Kemin kaupungin ja kaupunkikonsernin

Tietoturva- ja tietosuojapolitiikka

Tietosuoja- ja tietoturvatyöryhmä 10.12.2018

Hyväksytty: Kaupunginhallitus 17.12.2018 § 450

Sisällysluettelo

1. Johdanto

Tietoturvan ja tietosuojan on oltava osa koko organisaation jokapäiväistä toimintaa, jonka avulla tunnistetaan toiminnan kannalta elintärkeät palvelutehtävät ja määritellään sekä kuvataan näiden turvaamiseksi riittävät tietoturva- ja tietosuojaperiaatteet.

Kemin kaupungin palveluiden perustana ovat kuntalaisten tarpeet. Palveluiden tuottaminen perustuu tietoon ja sen käsittelyyn Kemin kaupungin ja sen konserniyhtiöiden toimintaympäristöissä. Tässä tietoturva- ja tietosuojapolitiikassa määritellään, miten Kemin kaupunki ja sen konserniyhtiöt keräävät, käyttävät ja käsittelevät erilaisia henkilötietoja ja varmistavat yksityisyyden suojan. Tietoturva- ja tietosuojapolitiikka määrittelee ne periaatteet, vastuut, velvoitteet, toimintatavat sekä seurannan ja valvonnan, joita konsernissa noudatetaan tietoturvan ja -suojan toteuttamisessa ja kehittämisessä. Tätä politiikkaa täydentävät yksityiskohtaisemmat ohjeet, jotka on koottu kaupungin intranet -sivuille.

Kaupungin ja konserniyhtiöiden rekisterit sisältävät kuntalaisiin, asiakkaisiin, työntekijöihin, sidosryhmiin, toimittajiin ja toimintaan liittyvää tietoa, joka on lainsäädännön perusteella suojattava. Tällä politiikalla vastataan EU:n tietosuoja-asetuksen ja siitä johdettavien kansallisten lakien ja määräysten vaatimuksiin sekä tietoturvan, tietosuojan, riskienarvioinnin, kokonaisarkkitehtuurin ja yhteentoimivuuden huomioimiseen suunnittelun aikaisessa vaiheessa, suunnittelun kautta saatavaan kustannustehokkuuteen, tietojen käytettävyyteen ja tietoturvallisuuden tilintekokykyisyyteen. EU:n tietosuoja-asetuksen ja siitä johdettavien kansallisten lakien lisäksi mm. sosiaali- ja terveyspalveluiden asiakastietoja koskevat omat erityislakinsa.

Kemin kaupunginhallituksen ja tytäryhtiöiden hallitusten hyväksymä tietoturva- ja tietosuojapolitiikka kattaa kaupungin ja konserniyhtiöiden kaikkeen toimintaan liittyvät tietojenkäsittelyn sekä henkilötietojen käsittelyyn liittyvät tehtävät. Jokaisen kaupungin ja konserniyhtiöiden työntekijän on tunnettava tämä politiikka ja noudatettava sen perusteella annettuja ohjeita.

Kaupungin ja konserniyhtiöiden ulkopuolisten toimijoiden, toimittajien ja muiden yhteistyökumppaneiden tulee myös sitoutua noudattamaan lainsäädäntöä, tätä tietoturva- ja tietosuojapolitiikkaa sekä tietoturvaa ja -suojaa koskevia ohjeita ehtona tehtäviensä mukaiselle pääsylle kaupungin ja konserniyhtiöiden tietojärjestelmiin ja tietoihin. Kaupungin tai konserniyhtiön toimiessa rekisterinpitäjänä edellytetään yhteistyökumppaneilta erillisen henkilötietojen käsittelyä koskevan sopimuksen allekirjoitusta. Kaupungin tai konserniyhtiön toimiessa henkilötietojen käsittelijänä solmitaan erillinen sopimus henkilötietojen käsittelystä rekisterinpitäjän kanssa.

