TIETOTURVA- JA TIETOSUOJAPOLITIIKKA

Kiuruveden kaupunki

Khall 11.6.2018/§ 103

SISÄLLYSLUETTELO

1. TIETOTURVA- JA TIETOSUOJAPOLITIIKKA

Tietoturva- ja tietosuojapolitiikka on Kiuruveden kaupungin ylimmän johdon hyväksymä strateginen asiakirja, joka on kannanotto tietosuojan ja tietoturvan kehittämiseen. Politiikan tavoitteena on luoda yhdenmukaiset toimintaperiaatteet ja käytännöt hyvän tietosuoja- ja tietoturvatason toteuttamiseksi. Politiikassa määritellään kaupungin tietosuoja- ja tietoturvatyön tavoitteet, vastuut, toimintatavat, valvonta ja seurantajärjestelmä. Politiikalla luodaan edellytykset toiminnan pitkäjänteiseen kehittämiseen. Työssä onnistuminen edellyttää kaupungin johdon sitoutumista tietosuoja- ja tietoturvatyön tukemiseen.
Tietoturva- ja tietosuojapolitiikkaa ja sen perusteella annettuja ohjeita ja määräyksiä noudatetaan kaupungin kaikessa toiminnassa ja ne koskevat kaikkia Kiuruveden kaupungin palveluksessa olevia viranhaltijoita, työntekijöitä ja luottamushenkilöitä, tytäryhtiöitä sekä erikseen toimeksiantosopimuksin sovittuja ulkopuolisia palvelun toteuttajia.

1.1. Tietoturva ja tietosuoja

Tietoturvalla tarkoitetaan eri muodoissa olevien tietojen (mm. sähköisesti tallennettu, välitetty tai rekisteröity tieto, suullinen, puhuttu, postin kuljettama tai paperilla oleva tieto) suojaamista erilaisilta uhkatekijöiltä varmistaen palvelutoiminnan jatkuvuus, minimoiden toimintaan tai asiakkaiden tietoihin liittyvät riskitekijät.

Tietosuojalla tarkoitetaan ihmisten yksityisyyden kunnioittamista ja suojelemista oikeudellisia säännöksiä ja organisaation ohjeita noudattaen.
Tietosuojaa säätelee Suomessa useampikin laki eri toimialoilla, mutta keskeinen tietosuojaan liittyvä lainsäädäntö on EU:n tietosuoja-asetus[1] ja sen kansallinen tietosuojalaki. Kaikki viranomaiset sekä yritykset, jotka käsittelevät asiakkaiden henkilötietoja, ovat velvollisia noudattamaan tietosuojaan liittyvää lainsäädäntöä. Lainmukaisuutta ja tietosuojakäytäntöjä maassamme valvoo tietosuojaviranomaiset, joita tällä hetkellä ovat:

Tietosuojavaltuutettu – antaa henkilötietojen käsittelyä koskevaa ohjausta ja neuvontaa sekä valvoo henkilötietojen käsittelyä tämän lain tavoitteiden toteuttamiseksi ja käyttää päätösvaltaa siten kuin tässä laissa säädetään.

Tietosuojalautakunta – käsittelee henkilötietojen käsittelyyn liittyviä lain soveltamisalan kannalta periaatteellisesti tärkeitä kysymyksiä ja käyttää päätösvaltaa tietosuoja-asioissa siten kuin tässä laissa säädetään.

[1] Suomen ja Euroopan unionin tietosuojalait ovat uudistumassa. EU:n yleistä tietosuoja-asetusta sovelletaan 25.5.2018 alkaen kaikissa EU:n jäsenmaissa. Tietosuoja-asetusta (General Data Protection Regulation, GDPR) sovelletaan lähtökohtaisesti kaikkeen henkilötietojen käsittelyyn.
Tietosuoja-asetusta täydennetään ja täsmennetään kansallisella lainsäädännöllä. Hallituksen esitys HE 9/2018 eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi annettiin 1.3.2018. Uuden tietosuojalain myötä kumottaisiin nykyinen henkilötietolaki sekä laki tietosuojalautakunnasta ja tietosuojavaltuutetusta. Lähde: https://www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/HE_9+2018.aspx, luettu 28.5.2018.

1.2. Tietoturva- ja tietosuojatyön tavoitteet

Kiuruveden kaupungin tavoitteena on turvata henkilötietojen käsittely toteuttamalla EU:n tietosuoja-asetuksen mukaisesti tarvittavat tekniset ja organisatoriset toimenpiteet. Kaupunki pyrkii huolehtimaan tietoturvallisuudesta koko henkilötietojen elinkaaren ajan turvallisella verkko- ja järjestelmäarkkitehtuurilla (turva-arkkitehtuuri). Jo suunniteltaessa tietojärjestelmähankintoja ja ulkoistettaessa henkilötietoja sisältäviä palveluita tulee arvioida tietoturvaa ja tietosuojaa. Tehtävillä toimenpiteillä kaupunki pyrkii siihen, että tieto on vain niiden käytettävissä, joilla on siihen oikeus (luottamuksellisuus). Tietojen oikeellisuus ja suojaus (eheys) pyritään järjestämään niin, ettei tietoa voi tahallisesti tai tahattomasti muuttaa toiminnan luotettavuutta vaarantaen. Tieto ja palvelu ovat saatavissa silloin kun niitä tarvitaan.

