Espoon kaupunki

Tietoturva- ja tietosuojapolitiikka

Tietoturva- ja tietosuojapolitiikan käsittely:

Tarkastettu	Tietoturvaryhmä	19.4.2018
Hyväksytty	Kaupunginhallitus	28.5.2018

Tietoturva- ja tietosuojapolitiikan muutokset:

Päiväys / Tekijä	**Kohta**	**Muutoksen kuvaus**
9.5.2018 / Matti Parviainen	Koko asiakirja	Koko asiakirja
9.5.2018 / Juho Nurmi	Koko asiakirja	Koko asiakirja

Sisällysluettelo

1 Johdanto 3
2 Tietoturvallisuus 3
3 Tietosuoja 4
4 Riskienhallinta 5
5 Varautuminen 5
6 Vaatimustenmukaisuus ja tavoitteet 5
7 Organisointi, roolit ja vastuut 6
8 Tiedon ja tietojärjestelmien käyttö 8
9 Tietoturva- ja tietosuojaosaaminen 8

1 Johdanto

Tieto on keskeisessä roolissa Espoon kaupungin toiminnassa ja palvelutuotannossa. Jotta tieto on tehokkaasti hyödynnettävissä, tiedon hallinta- ja käsittelykäytäntöjen tulee toimia asianmukaisesti kaikissa tilanteissa.

Espoon kaupungin johto määrittelee tässä politiikassa tietoturvallisuutta sekä tietosuojaa koskevat periaatteet ja linjaukset. Politiikka toimii perustana kaupungin tietoturvallisuutta ja tietosuojaa koskeville ohjeille, joiden tehtävänä on tarkentaa politiikkaa ja auttaa sen käytäntöön soveltamisessa.

Tämä politiikka koskee jokaista kaupungin työntekijää, viranhaltijaa, luottamushenkilöä ja sidosryhmän edustajaa, joka työnsä tai toimeksiantonsa puitteissa käsittelee Espoon kaupungin omistamaa tai hallinnoimaa tietoa.

Tätä politiikkaa sovelletaan kaikkeen tietoon ja muuhun dataan (myöh. tieto) riippumatta sen esitystavasta, muodosta, suojaustasosta, elinkaaren vaiheesta, esiintymisympäristöstä tai siirtotiestä.

2 Tietoturvallisuus

Espoon kaupungissa tietoturvallisuudella tarkoitetaan hallinnollisia, teknisiä ja muita keinoja, joilla suojataan kaupungin omistamaa tai hallinnoimaa tietoa sekä normaalitilanteissa, normaaliolojen häiriötilanteissa, että poikkeusoloissa. Tietoturvallisuus tulee huomioida mahdollisimman varhaisessa vaiheessa toiminnan suunnittelua.

Toteutuakseen tietoturvallisuus vaatii seuraavien, painoarvoltaan tapauskohtaisesti vaihtelevien asioiden, toteutumista:

- **Luottamuksellisuus:** Tieto on vain tietoon oikeutettujen käytettävissä.
- **Eheys:** Tietoa ei ole muutettu tahallisesti tai tahattomasti, eikä tieto ole muuttunut teknisen häiriön seurauksena.
- **Saatavuus:** Tieto, tietojärjestelmä tai palvelu on siihen oikeutettujen henkilöiden ja järjestelmien saatavilla ja käytettävissä silloin kun sitä tarvitaan.
- **Kiistämättömyys:** Tiedonkäsittelytoimenpiteet suoritetaan niin, että käsittelyn osapuolet voidaan yksiselitteisesti tunnistaa sekä toimenpiteiden aikana, että jälkikäteen.

