäisen valvonnan ohjeessa.

Tietosuojapolitiikka koskee koko Turun kaupungin organisaatiota ja sen henkilöstöä mukaan lukien konsernin sekä niitä organisaation sidosryhmien edustajia, jotka toimeksiantojensa puitteissa käsittelevät Turun kaupungin omistamaa tai hallinnoimaa tietoa. Politiikka kattaa kaupungin omistaman tiedon riippumatta sen esitystavasta, muodosta, suojaustasosta tai elinkaaren vaiheesta.

Tässä dokumentissa rekisterinpitäjällä tarkoitetaan Turun kaupunkia tai sen organisaatioyksikköä, lautakuntaa tai muuta tahoa, joka toimii rekisterinpitäjänä Turun kaupungin omistamalle tai hallinnoimalle henkilörekisterille.

2. Tietosuojan määritelmä

Oikeus henkilötietojen suojaan on jokaiselle kuuluva perusoikeus. 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.

Tietoturva tarkoittaa tietosuojan kannalta teknisiä ja hallinnollisia toimenpiteitä, joilla tietosuojaa tuetaan. Tietoturvallisuudella tarkoitetaan sitä, että tieto on eheää, luottamuksellista sekä saatavilla.

Eheys: Tieto ei muutu ilman asianmukaisin valtuuksin tehtyjä toimenpiteitä.
Luottamuksellisuus: Tietoa voivat käsitellä vain kyseisen tiedon käsittelyyn oikeutetut tahot.
Saatavuus: Tieto on (oikeutettujen tahojen) saatavilla silloin kuin sitä tarvitaan.

3. Tietosuojan tavoitteet ja periaatteet

Turun kaupungin lähtökohtana tietosuojassa on riskilähtöisyys. Kaupunki tai sen alainen organisaatioyksikkö rekisterinpitäjänä arvioi henkilötietojen käsittelyyn liittyvät riskit ja valitsee arvioidun riskitason mukaan tarvittavat hallintatoimenpiteet. Tietosuojariskien hallinta on osa Turun kaupungin riskienhallintaprosessia, jolloin erityisesti merkittävän tason riskit raportoidaan johdolle saakka. Riskilähtöisyys ohjaa organisaation henkilötietojen käsittelyä ja on erittäin tärkeä osa rekisterinpitäjän osoitusvelvollisuuden toteuttamista.

Turun kaupunki toteuttaa riskilähtöisen toimintaperiaatteen varmistamiseksi tietosuojan vaikutustenarviointeja sellaisten henkilötietojen käsittelytoimille, joiden kohdalla 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 EU:n yleisen tietosuoja-asetuksen vaatimusten toteutuminen.

Turun kaupungin 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.

Turun kaupungin tavoitteena on huolehtia EU:n 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.

4. Tietosuojan organisointi ja vastuut

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

Turun kaupungille on nimetty tietosuojavastaava. Kaupunginjohtaja päättää rekisterinpidon ja tietosuojan kokonaisuudesta antamalla tietosuojaa ja rekisterinpitoa koskevat periaateohjeet. Tietosuojan toteutumista ja kehittämistä kaupungin organisaatiossa valvoo ja koordinoi tietoturvan kehittämisryhmä. Toimialojen, palvelukeskusten ja muiden organisaatioyksiköiden omat tietoturvaryhmät vastaavat kaupungin tasoisten tietosuojalinjausten toteuttamisesta omissa yksiköissään. Tietoturvan kehittämisryhmä ylläpitää tietosuojan ja tietoturvan kehittämissuunnitelmaa, valmistelee tietosuojaan liittyvää ohjeistusta, tiedottaa tietosuojatyöhön liittyvistä hankkeista ja muutoksista sekä vie tietosuojatyön osaksi organisaation operatiivista toimintaa.

Turun kaupungin tietosuojavastaava toimii tietosuojan erityisasiantuntijana, joka valvoo tietosuojalainsäädännön noudattamista organisaatiossa sekä vastaa neuvonnasta ja kouluttamisesta tietosuoja-asioissa. Tietosuojavastaava raportoi organisaation johdolle tietosuojan toteutumisesta. Tietosuojavastaavan asema organisaatiossa on riippumaton.

Henkilöstöhallinnolliset esimiehet vastaavat alaistensa toimintatavan tietosuojalainsäädännön mukaisuudesta organisaatiossa ja omassa yksikössä annettujen ohjeiden mukaisesti. Jokainen Turun kaupungin organisaatiossa tietoja käsittelevä, tietojärjestelmien ylläpitäjä ja käyttäjä on vastuussa tietosuojan toteuttamisesta omalta osaltaan.