2. Tavoitteet

Tietoturvan ja -suojan ensisijaisena tavoitteena on kaupungin vastuulla olevien palveluiden jatkuvuuden turvaaminen kaikissa olosuhteissa. Tietoturvan tavoitteena on suojata salassa pidettävää tai muutoin suojattavaa tietoa sekä normaali- että poikkeusoloissa hallinnollisten, fyysisten, henkilöstöpoliittisten ja tietoteknisten toimenpiteiden avulla. Suojattavan tiedon turvallisuus taataan huolimatta siitä missä muodossa sitä käsitellään, tallennetaan tai säilytetään. Tieto voi siis olla suullisessa, kirjallisessa, sähköisessä tai missä muodossa tahansa olevaa tietoa. Tietosuoja on oleellinen osa tietoturvallisuutta. Tietosuojan tavoitteena on estää henkilötietojen valtuudeton saanti ja säilyttää tietojen luottamuksellisuus ja siten turvata tiedon kohteen yksityisyys sekä oikeusturva.

Tavoitteena on, että kaupungin ja konserniyhtiöiden henkilöstö sekä luottamusmiehet ymmärtävät tietoturvan merkityksen ja noudattavat tietoturvaohjeita ja -määräyksiä. Toimivalla tietoturvakulttuurilla voidaan hallita Kemin kaupungin ja sen konserniyhtiöiden omistamaa tietoa lainsäädännön sille asettamien vaatimusten mukaisesti.

3. Toteutus

Tietoturvan ja -suojan toteuttamisen perusta on tämä politiikka ja siitä johdettavat ohjeet sekä periaatteet, joihin jokaisen Kemin kaupungin ja sen konserniyhtiöiden työntekijöiden on perehdyttävä.

Kemin kaupungin tietosuojan lähtökohtana on riskilähtöisyys. Kemin kaupunki ja sen konserniyhtiöt rekisterinpitäjinä arvioivat henkilötietojen käsittelyyn liittyvät riskit ja valitsevat arvioidun riskitason mukaan tarvittavat hallintatoimenpiteet. Tietosuojariskien merkittävät tasot raportoidaan johdolle.

Riskilähtöisyys ohjaa organisaation henkilötietojen käsittelyä ja on tärkeä osa rekisterinpitäjän osoitusvelvollisuuden toteuttamista. Kemi -konserni toteuttaa riskilähtöisen toimintaperiaatteen varmistamiseksi tietosuojan vaikutustenarviointeja, jos käsittelytoimiin liittyy yksilöiden oikeuksien ja vapauksien kannalta merkittäviä riskejä. Vaikutusten arvioinnin tuloksia käytetään hallintakeinojen määrittelemisessä. Samalla varmistetaan tietosuoja-asetuksen vaatimusten toteuttaminen.

Konsernin toiminnassa toteutetaan sisäänrakennetun ja oletusarvoisen tietoturvan ja -suojan periaatetta. Tietoturva ja -suoja otetaan huomioon mm. johtamisessa, hankinnoissa, kehitystyössä sekä toimintaprosesseissa.

Tietoturva- ja tietosuojaperiaatteet perustuvat EU:n tietosuoja-asetukseen ja kansalliseen lainsäädäntöön.

Tietoturvan ja -suojan toteuttamistapoina ovat organisaatioiden määrittelemät ja toteuttamat:

- Ohjeet ja periaatteet
- Koulutukset, perehdyttäminen sekä pääsynvalvonta niin tiloihin kuin järjestelmiin
- Tietoturva- ja tietosuojatietoisuutta lisätään henkilöstölle kohdistetuin nettitestein, itseopiskeluaineistojen ja videoiden avulla
- Tietoturva- ja tietosuojapoikkeaminen käsittelyohjeet

Tietoturvan ja -suojan toteuttaminen ja ylläpito kuvataan yksityiskohtaisesti erillisissä tietoturva- ja tietosuojaohjeissa, jotka tullaan päivittämään ja uudistamaan EU-tietosuoja-asetuksen ja lainsäädännön vaatimalle tasolle.

4. Organisointi ja vastuut

Tietoturva- ja tietosuojavastuut Kemin kaupungin ja konserniyhtiöiden organisaatioissa on kuvattu alla. Tietoturva- sekä tietosuojavastuut ja niiden jakautuminen Kemin kaupungin ja keskeisten sidosryhmien ja yhteistyökumppaneiden osalta tulee kuvata ja sopia kirjallisesti. Tästä vastaavat palveluista vastaavat henkilöt.