Espoon kaupungissa tietoturvallisuutta toteutetaan tietoturvasuunnitelman pohjalta, tietoturvallisuuden hallintajärjestelmässä kuvattavilla, tietoturvallisuuden parantamiseen tähtäävillä johtamis- ja muilla käytännöillä. Keskeistä toteuttamisessa on, että kaupungilla on riittävät kyvykkyydet aktiivisesti:

- johtaa tietoturvallisuutta
- seurata toimintaympäristön tilaa
- havaita ja tunnistaa uhkat
- varautua poikkeamiin ja häiriöihin ennakolta sekä reagoida tilanteen edellyttämällä tavalla

Tietoturvallisuus Espoon kaupungissa sisältää tiedon suojaamisen lisäksi kyberturvallisuuteen, tietosuojaan ja muihin turvallisuuden osa-alueisiin liittyviä toteutuksia, joista kaupungin kannalta keskeisimpiä ovat:

- Toimenpiteet, joilla turvataan kybertoimintaympäristön[1] luottamuksellisuus, eheys, saatavuus ja jatkuvuus.
- Velvoittavien tietosuojasäädösten mukaiset toimenpiteet, joilla varmistetaan henkilön yksityisyyden suojan ja muiden sitä turvaavien oikeuksien toteutuminen henkilötietoja käsiteltäessä.
- Toimenpiteet, järjestelmät ja rakenteet, joiden avulla kaupungin tiloja, siellä olevia ihmisiä, tietoa ja muuta omaisuutta suojataan fyysisiltä ja kiinteistövahingoilta, vahingoittamisyrityksiltä ja oikeudettomilta henkilöiltä.
- Tietoturvallisuuteen vaikuttavat toimenpiteet, joita suoritetaan henkilöstöprosessissa ennen palvelussuhdetta, sen aikana ja sen päättymisen yhteydessä.
- Sopimustekniset toimenpiteet, joilla varmistetaan tässä politiikassa kuvattujen periaatteiden toteutuminen myös sidosryhmien kanssa tehtävässä yhteistyössä.

3 Tietosuoja

Tietosuojalla tarkoitetaan toimenpiteitä, joiden tarkoituksena on suojata henkilön yksityisyys henkilötietojen käsittelyssä. Espoon kaupungilla tämä tarkoittaa asiakkaiden, henkilöstön ja sidosryhmien henkilötietojen suojaamista. Tietosuoja on osa toiminnan vaatimustenmukaisuutta, tietoturvallisuutta ja riskienhallintaa.

Espoon kaupunki käsittelee henkilötietoja sisäänrakennetun ja oletusarvoisen tietosuojan periaatteiden mukaisesti:

1. Meillä on selkeä kokonaiskuva hallussamme olevista henkilötiedoista ja niiden käsittelyyn sisältyvistä riskeistä.
2. Keräämme ainoastaan ennalta määriteltyjen käyttötarkoitusten kannalta tarpeellisia henkilötietoja kaupungin tehtävien suorittamiseksi ja palveluiden kehittämiseksi.
3. Huolehdimme suunnitelmallisesti ja läpinäkyvästi henkilötietojen elinkaaren hallinnasta ja suojaamisesta.
4. Varmistamme säännöllisten koulutusten avulla, että henkilöstöllämme on riittävä tietosuojaosaaminen tehtävänkuvasta riippuen.
5. Mahdollistamme asiakkaillemme tiedonsaannin omiin henkilötietoihinsa ja informoimme kattavasti henkilötietojen käsittelyperiaatteista.
6. Arvioimme jatkuvasti henkilötietojen käsittelyyn liittyviä riskejä yksilöiden oikeuksille ja vapauksille.
7. Varmistamme, että sopimuskumppanimme noudattavat vähintään lainsäädännön mukaisia tietosuojaperiaatteita.

Rekisterinpitäjällä on vastuu henkilötietojen käsittelyn lainmukaisuudesta. Rekisterinpitäjä määrittää mihin tarkoituksiin ja millä keinoin henkilötietoja käsitellään. Espoon kaupungilla rekisterinpitäjä on Espoon kaupunki, ellei lainsäädännössä tai viranomaismääräyksissä määrätä toisin rekisterinpitovastuusta. Tällöin esim. lautakunta on rekisterinpitäjä.

[1] Toistensa kanssa eri teknologioiden avulla vuorovaikutuksessa olevien henkilöiden, järjestelmien sekä palveluiden muodostama ympäristö.