Turun kaupungin rekisterihallinnon vastuut ja menettelytavat määritellään tarkemmin organisaaton rekisterihallinnosta annetussa ohjeessa.

5. Tietosuojan toteuttaminen

Turun kaupunki haluaa toteuttaa sisäänrakennetun ja oletusarvoisen tietosuojan periaatetta ja sisällyttää tietosuojaperiaatteet ja -vaatimukset jo aikaisessa vaiheessa osaksi henkilötietojen käsittelyä. Näin varmistetaan, että käsittely vastaa EU:n yleisen tietosuoja-asetuksen vaatimuksia.

Turun 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 henkilömäärän saataville,
- taataan rekisteröityjen oikeuksien toteutuminen sekä
- taataan henkilötietojen suoja tarvittavin tietoturvakeinoin.

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

Turun kaupungin järjestelmä- ja sovellus- sekä muissa kehitysprosesseissa on mukana työvaiheet, joissa analysoidaan henkilötietojen käyttötarkoituksiin sovellettavat tietosuojavaatimukset. Sovellettavat tietosuojavaatimukset vaihtelevat kerättävien henkilötietojen ja tietojen käyttötarkoituksen mukaan. 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.

Rekisterinpitäjä voi ulkoistaa valitsemansa osan henkilötietojen käsittelystä toimeksisaajalle, henkilötietojen käsittelijälle. 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.

Turun kaupungin ja erikseen valitun henkilötietojen käsittelijän välille laaditaan kirjallinen sopimus. Tietosuoja-asetuksen mukaan sopimuksessa tulee määritellä henkilötietojen käsittelyn kohde, tarkoitus ja kesto sekä sopia käsiteltävät henkilötiedot. Sopimuksen sisältö vaatimuksineen tulee määritellä mahdollisimman tarkasti.

Turun kaupunki ohjeistaa ulkoistettua henkilötietojen käsittelijää kyseistä tarkoitusta varten tehdyllä ohjeistuksella. Samaa ohjeistusta sovelletaan myös kaupungin oman henkilöstön kohdalla.

Rekisterinpitäjä sisällyttää tietosuojan myös projektinhallinta- ja kehittämismallinsa osaksi.

Turun kaupungissa on määritetty toimintaprosessi ja ohje liittyen toimintaan rekisteröityjen käyttäessä oikeuttaan saada pääsy henkilötietoihinsa. Prosessin mukaista toimintatapaa noudatetaan niissä tapauksissa, joissa rekisteröidyt haluavat saada nähtäväkseen omia rekistereissä olevia henkilötietojaan.

Turun kaupunki huolehtii henkilöstön riittävästä tietosuojaosaamisesta henkilöstökoulutuksien ja tiedottamisen kautta. Organisaatioon tulevat uudet työntekijät perehdytetään tietosuoja-asioihin järjestelmällisesti. Erityisesti tämä korostuu niissä tehtävissä, joissa käsitellään henkilötietoja ja toteutetaan rekisteröityjen oikeuksien toteuttamisprosesseja.

6. Toiminta tietosuoja- ja tietoturvapoikkeamatilanteissa sekä ilmoitusvelvollisuus

Turun kaupungin organisaatiossa on määritetty toimintaprosessi ja ohje liittyen toimintaan henkilötietoihin kohdistuvien tietoturvaloukkausten tapahtuessa. Prosessin mukaista toimintatapaa noudatetaan tietosuojapoikkeamien sattuessa.

Henkilötietojen tietoturvaloukkauksen sattuessa rekisterinpitäjällä on ilmoitusvelvollisuus valvontaviranomaisen sekä rekisteröidyn suuntaan. Valvontaviranomaiselle tehdään ilmoitus EU:n yleisen tietosuoja-asetuksen mukaisesti 72 tunnin kuluessa siitä, kun henkilötietojen tietoturvaloukkaus on tullut ilmi. Rekisteröidylle henkilötietojen tietoturvaloukkaus ilmoitetaan ilman aiheetonta viivytystä.

7. Rikkomukset ja seuraamukset

Jokainen Turun kaupungin tietojärjestelmien käyttäjä on sitoutunut noudattamaan organisaation tietosuoja- ja tietoturvaperiaatteita allekirjoittamalla tietosuoja- ja tietoturvaohjeen. Tietosuoja- ja tietoturvaohjeen sekä muiden ohjeiden, politiikkojen ja lainsäädännön vastainen toiminta käsitellään tapauskohtaisesti. Tietosuojarikkomusten mahdollisiin seuraamuksiin sovelletaan asiasta annettua ohjeistusta. Tietosuojarikkomukset raportoidaan organisaation johdolle ja tietosuojavastaavalle.