Toimenpiteet tavoitteiden toteuttamiseksi:

- Otetaan huomioon uusin tekniikka, toteuttamiskustannukset ja toisaalta arvioidaan tietoturvakeinojen kohtuullisuutta verrattuna arvioituun riskiin.
- Turva-arkkitehtuuriin sisällytetään asianmukaiset palomuurit, verkkojen eriyttäminen, palvelinten kovennukset sekä henkilötietojen ja muiden tietojen siirtoväylien salaaminen.
- Hankinnoissa ja kehityksessä: henkilötietojen käytön rajoittaminen tietojärjestelmien testauksessa ja näiden testausten suorittaminen järjestelmien hyväksyntätestausten yhteydessä. Henkilötietoja käsittelevien järjestelmien ylläpitohenkilöstön sijainnin huomioiminen.
- Pääsyn rajaaminen ja pääsyoikeuksien hallinta. Etäyhteydet rajataan EU:n tai Euroopan talousalueen ulkopuolelta, koska etäyhteyden ottaminen rinnastetaan henkilötietojen siirtoon, mikäli toimenpiteessä käsitellään henkilötietoja.
- Henkilöstölle selvennetään, miten henkilötietoja on sallittua käsitellä esim. pilvipalveluun tallentamisessa, sähköpostilla siirtämisessä sekä siirrettäville tietovälineille tallentamisessa. Huomioidaan tietovälineiden käsittely sekä tietojen luokittelu ja luokitellun tiedon käsittelyohjeistukset.
- Järjestelmien tietoturvallisuudesta huolehditaan päivitysten ja muutosten yhteydessä.
- Fyysinen turvallisuus huolehditaan tarvittavin pääsykontrollein ja -rajauksin. Tietovälineiden turvallinen huolto ja hävittäminen niin, ettei henkilötietoja päädy luvattomasti kolmansille osapuolille.
- Koska rekisterinpitäjän tulee voida jälkikäteen todentaa kuka on suorittanut henkilötietojen haun järjestelmästä, mitä henkilötietoja on katseltu, muutettu, lisätty tai poistettu ja milloin, tämä suunnitellaan etukäteen esim. huolehtimalla lokitietojen automatisoidusta seurannasta mahdollisuuksien mukaan. Lokitietoja tarkastellaan säännöllisesti satunnaisotannalla.

2. TIETOTURVA- JA TIETOSUOJATYÖN HALLINNOINTI, ROOLIT JA VASTUUT

2.1. Kaupunginhallituksen ja johdon vastuut:

Tietosuoja-asetuksen mukaisesti vastuu tietosuojan ja tietoturvan toteuttamisesta on kaupungin johdolla eli rekisterinpitäjällä – kaupunginhallituksella.
Kaupunginhallitus johtaa ja valvoo tietoturva- ja tietosuojatyötä sekä päättää kaupungin tietoturvallisuuden kehittämisen tavoitteista, organisoinnista, resursseista ja toimintavaltuuksista hyväksymällä tietoturva- ja tietosuojapolitiikan sekä nimeämällä tietosuoja- ja tietoturvavastaavan sekä tietohallintovastaavan.

Kaupungin johdon ja esimiesten vastuulla on sitoutua tietosuoja- ja tietoturvatyön jatkuvaan kehittämiseen, huolehtia alaistensa riittävästä perehdytyksestä ja tietoturva- ja tietosuojatyön jatkuvuudesta.

2.2. Tietoturvavastaava ja tietosuojavastaava

Tietoturvavastaava (kaupunginsihteeri) huolehtii:

- Menetelmien kehittämisestä tietoturvan arvioimiseen, parantamiseen ja ylläpitämiseen
- Tietoturvallisten toimintaperiaatteiden toteutuksesta
- Säännöllisistä auditoinneista, tietoturvavastaavalla on johdon antama valtuutus tietoturvallisuuskartoitusten tekemiseen ja havaittujen heikkouksien parantamiseen
- Tietoturvatietoisuuden lisäämisestä ja ylläpidosta
- Tietoturvaohjeiden noudattamisen valvomisesta ja tietoturvatason arvioinnista koko organisaatiossa

Tietosuojavastaavan (arkistosihteeri) tehtävät:

- Asetuksen vaatimusten täytäntöönpano ja soveltaminen organisaatiossa
- Organisaation neuvonta ja ohjaus kaikissa tietosuojakysymyksissä
- Dokumentaation laatimisen, saatavuuden ja säilyttämisen valvonta
- Ilmoitusvelvollisuuden toteutumisen seuranta
- Vaikutusten arviointien tekemisen tukeminen ja valvonta
- Yhteistyö valvontaviranomaisen kanssa
- Tietosuojan ohjeistusten kokoaminen ja kouluttaminen henkilöstölle
- Rekisteröityjen oikeuksien toteuttamisen tukeminen
- Käsittelytoimiin liittyvän riskin asianmukainen huomiointi tehtävien suorittamisessa

Tietosuojavastaavan asemaan ja tehtäväkuvaan liittyvät tietosuoja-asetuksen määrittämät seikat:

- Riippumaton asema organisaatiossa
- Raportoi suoraan rekisterinpitäjän tai käsittelijän ylimmälle johdolle

- Otetaan asianmukaisesti ja riittävän ajoissa mukaan kaikkiin tietosuojaan liittyviin kysymyksiin
- Pätevyysvaatimus tietosuojan alalta: tietosuojalainsäädäntötuntemus, lain vaatimusten soveltamisosaaminen ja alan käytäntöjen tuntemus
- Voi olla rekisterinpitäjän tai käsittelijän palkkalistoilla tai ulkoistettu palveluntuottajalle
- Taattava tarvittavat resurssit sekä asianmukainen pääsy henkilötietoihin ja niiden käsittelytoimiin tietosuojavastaavan tehtävien hoitamiseksi
- Tehtävä yhteistyötä kaikkien organisaation yksiköiden kanssa
- Kaupungin yhteyshenkilö valvontaviranomaisen ja rekisteröityjen suuntaan
- Salassapitovelvollisuus
- Ei saa erottaa tai rangaista tietosuojavastaavan tehtävien hoitamisen vuoksi
- Voi suorittaa muitakin tehtäviä tietosuojavastaavan tehtävien ohella kuitenkin niin, ettei niistä aiheudu eturistiriitoja

2.3. Tietohallintotyöryhmän tehtävät ja rooli

Ryhmään kuuluu tietohallinto- ja tietoturvavastaava (kaupunginsihteeri), joka toimii puheenjohtajana, tietosuojavastaava (arkistosihteeri), joka toimii sihteerinä ja kaupungin johtoryhmän jäsenet. (Khall 13.1.14/§ 11 & 12)
Tarvittaessa ryhmään kutsutaan konsernihallinnon asiantuntijoita eri roolien mukaisesti mm. riskienhallinta, laki, ICT-tukipalveluiden edustaja Ysit Oy, sisäinen tarkastus, pääkäyttäjät jne.