4 Riskienhallinta

Riskienhallintaa toteutetaan Espoon kaupungin riskienhallintapolitiikan mukaisesti. Politiikassa kuvattu prosessi (mukaan lukien raportointi, seuranta, vastuut) toimii myös kaupungin tietoturvallisuuden perustana. Periaatteena on, että riskienhallintaprosessia käytetään säännöllisesti toteutettavaan sisäisten ja ulkoisten tietoon kohdistuvien ja tiedosta aiheutuvien riskien hallintaan.

Tietosuojalainsäädännön lähtökohtana on riskiperusteinen lähestymistapa. Tällöin pienen riskin henkilötietojen käsittelyyn ei kohdisteta ylimitoitettuja toimenpiteitä, ja toisin päin. Esimerkiksi yhteystietoluettelon suojausvaatimukset ovat erilaiset kuin potilastietojärjestelmän vaatimukset. Riskipohjaisen lähestymisen avulla tietosuojaan liittyvät velvoitteet ja suojaustoimet räätälöidään Espoon kaupungilla aina kyseiseen henkilötietojen käsittelyyn liittyvien ja havaittujen riskien pohjalta.

5 Varautuminen

Espoon kaupunki varautuu turvaamaan ensisijaisesti kriittisten toimintojensa ja palveluidensa jatkuvuuden normaalioloissa, normaaliolojen häiriötilanteissa sekä poikkeusoloissa. Varautumista toteutetaan ylläpitämällä, harjoittelemalla ja testaamalla tarvittavia valmius- ja muita suunnitelmia. Varautumiseen liittyvät roolit ja vastuut kuvataan em. suunnitelmissa. Tavoitteena on varautua toiminnan häiriöihin ja keskeytyksiin niin, että toimintaa voidaan jatkaa mahdollisimman normaalisti, häiriöiden haittavaikutuksia rajoittaa sekä toipua häiriöistä mahdollisimman nopeasti.

6 Vaatimustenmukaisuus ja tavoitteet

Espoon kaupunkia velvoittavien säädösten lisäksi kaupungin tietoturvallisuudelle sekä tietosuojalle asettaa vaatimuksia ja tavoitteita Espoo-tarina (kaupungin strategia). Lisäksi tietoturvallisuutta ohjaavat lainsäädäntö ja soveltuvilta osin Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmän (VAHTI) ohjeet sekä Kansallinen turvallisuusauditointikriteeristö (KATAKRI).

Lainsäädännössä on asetettu vaatimuksia, erityisesti EU:n yleinen tietosuoja-asetus 2016/679, jotka tulee huomioida henkilötietoja käsiteltäessä. Tietosuojaa säännellään sekä kansallisella että EU:n tasolla.

Kaupungin tietoturvallisuuden tavoitteena on rakentaa ja varmistaa kaupungin toimintaympäristö siten, että häiriön (kuten inhimillinen erehdys, tekninen vika tai tahallinen haitanteko) vaikutukset saadaan rajoitettua ja toiminnot palautettua mahdollisimman nopeasti normaalitilanteeseen. Näin varmistetaan kuntalaisille tarjottavien palveluiden ja kaupungin sisäisten toimintojen korkea laatu. Lisäksi tavoitteena on kaupungin tieto- ja kyberturvallisuus- sekä tietosuojakäytäntöjen yhdenmukaistaminen.

Tietosuojan tavoitteena on huolehtia henkilötietojen oikeaoppisesta ja lainsäädännön mukaisesta käsittelystä, jolloin minimoidaan tietojen väärinkäytön mahdollisuudet. Tietosuojalla parannetaan luottamusta verkkopalveluihin sekä hyödynnetään digitalouden tarjoamia mahdollisuuksia Espoon kaupungin toiminnassa.

Tavoitteiden saavuttamiseksi toteutetut ja suunnitellut toimenpiteet, seurantakäytäntöineen, kuvataan kaupungin tietoturvasuunnitelmassa. Tietoturvatavoitteet saavutetaan vain, jos kaikki noudattavat yhteisesti sovittuja periaatteita.

7 Organisointi, roolit ja vastuut

Tietoturvallisuuteen ja tietosuojaan liittyvät roolit vastuineen on organisoitu kaupungin sääntöjen mukaisesti.