SEURAAMUKSET TIETOSUOJARIKKOMUKSISTA JA -RIKOKSISTA

Turun kaupungin tietosuojapolitiikka kuvaa periaatteet, toimintatavat, vastuut, valvonnan ja seuraamusjärjestelmän, joita noudatetaan Turun kaupungin tietosuojan toteuttamisessa ja kehittämisessä Tämä ohje täydentää tietosuojapolitiikkaa kuvaamalla mahdolliset seuraamukset tietosuojarikkomuksista ja -rikoksista. Dokumentissa on myös esimerkkejä mahdollisista tietosuojaan liittyvistä rikkomuksista.

TAULUKKO: MAHDOLLISET SEURAAMUKSET

TAHALLISUUDEN ASTE **RIKKOMUKSEN VAKAVUUS**	**Tietämättömyys, osaamattomuus, erehdys, vahinko, huolimattomuus** *Ei hyötymistarkoitusta*	**Piittaamattomuus, tahallisuus, toistuvuus** *Hyötymistarkoitus*
Vakava rikkomus **(esim. lain mukaan rikkomuksena tai rikoksena rangaistava teko)**	- puheeksi ottaminen ja opastus - suullinen huomautus - kirjallinen varoitus - tehdään rikosilmoitus	- tehdään rikosilmoitus - palvelussuhteen päättämismenettelyn käynnistys
Rikkomus **(vakava väärinkäyttö tai turvallisuuden rikkominen)**	- puheeksi ottaminen ja opastus - suullinen huomautus - kirjallinen varoitus	- kirjallinen varoitus - tehdään rikosilmoitus - palvelussuhteen päättämismenettelyn käynnistys
Lievä rikkomus **(asiaton toiminta tai väärinkäytös)**	- puheeksi ottaminen ja opastus - suullinen huomautus	- suullinen huomautus - kirjallinen varoitus - palvelussuhteen päättämismenettelyn käynnistys

ESIMERKKEJÄ RIKKOMUKSISTA

Vakava rikkomus **(esim. lain mukaan rikkomuksena tai rikoksena tuomittava teko)**

- Salassa pidettävien tietojen luvaton katselu, levittäminen ym. asiaton käsittely
- Tekijänoikeuden loukkaus tai rikoslain alaisen materiaalin oikeudeton käsittely
- Murtautuminen tietojärjestelmiin, tietoverkkoon tai muihin laitteisiin
- Tietojen luvaton muuttaminen, tuhoaminen, siirtäminen ja luovuttaminen
- Virusten ja muiden haittaohjelmien asentaminen tai levittäminen, palvelun tahallinen estäminen tai häirintä ym. vahingonteko

Rikkomus **(vakava väärinkäyttö tai turvallisuuden rikkominen)**

- Tunnuksen luovuttaminen, kuten salasanan kertominen toiselle käyttäjälle tai avoimen työaseman luovuttaminen niin, että toinen pääsee valvomatta käyttämään luovuttajan tunnusta
- Lukitsemattoman työaseman tai päätelaitteen jättäminen valvomatta
- Tiedon luottamuksellisuuden vaarantaminen, kuten salassa pidettävän tiedon lähettäminen suojaamattomassa sähköpostissa tai työsähköpostin automaattinen jatkolähetys ulkopuoliseen sähköpostiosoitteeseen
- Salasanan tai salassa pidettävien asiakirjojen jättäminen sivullisten saataville
- Ohjelmien asentaminen ilman työnantajan lupaa
- Ylläpito-oikeuksien luvaton hallussapito
- Työnantajan tarjoamien työvälineiden ja ohjelmien käyttö asiattomiin tarkoituksiin
- Luvattomien työvälineiden ja ohjelmien käyttö työtehtävien hoitamiseen
- Ohjeiden vastainen laitteistojen tai ohjelmien käyttö
- Laitteiden kytkeminen verkkoon luvattomasti
- Ohjelmien ja pelien luvaton kopiointi
- Henkilön päästäminen tilaan, johon hänellä ei ole oikeutettua pääsyä tai muu kulunvalvontaohjeiden rikkominen

Lievä rikkomus **(asiaton toiminta tai väärinkäytös)**

- Haitan tai kiusan aiheuttaminen, kuten laitteille tai ohjelmiin oikeutetun pääsyn tilapäinen estäminen
- Luvaton kaupallinen tai vastaava toiminta, kuten sähköpostin käyttäminen henkilökohtaiseen markkinointiin
- Vähäinen henkilökohtaisen tietosuojan tai tietoturvan laiminlyönti, kuten liian laaja sähköpostijakelu, päätelaitteen näytön puutteellinen suojaaminen, huolimaton tulostimen käyttö