Työryhmä

- Käsittelee, kommentoi, antaa lausuntoja sekä hyväksyy tietoturvaan, kyberturvallisuuteen ja tietosuojaan liittyviä kaupungin ohjeita, linjauksia ja asioita
- Käsittelee merkittävät tietoturvaan ja tietosuojaan liittyvät poikkeamat
- Käsittelee ja hyväksyy osaltaan projektit/hankkeet tietoturvaan ja tietosuojaan liittyvissä kysymyksissä/kehittämiskohteissa
- Kehittää ja edistää kaupungin tietoturvan ja tietosuojan toteutumista
- Ryhmä kokoontuu vähintään kaksi kertaa vuodessa, keväällä ja syksyllä

2.4. Kaupungin eri toimijoiden vastuut

Palvelukeskusten, liikelaitosten ja tytäryhteisöjen vastuut

Palvelukeskusten, liikelaitosten ja tytäryhteisöjen johtajat vastaavat tietoturva- ja tietosuojapolitiikan ja ohjeiden noudattamisesta toiminnassaan. Määritelty tietoturvataso on myös vaadittava ICT-ostopalveluiden toimittajilta läpi koko alihankintaketjun. Johtajien ja nimettyjen vastuuhenkilöiden tulee tuntea toimialansa erityispiirteet, lainsäädäntö ja selventää tietoturvavastuut sekä ICT-varautuminen osaksi kokonaisvaltaista johtamista. Tietojärjestelmien ja tietovarastojen omistajat sekä pääkäyttäjät vastaavat järjestelmien tietoturvasta ja sen jatkuvasta kehittämisestä.

Esimiesten ja pääkäyttäjien vastuut

Esimiesten vastuulla on huolehtia ja noudattaa työnantajaa koskevien lakisääteisten tietoturva- ja tietosuojavelvoitteiden toteutumista. Esimiehet ja tietojärjestelmien pääkäyttäjät vastaavat työntekijöiden käyttöoikeuksista tietojärjestelmiin ja niiden tietosisältöihin työtehtävien edellyttämässä laajuudessa.
He huolehtivat loppukäyttäjän riittävästä perehdytyksestä Kiuruveden kaupungin tietoturvakäytänteisiin varmistaen, että jokainen ymmärtää niiden merkityksen työtehtävissään.

Esimiesten ja pääkäyttäjien vastuulla on myös huolehtia, että työtehtävien muutokset huomioidaan järjestelmien käyttöoikeuksissa ja työsuhteen päättyessä työntekijät palauttavat kaiken työnantajalle kuuluvan omaisuuden sekä käyttöoikeudet tietojärjestelmistä poistetaan. Esimiehiltä odotetaan esimerkillistä sekä vastuullista tietoturvakäyttäytymistä ja heillä sekä pääkäyttäjillä on raportointivelvollisuus tietoturvapoikkeamista tietoturva- ja tietosuojavastaavalle.

Lisäksi etätyössä esimies määrittelee työtehtävät, joita alainen voi tehdä. Etätyön tekeminen pyritään rajaamaan sähköiseen tietoaineistoon, jonka paljastuminen ei vaaranna tietoturvaa ja tietosuojaa. Esimiehellä on velvollisuus tarkistaa, että työntekijällä on etätyön suorittamiseksi riittävät taidot ja tietämys päätelaitteiden ja niillä käsiteltävien tietojen tietoturvallisuudesta. Etätyössä korostuu työntekijän henkilökohtainen vastuu siitä, että luottamukselliset tiedot ovat vain niiden käyttöön oikeutettavien saatavissa ja vain työtehtävien edellyttämässä laajuudessa. Etätyössä on noudatettava hyvän tiedonhallinnan käytänteitä ja erityistä huolellisuusvelvoitetta tietosuojan turvaamiseksi.

Työntekijöiden vastuut

Kaupungin työntekijän velvollisuus on allekirjoittaa salassapito- ja vaitiolositoumus sekä suorittaa hyväksytysti kulloinkin voimassa oleva tietoturva- tai tietosuojakoulutus säännöllisin väliajoin.
Työntekijällä on vastuu noudattaa hyväksyttyjä tietoturvaohjeita ja huolehtia päivittäisissä työtehtävissään hyvän tiedonhallintatavan käytänteistä. Työntekijän vastuulla on myös huolehtia käsittelemänsä tiedon oikeellisuudesta, saatavuudesta ja luokittelusta sekä huolehtia, että organisaation tiedot ovat asianmukaisesti käytettävissä. Tietojen säilytys- tai arkistointiajan päätyttyä ne on hävitettävä ohjeiden mukaisesti. Työntekijällä on velvollisuus raportoida tietoturvaongelmista oman organisaation tietoturva- tai tietosuojavastaavalle.

Työntekijä, joka luo tai tuottaa tietoa, määrittelee tiedon julkisuuden ja sen, kenellä on oikeus käsitellä tietoa. Tiedon tuottajat vastaavat siitä, että käytettävä tieto on luotettavaa ja niiden käytettävissä, jotka tietoa tarvitsevat.