Kaupunginhallitus seuraa tietoturvallisuuden sekä tietosuojan toteutumista kaupungissa. Kaupunginhallitus hyväksyy tietoturva- ja tietosuojapolitiikan ja siihen ehdotetut muutokset. Kaupunginhallituksella on vastuu kaupungin sisäisen valvonnan ja riskienhallinnan järjestämisestä.

Kaupunginjohtajalla on kokonaisvastuu tietoturvallisuuden sekä tietosuojan toteuttamisesta ja näiden toteutumisen raportoinnista kaupunginhallitukselle. Kaupunginjohtaja omistaa tietoturva- ja tietosuojapolitiikan ja esittelee muutokset kaupunginhallitukselle. Kaupunginjohtaja hyväksyy kaupunkitasoiset ohjeet ja linjaukset. Kaupunginjohtajan tukena tietosuoja- ja tietoturvallisuusasioissa on kaupungin johtoryhmä.

Toimialajohtaja vastaa toimialansa riskienhallinnasta ja varautumisesta sekä tietoturvallisuuden ja tietosuojan toteutumisesta.

Tytäryhtiöiden ja -säätiöiden hallitukset ja toimitusjohtajat vastaavat tietoturvallisuuden ja tietosuojan toteutumisesta omissa organisaatioissaan.

Esimies vastaa tietoturvallisuuden ja tietosuojan toteutumisesta omalla vastuualueellaan. Esimiehen keskeisimmät tehtävät ovat huolehtia:

- oman organisaationsa perehdyttämisestä kaupungin tietoturva- ja tietosuojaohjeisiin sekä jokaisen työntekijän työtehtäviin liittyviin tietoturva- ja tietosuojavastuisiin,
- hallita lainsäädännönmukainen tiedon oikeaoppinen käsittely,
- tiedostaa väärinkäytösten rikosoikeudellinen luonne,

- työntekijän palvelussuhteen päättyessä tai henkilön siirtyessä toisiin tehtäviin:
  - kaupungin tiedon ja muun omaisuuden palauttamisesta
  - työntekijän käyttöoikeuksien ja -valtuuksien poistamiseksi.

Henkilöstö vastaa omalta osaltaan ohjeiden noudattamisesta. Jokaisen vastuulla on lisäksi tietoturvallisuuteen ja tietosuojaan liittyvien poikkeamien, uhkien ja riskien ilmoittaminen välittömästi tietoturvapäällikölle, tietosuojavastaavalle tai omalle esimiehelleen. Jokaisella on vastuu omaan tehtäväänsä liittyvän tietosuojan toteuttamisesta sekä tiedon ja tietojärjestelmien asianmukaisesta käytöstä.

Tiedon omistaja vastaa tiedon elinkaaren hallinnasta, luokittelusta (julkisuuden ja salassapidon määrittely) ja eheyden varmistamisesta sekä tallentamisesta luokituksen edellyttämään ympäristöön.

Tietojärjestelmän omistaja (toimiala/vast) vastaa tietojärjestelmänsä ja sen sisältämän tiedon riskienhallinnasta ja varautumisesta sekä tietoturvallisuuden toteutumisesta. Käyttöoikeudet tietojärjestelmään hyväksyy henkilön esimiehen hakemuksen perusteella tietojärjestelmän omistaja tai hänen valtuuttamansa taho.

Prosessin omistaja vastaa prosessinsa riskienhallinnasta ja varautumisesta sekä tietoturvallisuuden ja tietosuojan toteutumisesta. Lisäksi hän vastaa prosessin riippuvaisuuksien tunnistamisesta ja kriittisyyden arvioinnista.

Rekisterin vastuuhenkilö vastaa omalta osaltaan kyseisen rekisterin tietosuojasta ja tietosuojaselosteen lainmukaisuudesta. Vastuuhenkilöiden lisäksi toimialoilla on oltava riittävästi avustavaa henkilökuntaa, joka osallistuu erityisesti rekisteröityjen tekemiin tiedusteluihin vastaamiseen.

Rekisterin yhteyshenkilö vastaa rekisteröityjen informoinnista kyseisen rekisterin osalta. Rekisteröity voi kääntyä rekisterin yhteyshenkilön puoleen saadakseen tarkempia tietoja rekisteristä tai omista oikeuksistaan.