Kaupunginhallitus/konserniyhtiön hallitus hyväksyy tietoturva- ja tietosuojapolitiikan ja vastaa tarvittavien edellytysten luomisesta niiden toteuttamiseksi. Tietoturva ja -suoja ovat osa sisäistä valvontaa ja riskienhallintaa, joista **kaupunginjohtaja/toimitusjohtaja** on kokonaisvastuussa. Kaupunginjohtaja ottaa tietoturvaan ja -suojaan liittyvät tekijät huomioon päätöksenteossa, suunnittelussa ja seurannassa. Kaupunginjohtajan viranhaltijapäätöksellä nimettävä **johtoryhmä** toimii kaupunginjohtajan apuna myös tietoturva- ja tietosuoja-asioissa. Konserniyhtiöt voivat nimetä myös tietosuojavastaavat.

Tietosuojavastaava vastaa EU:n tietosuoja-asetuksen ja kansallisen tietosuojalainsäädännön täytäntöönpanosta ja soveltamisesta organisaatiossa. Neuvoo kaupunkiorganisaatiota kaikissa

tietosuojakysymyksissä sekä konsultoi tarvittaessa konserniyhtiöitä. Valvoo dokumentaation laatimista, saavutettavuutta ja säilyttämistä. Tukee ja antaa neuvoja tietosuojaa koskevasta vaikutustenarvioinnista ja valvoo sen toteuttamista. Apunaan hänellä on näihin tehtäviin kaupunginhallituksen nimeämä tietoturva- ja tietosuojatyöryhmä. Tietosuojavastaava toimii valvontaviranomaisen ja rekisteröityjen yhteyspisteenä. Seuraa rekisteröityjen oikeuksien toteuttamista ja rekisterinpitäjän velvollisuuksien toteuttamista. Toteuttaa riskiperusteista lähestymistapaa. Osallistuu rekisterinpitäjän osoittamisvelvollisuuden toteuttamiseen. Tehtävässään tietosuojavastaava on riippumaton ja raportoi suoraan ylimmälle johdolle. Tietosuojavastaavaa sitoo salassapitovelvollisuus.

Tietoturvapäällikkö vastaa tietoturvallisuuden ylläpidon, kehittämisen ja valvonnan prosessien, menettelytapojen ja turvamekanismien toteuttamisesta. Apunaan hänellä näihin tehtäviin on kaupunginhallituksen nimeämä tietoturva- ja tietosuojatyöryhmä. Tietoturvapäällikkö vastaa keskitettyjen tietoturvallisuuden kehittämishankkeiden valmistelusta ja toteutuksesta. Viestii tietoturva-asioista ja vastaa tietoturvapuutteiden ja -poikkeamien käsittelyn käynnistämisestä. Tehtäviin kuuluu osallistua tietoturvan periaatteiden määrittelyyn, avustaa johtoa ja yksiköitä tietoturvallisuuden toimeenpanossa sekä konsultoi tarvittaessa konserniyhtiöitä. Lisäksi valmistelee tietoturvastrategian, tietoturvallisuuden mittariston ja järjestää tietoturvallisuutta koskevan seurannan ja huolehtii riskianalyysin tekemisestä säännöllisesti. Tehtävässään tietoturvapäällikkö on riippumaton ja raportoi suoraan ylimmälle johdolle.

Tietoturva- ja tietosuojatyöryhmä valmistelee ja ohjaa tietoturvan ja tietosuojan käytännön toteutusta ja kehittämistoimenpiteitä sekä niihin liittyvää riskienhallintaa. Ryhmän tehtäviin kuuluu tietoturvaan ja tietosuojaan liittyvien suunnitelmien, määräysten ja ohjeiden valmistelu ja ylläpito. Tietoturva- ja tietosuojatyöryhmä vastaa tietoturva ja tietosuoja-asioiden tiedottamisesta asiakkaille, henkilöstölle ja muille sidosryhmille. Ryhmä vastaa koko konsernin henkilöstön kouluttamisesta.