Palveluostoihin liittyvät vastuut

Ostopalveluna hankitun ICT–palvelun operatiivisesta ja teknisestä tietoturvasta ja sen ohjeistamisesta vastaavat palveluntuottajat, joille palvelun toteutus on sopimuspohjaisesti luovutettu. ICT-palveluiden tuottajien tehtävänä on laatia ja ylläpitää keskitetysti tietohallinnon hyväksymien palvelukonseptien mukaisia käytännön tietoturvaohjeita.
Tilaajan tulee huolehtia, että kaikkiin tarjouspyyntöihin ja palvelusopimuksiin sisällytetään tietohallinnon ylläpitämät yleiset tietoturvavaatimukset täydennettynä kyseisen palvelun erityisvaatimuksilla sekä häiriötilanteiden toimintamallit ja selkeä vastuunjako läpi koko palveluketjun. Tilaajan tehtävä on huolehtia ja vaatia palvelutuottajaa raportoimaan ja tiedottamaan merkittävistä tietoturvaan kohdistuvista poikkeustilanteista, riskitekijöistä sekä uhkatilanteista välittömästi palvelusopimuksessa määritellyille yhteyshenkilöille.

Luottamushenkilöiden vastuut

Luottamushenkilö hoitaa tointaan virkavastuulla. Luottamushenkilöt ovat tehtävässään velvollisia käsittelemään ja säilyttämään huolellisesti käsiteltävänään olevia paperisia ja sähköisiä asiakirjoja. Luottamushenkilöitä koskevat samat salassapitosäännöt kuin viranhaltijoita ja työntekijöitä. Luottamushenkilöille on laadittu oma ohje tietoturva- ja tietosuojaperiaatteiden noudattamisesta.

2.5. Seudullinen tietosuoja- ja tietoturvatyöryhmä

Ylä-Savon tasolla (Iisalmi, Kiuruvesi, Sonkajärvi, Vieremä ja näiden omistamat yhtiöt ja säätiöt) tietohallintovastaavien/tietosuojavastaavien/tietoturvavastaavien yhteinen tietohallintotyöryhmä koordinoi tietoturvanäkemyksiä seudullisesti.
Työryhmä kokoontuu noin 2 kertaa vuodessa, kokoonkutsujana toimii Ysit Oy.

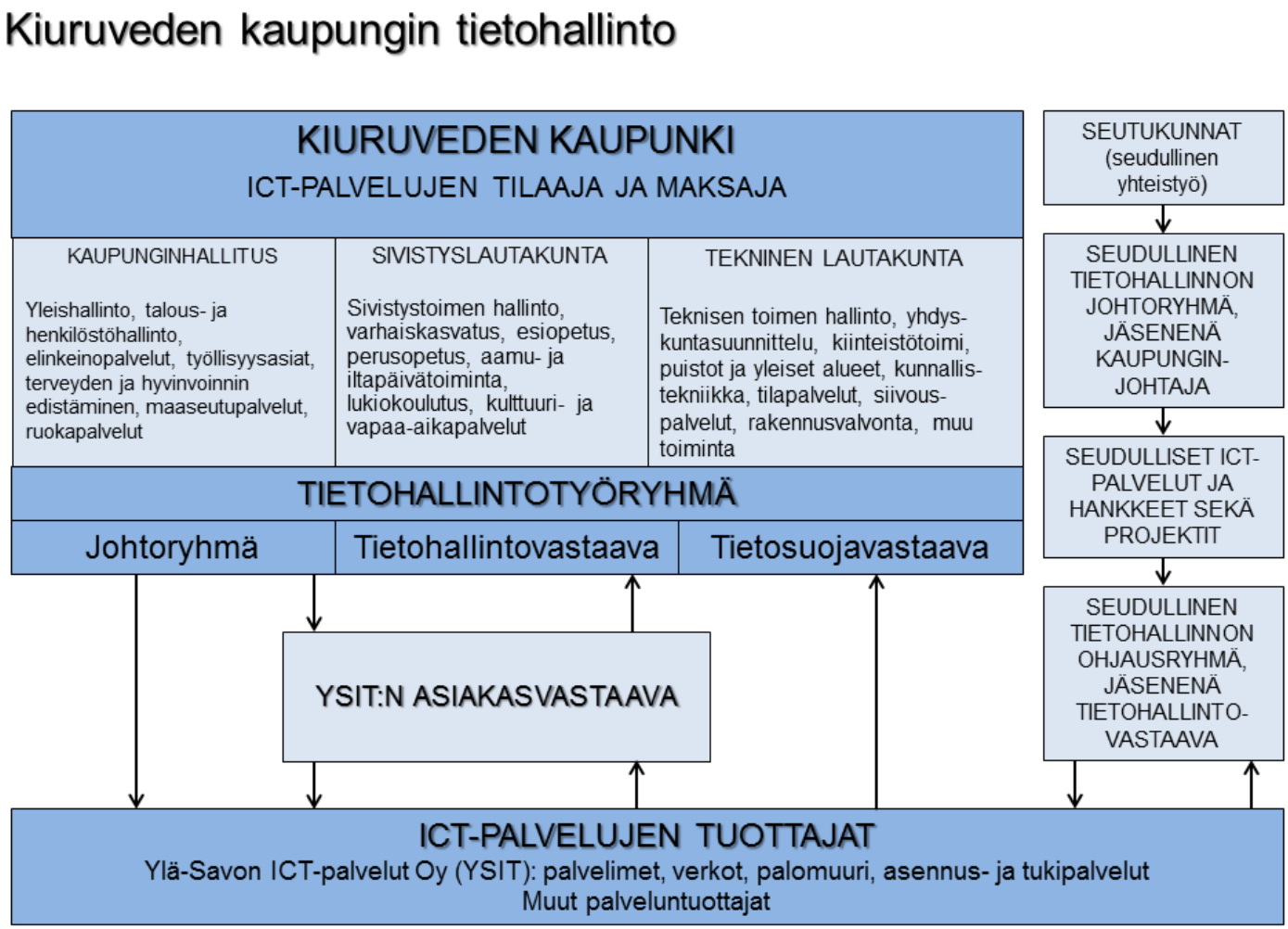
3. TIETOTURVA- JA TIETOSUOJAPERIAATTEET (hallintamalli)

Kiuruveden kaupungin tulee pystyä osoittamaan, että se toteuttaa EU:n tietosuoja-asetuksen ja lain velvoitteet sekä tietoturva- ja tietosuojatyölle asettamansa tavoitteet tietojen käsittelyssä. Tässä kappaleessa on kuvattu Kiuruveden kaupungin tietohallinnon organisaatio sekä tietoturvallisuuden ja tietosuojan hallinnan eri osa-alueet, jotka kaupungin tulee ottaa huomioon tietoturva- ja tietosuojatyössä.