Tietoturvapäällikkö toimii kaupunkiorganisaation tukena ja antaa neuvoja ja ohjausta tietoturvan toteuttamiseksi. Hän vastaa tietoturvaryhmän toiminnasta, tietoturvallisuuden hallintajärjestelmän toimivuudesta sekä tietoturvapolitiikan ja kaupunkitasoisen tietoturvadokumentaation valmistelusta ja kehittämisestä. Tietoturvapäällikkö raportoi tietoturvallisuuden toteutumisesta kaupunginjohtajalle ja turvallisuuspäällikölle sekä vastaa tietoturvallisuuteen liittyvästä viestinnästä yhdessä konserniesikunnan viestintäyksikön kanssa. Tietoturvapäällikkö toimii turvallisuuspäällikön sijaisena sekä tietosuojavastaavan sijaisena yhdessä tietosuojaryhmän kanssa.

Tietosuojavastaava toimii kaupunkiorganisaation tukena ja antaa neuvoa ja ohjausta tietosuojan toteuttamisesta. Tietosuovastaava seuraa kaupungin tietojenkäsittelyyn liittyviä toimintatapoja ja huolehtii, että ne vastaavat lainsäädännön vaatimuksia. Tietosuojavastaava toimii kaupungin yhteyshenkilönä sekä valvontaviranomaisiin että rekisteröityihin. Tietosuojavastaava raportoi tietosuojan toteutumisesta kaupunginjohtajalle ja turvallisuuspäällikölle sekä vastaa tietosuojaan liittyvästä viestinnästä yhdessä konserniesikunnan viestintäyksikön kanssa. Tietosuojavastaava ei vastaa kaupungin henkilötietojen käsittelyn lainmukaisuudesta, vaan siitä on vastuussa kaupungin johto. Tietosuojavastaava toimii tietoturvapäällikön sijaisena.

Turvallisuuspäällikkö vastaa kaupungin turvallisuussuunnittelusta ja varautumisesta.

Konserniesikunnan turvallisuus ja valmiusryhmä ohjaa turvallisuussuunnittelun, tieto- ja kyberturvallisuuden, tietosuojan ja varautumisen kaupunkitasoista valmistelua, kehittämistä sekä toimeenpanoa ja valvoo niiden toteutumista.

Tietoturvaryhmä seuraa tietoturvallisuuden yleistä kehittymistä, uhkia ja riskejä sekä tietoturvallisuuden toteutumista kaupungissa. Ryhmä analysoi ja arvioi em. kokonaisuutta ja tekee siihen perustuen kehitysehdotuksia ja linjauksia[2] kaupungin tietoturvallisuuden parantamiseksi. Lisäksi ryhmä toimii koko kaupunkiorganisaation tukena tietoturva-asioissa.

Tietosuojaryhmä seuraa tietosuojan toteutumista kaupungissa. Ryhmä tekee kaupunkitasoisia linjauksia ja tulkintoja tietosuojan toteuttamiseksi ohjeiden, toimintatapojen, koulutusten ja raporttien muodossa, analysoi toimintaympäristön ja lainsäädännön muutoksia ja arvioi kokonaisvaltaisesti tietosuojariskejä. Ryhmä toimii koko kaupunkiorganisaation tukena tietosuoja-asioissa.

Tietoturvavastaavat huolehtivat toimialojensa sekä konsernihallinnon johdon ohjauksessa tietoturvallisuuden toteutumisesta. He kuuluvat tietoturvaryhmään ja raportoivat toimialajohdolle sekä tietoturvapäällikölle.

Toimialojen ja yksiköiden tietosuojan yhdyshenkilöt huolehtivat vastuualueensa tietosuojan toteutumisesta toimialojensa sekä konsernihallinnon johdon ohjauksessa. He kuuluvat tietosuojaryhmään ja raportoivat vastuualueidensa johdolle. He huomioivat vastuualueidensa erityislainsäädännön ja -tarpeet tietosuojaohjeistuksen osalta.