Tietoturvapoikkeamien käsittelyryhmän tehtävänä on käsitellä tietoturvapoikkeamat ja käynnistää tarvittavat toimenpiteet niiden johdosta sekä konsultoi tarvittaessa konserniyhtiöitä.

Esimiehet vastaavat siitä, että heidän alaisillaan on riittävä osaaminen, mahdollisuus riittävään kouluttautumiseen ja että työntekijät ovat perehtyneet kaupungin/konserniyhtiön sisäiseen ohjeistukseen. Esimiesten tehtävänä on vastata myös siitä, että työntekijöillä on oikeudet vain tehtävän edellyttämässä laajuudessa tarvittaviin tietojärjestelmiin ja tietoihin. Esimiehet myös huolehtivat, että muutokset työtehtävissä huomioidaan käyttöoikeuksissa ja työsuhteen päättyessä käyttöoikeudet järjestelmistä poistetaan.

Henkilöstön ja luottamushenkilöiden tulee tuntea tietoturvasta ja tietosuojasta annetut ohjeet ja

noudattaa niitä ja osallistua heille suunnattuun koulutukseen sekä raportoida havaitsemistaan ongelmista ja uhkista tai menettelyvirheistä lähimmälle esimiehelleen, tietoturvapäällikölle, tietosuojavastaavalle tai tietoturvapoikkeamien käsittelyryhmälle. Jokainen tietoja käsittelevä työntekijä, tietojärjestelmien ja sovellusten ylläpitäjä ja käyttäjä on vastuussa tietoturvallisuuden sekä tietosuojan toteuttamisesta omalta osaltaan.

5. Seuranta ja valvonta

Tietoturva- ja tietosuojapolitiikan sekä ohjeiden noudattamisen valvonta on tärkeä osa organisaation sisäistä valvontaa ja tietosuojan osoitusvelvollisuuden toteuttamista. **Operatiivisesta seurannasta**, raportoinnista ja kehittämistoimista vastaavat tietoturvapäällikkö ja tietosuojavastaava.

Henkilöstön tietoturva- ja tietosuojaosaamista ylläpidetään ja lisätään tiedottein ja koulutuksin. Yksikön esimiesten tehtävänä on valvoa tietoturvallisuuden ja tietosuojan toteutumista omassa yksikössään.

Tietoturvaan ja tietosuojaan liittyvissä uhkatilanteissa esimiehellä on oikeus sulkea (tietoturvapäällikön ja/tai tietosuojavastaavan avustuksella) tiedossa oleva tietoliikenneyhteys, järjestelmä, tunnus tai laite. Asianosaisia on viipymättä informoitava tehdyistä toimenpiteistä ja mahdollisista jatkotoimista.

5.1 Tietoturvarikkomukset ja seuraamukset

Jokainen tietojenkäsittelyjärjestelmien käyttäjä on velvollinen noudattamaan hyväksyttyjä tietoturva- ja tietosuojaohjeita. Tietosuoja- ja tietoturvarikkomukset, tietoturvaloukkaukset ja väärinkäytökset raportoidaan johdolle ja jokaiseen tilanteeseen reagoidaan sen vaatimalla tavalla. Tarkoituksellinen laiminlyönti tai muuten vaarantava toiminta voi johtaa työsuhteen purkamiseen ja lainsäädännön rajoissa oikeudellisiin toimiin. Tietosuojalaissa säädetään **tietosuojarikoksen** rangaistavuudesta ja **vaitiolovelvollisuudesta** sekä kielletään tietoja käsitellessä saatujen tietojen hyväksikäyttö omaksi tai toisen eduksi tai toisen vahingoksi. Tietosuojalaissa viitataan myös rikoslain **tietomurtoja** koskevaan pykälään.

6. Liite 1 Käsitteet

Tietosuoja: Yksityisyyden suojaaminen henkilötietoja käsiteltäessä.