3.1. Tietoturva- ja tietosuojaorganisaatio

Tietoturva- ja tietosuojaorganisaatio (Kuva 1) on määritelty rooleineen ja vastuineen sisältäen myös henkilöstölle määritellyt tietoturvavastuut. Tietoturvaa mitataan, todenne-

taan ja kehitetään säännöllisesti. Tietoturvaa voidaan todentaa esimerkiksi teknisellä testauksella ja hallinnollisten prosessien auditoimisella.



Kuva 1. Kiuruveden kaupungin tietohallinto

3.2. Henkilötietojen inventaario/luettelo rekistereistä ja käsittelijöistä

Kiuruveden kaupunki on määritellyt keskitetyn, ajantasaisen ja kattavan luettelon henkilötietojen käsittelyn ja rekisterien kokonaisuudesta. Henkilötietojen käsittelyä ja niihin liittyviä rekistereitä katselmoidaan määräajoin näissä tapahtuneiden muutosten tunnistamiseksi. Näiden muutosten mukaisten vaikutusten päivittäminen luetteloon on vastuutettu esimiehille ja tätä prosessia koordinoi tietosuojavastaava. Tieto rekistereistä löytyy myös kaupungin internet-sivuilta osoitteesta: http://www.kiuruvesi.fi/Suomeksi/Tietoa-Kiuruvedesta/Rekisterit.

3.3. Riskienarviointi ja -hallinta

Tietosuoja-asetus velvoittaa rekisterinpitäjää ottamaan huomioon uusimman tekniikan ja toteuttamiskustannukset sekä toisaalta arvioimaan tietoturvakeinojen kohtuullisuutta verrattuna arvioituun riskiin. Riskianalyysi toimii tietoturvan mitoittamisen apuvälineenä, tähän voidaan käyttää VAHTI 22/2017 Riskienhallinnan ohjetta ja työkalua.

Kiuruveden kaupunki rekisterinpitäjänä ja ulkopuolinen henkilötietojen käsittelijä ovat velvollisia arvioimaan henkilötietojen käsittelyyn liittyviä riskejä ja valitsemaan arvioidun riskitason mukaan tarvittavat hallintatoimenpiteet. Tietosuojariskien hallinta liitetään osaksi kaupungin riskienhallintaprosessia, jolloin erityisesti merkittävän tason riskit raportoidaan johdolle saakka. Tietosuojavastaava tukee eri yksiköitä, jotta tietosuojariskejä tunnistettaisiin paremmin ja on mukana määrittelemässä tunnistetuille, hallintaan otettaville riskeille tarvittavia hallintakeinoja.

3.4. Tietosuojaprosessit

Tietosuojan vaikutusten arviointi

Arviointi on pakollista tehdä silloin, kun henkilötietoihin sisältyy korkea riski sekä rekisteröityjen oikeuksien toteuttaminen. Tietosuojan vaikutustenarviointiprosessi tulee sisällyttää kaupungin muutosprosesseihin. Vaikutustenarviointiprosessin käynnistävät tekijät tulee määritellä ja niitä sovelletaan yhdenmukaisesti läpi organisaation.
Tietosuojan vaikutustenarviointiin liittyvät mallipohjat tulee vakinaistaa ja niiden tueksi laaditaan ohjeet varmistamaan yhdenmukaiset ja täsmälliset toimintatavat. Tietosuojavastaava osallistuu vaikutustenarviointien tekemiseen arvioiden analyysin tuloksia ja antaen neuvoja riskienhallintakeinojen suunnittelussa. Tarvittavat prosessit on laadittu seuraamaan ja varmistamaan, että tietosuojan vaikutustenarviointia koskevaa prosessia noudatetaan. Valvontaviranomainen on julkaissut tarkemman ohjeen, milloin ja miten vaikutustenarviointi tehdään. Ohjeessa käsitellään keinoja selvittää, liittykö henkilötietojen käsittelyyn korkea riski.

Rekisteröityjen oikeudet ja tietopyynnöt

Kiuruveden kaupunki määrittelee tiedonohjaussuunnitelmaan *Asiakastietojen tarkastus, korjaus ja poistaminen* -prosessin rekisteröityjen oikeuksiin liittyvien pyyntöjen käsittelemiseksi (ml. oikeuksien laajuuksien ja sovellettavuuden määrittely, yhteyspisteen määrittäminen organisaatiossa, pyyntöä esittävän rekisteröidyn identiteetin varmistaminen, pyynnön reitittäminen, tietojen koostaminen, pyynnön sisällön toteuttaminen). Rekisteröityjen esittämät pyynnöt käsitellään ilman aiheetonta viivytystä ja rekisteröidylle ilmoitetaan kuukauden kuluessa ne toimenpiteet, joihin organisaatio aikoo pyynnön johdosta ryhtyä. Pyynnöt osoitetaan kirjaamoon, jossa ne kirjataan asianhallintajärjestelmään ja ohjataan oikealle taholle käsittelyä varten.

4. HENKILÖTIETOJEN KÄSITTELYN PERIAATTEET

4.1. Kaupungin tietoturva- ja tietosuojapolitiikka ja henkilöstön kouluttaminen

Kiuruveden kaupungin tietoturva- ja tietosuojapolitiikka määrittää ylätason linjaukset, periaatteet ja vastuut tietosuojan hallinnoinnissa ja henkilötietojen käsittelyssä. Tietosuojapolitiikka on kaupungin johdon hyväksymä asiakirja, ja se on julkaistu kaupungin verkkosivustolle ja siitä on tiedotettu henkilöstöä, luottamushenkilöitä sekä tytäryhtiöitä läpi koko organisaation. Kiuruveden kaupungin henkilötietojen käsittelijöihin kohdistuvat velvoitteet ja sanktiomenettelyt ovat kuvattuna erikseen henkilötietojen käsittelystä koottuun ohjeeseen, joka on tämän asiakirjan liitteenä (Liite 1. Ohje henkilötietojen käsittelijöille).