[2] Linjauksista ei saa tulla kustannusvaikutuksia ilman prosessin tai määrärahan haltijan hyväksyntää.

Tietohallinto vastaa teknisestä tietoturvallisuudesta vastuullaan olevien tietojärjestelmien ja sovellusten osalta, sitä tukevien tietoturvalinjausten tekemisestä ja asetettujen tietoturvavaatimusten toteuttamisesta. Tietohallinto seuraa ja informoi tietoturvapäällikölle vastuualueensa tietoturvallisuuden toteutumisesta.

Asiakirjahallinto vastaa asiakirjahallinnan suunnittelusta ja ohjeistuksesta sekä pysyvästi ja pitkään säilytettävien tietojen hallinnasta. Tiedon omistaja vastaa määräaikaisen tiedon elinkaaren hallinnan toimenpiteistä. Asiakirjahallinto voi tarvittaessa käsitellä kaupungin eri rekisterinpitäjien tietoja perustellusta syystä, esim. asiakkaiden tietopyyntöjen osalta, kun tiedot on siirretty sen säilytettäväksi. Tällöin asiakirjahallinnolla on velvollisuus konsultoida rekisterinpitäjää.

Sisäinen tarkastus vastaa tietoturvallisuuden ja tietosuojan toteutumisen asianmukaisuudesta ja riittävyyden arvioinnista sekä tarkastamisesta.

Henkilöstöhallinto vastaa tietoturvallisuuden ja tietosuojan toteutumisesta henkilöstöprosessissa. Tähän vastuuseen sisältyvät tietoturvaan ja tietosuojaan liittyvien perehdytysten ja koulutuksen organisointi ja taustatietojen tarkistaminen tarvittaessa.

8 Tiedon ja tietojärjestelmien käyttö

Kaupungin tietojärjestelmäympäristössä käytetään tietohallinnon hyväksymiä ja hallinnoimia tietojärjestelmiä, laitteita ja ohjelmistoja, jotka on tarkoitettu työtehtävien hoitamista varten. Otettaessa käyttöön uusia ratkaisuja, tulee varmistua, että ne ovat tietohallinnon tiedossa ja hyväksymiä.

Käyttöoikeudet kaupungin omistamaan ja hallinnoimaan tietoon sekä tietojärjestelmiin myönnetään työtehtävien hoitoon tarvittavassa laajuudessa.

Mahdollisiin laiminlyönteihin ja väärinkäytöksiin sovelletaan lakien lisäksi kaupungin ohjeita.

Kaupungin tietosuojavastaava, tietoturvapäällikkö, turvallisuuspäällikkö, toimialojen tietosuojan yhdyshenkilöt ja tietohallinnon tietoturvasta vastaava henkilö osallistuvat tietoturva- ja tietosuojapoikkeamien, väärinkäytösten sekä nykytilan arviointiin oman työroolinsa rajoissa. Näiden työtehtävien suorittamiseksi edellä mainituille henkilöille mahdollistetaan pääsy tehtävän edellyttämään tietoon.

Kaupungin tietoturva- ja tietosuojaperiaatteita sovelletaan yhtä lailla kokeiluhankkeisiin ja pilotteihin.

9 Tietoturva- ja tietosuojaosaaminen

Esimies huolehtii uudessa tehtävässä aloittavan työtekijän perehdyttämisestä tietoturva- ja tietosuojaohjeisiin, sekä työntekijän omissa työtehtävissä tarvittavaan erityisosaamiseen.

Tietoturvallisuuden ja tietosuojan perus- ja jatkokoulutusta on tarjolla säännöllisesti. Tietoturva- ja tietosuojatietoisuutta ylläpidetään: 1) työntekijän perehdytykseen sisältyvällä koulutuksella, 2) roolipohjaisilla lisäkoulutuksilla ja 3) säännöllisillä kertauskoulutuksilla.

Tämä politiikka on julkisesti saatavilla osoitteissa www.espoo.fi ja www.esbo.fi. Kaupungin tietoturvadokumentaatio kokonaisuudessaan on henkilöstön saatavilla kaupungin sisäisissä informaatiokanavissa työtehtävien edellyttämässä laajuudessa.