Tietoturva: Järjestelyt, joilla pyritään varmistamaan tiedon luottamuksellisuus, eheys ja saatavuus

Tietoturva- ja tietosuojapolitiikka: Kemin kaupungin ylimmän johdon hyväksymä asiakirja, jossa se määrittelee tietoturva- ja tietosuojapolitiikan tavoitteet, vastuut ja toteutuskeinot

EU:n tietosuoja-asetus/GDPR (General Data Protection Regulation): EU:n yleistä tietosuoja-asetusta sovelletaan 25.5.2018 alkaen kaikissa EU:n jäsenmaissa. Tietosuoja-asetusta sovelletaan lähtökohtaisesti kaikkeen henkilötietojen käsittelyyn.

Henkilötieto: Kaikki tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyvät tiedot kuten nimi, henkilötunnus, kotiosoite, sähköpostiosoite, kuva, IP-osoite, biometrinen tai geneettinen tieto

Rekisterinpitäjä: Luonnollinen tai oikeushenkilö, viranomainen, virasto tai muu elin, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot

Henkilötietojen käsittelijä: Luonnollinen tai oikeushenkilö, viranomainen tai muu elin, joka käsittelee henkilötietoja rekisterinpitäjän lukuun (toimeksiannosta) vain sovitussa käyttötarkoituksessa.

Henkilötietojen käsittely: Kaikki henkilötietoihin kohdistuvat toimet koko tiedon elinkaaren aikana tiedon suunnittelusta hävittämiseen tai arkistointiin.

Rekisteröity: Henkilö, jonka henkilötietoja käsitellään

Rekisteri: Henkilötietoja sisältävä tietojoukko, josta tiedot saatavilla tietyin perustein

Henkilötietojen tietoturvaloukkaus: Tapahtumaa, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu, henkilötietoja luovutetaan luvattomasti tai niihin pääsee käsiksi taho, jolla ei ole käsittelyoikeutta.

Osoitusvelvollisuus: Organisaatiolla on oltava kyky osoittaa noudattavansa tietosuoja-asetusta henkilötietoja käsiteltäessä sekä toteuttavansa tietosuojaperiaatteita myös käytännössä

Vaikutusten arviointi: Asetuksessa määritellyissä tilanteissa tehtävä riskiarvio ("Data Protection Impact Assesment, DPIA")

Kansallinen valvontaviranomainen: Tietosuojavaltuutettu (http://www.tietosuoja.fi)

7. Liite 2 Tietoturvaan ja tietosuojaan liittyviä ohjeita ja lakeja

- VM:n VAHTI ohjeet ja materiaalit https://vm.fi/vahti-materiaalit-ja-tilaisuudet
- Tietosuojavaltuutetun ohjeet, suositukset ja kannanotot https://tietosuoja.fi/etusivu
- EU:n yleinen tietosuoja-asetus EU 679/2016 https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=celex%3A32016R0679

https://www.finlex.fi/fi/

- Tietosuojalaki 1050/2018, voimaan 1.1.2019 alkaen
- Henkilötietolaki 523/1999 kumotaan Tietosuojalain voimaantulon yhteydessä
- Laki yksityisyyden suojasta työelämässä 759/2004: *Työntekijää koskevien henkilötietojen käsittely*
- Perustuslaki 731/1999
- Kuntalaki 410/2015
- Hallintolaki 434/2003
- Julkisuuslaki 621/1999 (Laki viranomaisen toiminnan julkisuudesta ja hyvästä tiedon hallintotavasta)
- Julkisuusasetus 1030/1999 (Asetus viranomaisen toiminnan julkisuudesta ja hyvästä tiedon hallintotavasta)
- Arkistolaki 831/1994: *Asiakirjallisten tietoaineistojen laatiminen, säilyttäminen ja hävittäminen*
- Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista 617/2009
- Laki sähköisestä asioinnista viranomaistoiminnassa 13/2003
- Laki sähköisen viestinnän palveluista 917/2014
- Laki valmiuslain muuttamisesta 198/2000
- Henkilötietojen käsittelyä koskevia erityissäännöksiä on lukuisissa eri toimialoja koskevissa erityislaeissa
- Osakeyhtiölaki 624/2006
- Hankinta- ja kilpailulainsäädäntö