Henkilöstön tietoturvatietoisuus ja osaaminen varmistetaan säännöllisillä, vuosittaisilla koulutuksilla ja ohjeiden jalkauttamisella. Vaitiolo- ja salassapitosopimukset allekirjoitetaan henkilöstön sekä alihankkijoiden kanssa. Sitoumukset säilytetään työ- ja toimeksiantosopimusten liitteinä. Tarvittaessa ja lain mahdollistaessa tehdään henkilöiden turvallisuusselvitykset.
Kaupungin eri rekistereistä vastaavat henkilöt huolehtivat ulkoisesta tiedoksiannosta rekisteröidyille, mm. julkaisemalla tietosuojaselosteen kaupungin verkkosivulle sekä linkittämällä sen rekisterin yhteyteen. Päivitettäessä tietosuojaselosteita aikaisempi, vanhentunut versio arkistoidaan.

4.2. Tietosuoja hankinnoissa sekä järjestelmä- ja sovelluskehityksessä

Kiuruveden kaupungin hankkiessa järjestelmiä, sovelluksia ja palveluja, jotka tulevat käsittelemään henkilötietoja, tietosuoja tulee huomioida jo hankintaprosessissa. Näin valitaan sellaisia toimittajia, joiden toimittamien tuotteiden tietosuojataso vastaa asetuksen vaatimuksia. Tietosuojavaatimukset tulee asettaa jo tarjouspyyntöön ja liittää ne osaksi tarjouspyynnön perusteella tehtäviä sopimuksia. Suositeltavaa on vaatia salassapitoa sopimuksissa ja tarvittaessa lisäksi myös erillisillä vaitiolositoumuksilla.

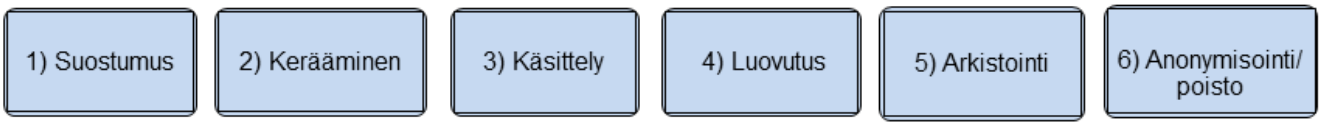
Kun uusia järjestelmiä, sovelluksia tai palveluja otetaan käyttöön, tulee ennen käyttöönottoa arvioida tarvittavat toimenpiteet tietosuojan säilymisen kannalta. Tällaisia toimenpiteitä voivat olla esimerkiksi rekisteriselosteen laadinta tai päivittäminen. Kiuruveden kaupunki ei voi tätä velvollisuutta rekisterinpitäjänä ulkoistaa. Käsittelyn periaatteet ja sisäänrakennettu tietosuoja on suunniteltava tapauskohtaisesti ja se vaatii ennakointia, esim. jo ennen tarjouspyynnön tekemistä pitää tietää mitä tarvitsee, eli tietosuoja tulee olla osa hankinnan vaatimusmäärittelyä.

Mikäli Kiuruveden kaupunki rekisterinpitäjänä ulkoistaa sovelluskehityksen kolmannelle osapuolelle, tulee ulkoistussopimuksessa vaatia sisäänrakennetun ja oletusarvoisen tietosuojan toteutuminen kehitysprosessissa. Vaatimukset tulisi pystyä yksilöimään mahdollisimman tarkasti eikä viittaamaan yleisesti ”riittävän tietosuojan toteuttamiseen”. Kaupungin tulee hallita sovelluskehityksen ulkoistussopimuksissa olevia vaatimuksia. Henkilötietojen käytön rajoittamisesta tulee huolehtia tietojärjestelmien testauksessa. Tietoturvatestaus tulee suorittaa järjestelmien hyväksyntätestauksen yhteydessä. Myös henkilö-

tietoja käsittelevien järjestelmien ylläpitohenkilöstön sijainti tulee huomioida, jotta ei luovuteta tietoja kolmansiin maihin.

4.3. Vaatimukset henkilötiedon elinkaaren ajan

Tietosuoja-asetuksen vaatimusten toteutuminen tulee taata määrittelyvaiheesta koko käsiteltävien henkilötietojen elinkaaren ajan. Elinkaarella tarkoitetaan ajanjaksoa henkilötietojen keräämisestä niiden anonymisointiin tai poistoon (Kuva 2).



Kuva 2. Henkilötietojen elinkaari

Seuraavat tekniset ja organisatoriset toimenpiteet ja menettelyt tulee toteuttaa, jotta voidaan hallita suostumuksia sekä kieltoja, ja myöhemmin tarvittaessa osoittaa rekisteröidyn antama suostumus käsittelytoimiin. Lisäksi alle 16-vuotiaat käyttäjät tulee tunnistaa riittävän luotettavasti.

1) Oletusarvoisesti kerätään vain henkilötietoja, jotka ovat välttämättömiä käsittelytarkoituksen kannalta (käsittelyllä on oikeudellinen peruste).

2) Pääsy henkilötietoihin on rajattu käyttäjätasolla. Pääsy perustuu aina työtehtäviin liittyvään tarpeeseen ja pääsyoikeuksissa noudatetaan vähimpien oikeuksien -periaatetta (principle of least privilege). Vähimpien oikeuksien periaatteella tarkoitetaan rajausta, jolla virheistä ja tarkoituksellisesta haitantehosta syntyvät vahingot jäävät mahdollisimman pieniksi.

3) Taataan rekisteröityjen oikeuksien toteutuminen varmistamalla, että käsiteltävät henkilötiedot ovat täsmällisiä ja tarvittaessa päivitettyjä. Käsittelyn tarkoituksiin nähden epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä.

4) Tietoja ei kerätä eikä säilytetä suurempia määriä eikä kauemmin kuin on välttämätöntä kyseiseen käsittelytarkoitukseen nähden.

5) Taataan henkilötietojen suoja tarvittavin tietoturvakeinoin.

Rekisterinpitäjän on ennen käsittelyn aloittamista määriteltävä henkilötietojen tarpeellinen säilytysaika, eli kuinka kauan henkilötietoja tarvitaan niiden käsittelytarkoitukseen. Vähintäänkin on määriteltävä ne kriteerit, joiden pohjalta säilytysaika määräytyy. Säilytysaika-

määritykset tulee tehdä lisäksi henkilötietoja käsitteleviin sovelluksiin ja järjestelmiin hallintakeinojen toteutusvaiheessa.

Säilytysaika on huomioitava myös palvelinten varmistuksissa, ettei vanhentunutta ja käsittelystä poistunutta tietoa pääse palautumaan esimerkiksi epäsuotuisista tilanteista järjestelmän toipumisen yhteydessä. Mikäli henkilötietoja ei enää tarvita niiden käsittelytarkoituksen toteuttamiseen, mutta niitä ei voida poistaa muun sääntelyn takia, tulee tiedot arkistoida ja niiden käsittelyä rajoittaa. Tällaisia tietoja voivat olla esimerkiksi kirjanpitoa varten säilytettävät tiedot. Kun määritelty säilytysaika tuotantojärjestelmissä ja arkistossa on umpeutunut, tiedot tulee joko poistaa tietoturvallisesti tai anonymisoida siten, että rekisteröidyt eivät enää ole tunnistettavissa. Säilytysaika tulee ilmoittaa myös rekisteröidyille suunnattavassa viestinnässä esim. tietosuojaselosteessa.

4.4. Viranomaisyhteistyö

Rekisterinpitäjällä on velvollisuus tehdä yhteistyötä valvontaviranomaisen kanssa valvontaviranomaisen niin pyytäessä. Kiuruveden kaupungilla yhteistyö valvontaviranomaisen kanssa kuuluu tietosuojavastaavan vastuulle. Mikäli Kiuruveden kaupungilla rekisterinpitäjänä on toimintaa useassa EU:n jäsenvaltiossa, voi se asioida päätoimipaikkansa valvontaviranomaisen kanssa.

Valvontaviranomaisen pyynnön ohella kaupungin on tehtävä yhteistyötä valvontaviranomaisen kanssa ennakkokuulemisen muodossa, jos tietosuojan vaikutustenarvioinnin perusteella suunniteltuun henkilötietojen käsittelyyn liittyy suuria riskejä, ja rekisterinpitäjällä ei ole keinoja riskitason pienentämiseksi.

Kiuruveden kaupungilla on myös ilmoitusvelvollisuus valvontaviranomaiselle henkilötietojen tietoturvaloukkaustilanteissa luvussa 5 kuvatulla tavalla. Valvontaviranomainen voi vaatia yhteistyötä tilanteen selvityksen yhteydessä, jotta se voi arvioida kaupungin asetuksen velvollisuuksien noudattamista. Henkilötietojen tietomurtotapauksissa kaupungin on hyvä tehdä yhteistyötä myös Viestintäviraston kanssa tekemällä ilmoitus tietoturvaloukkauksesta Kyberturvallisuuskeskukselle sekä tehdä tutkintapyyntö poliisille.

5. TIETOTURVALLISUUSTOIMINTA

Turva-arkkitehtuuri
Kiuruveden kaupungilla on turvallinen verkko- ja järjestelmäarkkitehtuuri, joka sisältää asianmukaiset palomuurit, verkkojen eriyttämisen, palvelinten kovennukset sekä henkilötietojen ja tietojen siirtoväylien salaamisen. Kiuruveden kaupungin käytössä on mm. salattu sähköposti arkaluonteisten ja salassapidettävien tietojen siirtoon.

Käyttäjä- ja pääsynhallinta
Käyttäjät ja admin-käyttäjät on dokumentoitu. Kaikilla järjestelmien ja rekisterien käyttäjillä on henkilökohtaiset käyttäjätunnukset. Järjestelmän käyttäjän luomis-, muutos- ja pois-

toprosessi dokumentoidaan ja toteutetaan määräysten mukaisesti. Järjestelmien ja rekisterien käyttäjät katselmoidaan säännöllisesti vastuuhenkilön toimesta. Käyttäjien tunnistaminen ja todentaminen on tietoturvallinen ja salasanavaatimukset ovat riittävällä tasolla. Pääsynhallinnassa tulee ottaa huomioon myös etäyhteydet EU:n tai Euroopan talousalueen ulkopuolelta, sillä etäyhteyden ottaminen rinnastetaan henkilötietojen siirtoon, mikäli toimenpiteessä käsitellään henkilötietoja.

Käsittelyn valvonta ja seuranta, lokitus
Rekisterinpitäjän tulee voida jälkikäteen todentaa lokitiedostoista, kuka on suorittanut henkilötietojen haun järjestelmästä, mitä henkilötietoja on katsottu, muutettu, lisätty tai poistettu sekä milloin toimenpide on suoritettu (aikaleima). Myös admin-käyttöä tulee seurata. On tärkeää, että menettelyt, joilla lokitiedostoja seurataan ja miten epäillyt väärinkäytökset käsitellään, on suunniteltu etukäteen. Kiuruveden kaupungilla eri rekistereitä sisältävien järjestelmätoimittajien ja pääkäyttäjien kanssa sovitaan tapauskohtaisesti säännöllisestä lokitietojen raportoinnista. Lokitiedot säilytetään asian-/dokumenttienhallintajärjestelmässä tietosuoja-asetuksen mukaisesti 5 vuotta. Lokitietojen seuranta ja valvonta on vastuutettu tietosuoja- ja tietoturvavastaaville, joilla on ainoastaan pääsy lokitietoihin. Seurannasta ja sen toteuttamisesta sovitaan tietohallintotyöryhmässä.

Henkilötietojen väärinkäytöksestä
Mahdolliset seuraamukset henkilötietojen väärinkäytöksistä on sisällytetty henkilötietojen käsittelijöille sekä luottamushenkilöille suunnattuihin ohjeisiin. Seurantaa on mahdollisuuksien mukaan hyvä suorittaa automatisoidusti, sillä lokia muodostuu tyypillisesti hyvin paljon. Poikkeamien hallintaa käsitellään tarkemmin kappaleessa 6.

Omaisuuden ja tiedon hallinta
Tietovälineiden käsittelyssä pitää ymmärtää käsiteltävien tietojen luonne ja varmistaa tarvittava tietoturvallisuus. Tietovälineiden käsittelyyn on olemassa ohjeistukset. Henkilöstölle tulee olla selvää, miten henkilötietoja on sallittua käsitellä esimerkiksi pilvipalveluun tallentamisessa, sähköpostilla siirtämisessä ja siirrettäville tietovälineille tallentamisessa.

Päivitysten ja muutosten hallinta
Ohjelmistokomponenttien haavoittuvuuksien saatavilla olevien päivitysten seuranta ja hallinta (CERT-ryhmät). Järjestelmien tietoturvallisuudesta huolehditaan päivitysten ja muutosten yhteydessä. Muutosten hallinnasta ja jäljitettävyydestä huolehditaan myös.

Fyysinen turvallisuus, toimitilat
Tilaturvallisuudesta huolehditaan tarvittavin pääsykontrollein ja -rajauksin. Tietovälineiden, joilla henkilötietoja käsitellään, turvallinen huolto ja hävittäminen, jotta henkilötietoja ei päädy luvattomasti kolmansille osapuolille. Henkilöstön tulee käyttää kulunvalvontaa varten annettuja tunnistusvälineitä.

Toimittajien ja sopimusten hallinta
Tietoturva- ja tietosuojavaatimusten määrittely sopimuksen/hankinnan kohteelle ja alihankkijoille. Sovittava tietoturvan ja tietosuojan hallinnan menettelyt, mukaan lukien hen-

kilötietojen käsittelyn seuranta ja valvonta sekä tietoturvaraportointi ja tietoturvapoikkeamien hallinta.

Toiminnan jatkuvuuden hallinta
Henkilötietojen varmuuskopioinnista huolehtiminen ja niitä käsittelevien järjestelmien kapasiteetin hallinta. Tarvittavat suunnitelmat epäsuotuisiin tilanteisiin ja niistä toipumiseen, jotta voidaan taata henkilötietojen saatavuus esimerkiksi teknisen vian sattuessa.

6. POIKKEAMIEN HALLINTA JA ILMOITUSVELVOLLISUUS

Kiuruveden kaupungilla tietoturvapoikkeamien käsittelystä ja sen kehittämisestä vastaa tietohallintotyöryhmä.

6.1. Tietoturvapoikkeamien hallintaprosessi

Vaihe 1. Tietoturvapoikkeamien käsittelykyvyn muodostaminen
Tämä vaihe käsittää erilaiset varautumistoimet, joiden avulla poikkeamatilanteessa voidaan toimia. Varautumistoimissa huomioidaan mm. järjestelmien ja prosessien riittävä dokumentaatio, päätöksenteko, riippuvuuksien tunnistaminen, omat ja yhteistyötahojen henkilöstöresurssit, tilannekuvan muodostaminen ja tiedon jakaminen, haittaohjelmien ja poikkeavan toiminnan havainnointikyvyn kehittäminen, sopimusmenettelyt ja harjoittelu.

Vaihe 2. Tietoturvapoikkeaman havaitseminen ja analysointi
Vaihe käsittää normaalista poikkeavan toiminnan havaitsemisen ja analysoinnin, minkä tavoitteena on selvittää, mitä on tapahtunut ja miksi. Poikkeamatiedon lähteitä voivat olla esim. järjestelmälokit, hyökkäyksen havainnointi- ja estojärjestelmät, tietoverkon aktiivilaitteet, haittaohjelmien ja roskapostin suodatusjärjestelmät, päätelaitteet, ulkoistetun palveluntoimittajan tai tietoliikenneoperaattorin järjestelmät, kulunvalvonta- ja kameravalvontajärjestelmät, käyttäjien ja asiakkaiden yhteydenotot sekä palvelutoimittajien ja sidosryhmien yhteydenotot.
On hyvä, että koko henkilöstö koulutetaan siten, että kaikilla on valmiudet havaita mahdollinen tietoturvapoikkeama tai sen uhka. Analysoinnin tuloksena voidaan todeta, onko kyseessä tietoturvapoikkeama tai esim. ICT-häiriötilanne. Valvontaa voidaan suorittaa myös esim. tietoturva-tapahtumien havainnointiohjelmistolla, jolla voidaan keskitetysti kerätä ja analysoida mm. palomuurien, hakemistopalvelun ja tietoturvaohjelmistojen tapahtumia sekä työasema- ja palvelinlokeja.

Vaihe 3. Reagointi tietoturvapoikkeamiin
Reagointiin liittyvät toimenpiteet vastuutetaan ja aikataulutetaan, jotta niiden avulla voidaan minimoida mahdolliset vahingot. Poikkeamasta informoidaan muita viranomaisia ja sidosryhmiä sekä käynnistetään toimenpiteet poikkeaman korjaamiseksi. Tietosuojavastaava tekee ilmoituksen sekä valvontaviranomaiselle että niille rekisteröidyille, joiden yksityisyyden suoja on vaarantunut, mikäli katsotaan, että tarvetta on tehdä tietosuoja-asetuksen mukainen ilmoitus. Jos tilanne vaatii, tulee tehdä tutkintapyyntö myös poliisille.

Vaihe 4. Toipumisvaihe

Organisaation ja palveluiden toiminta palautetaan normaalitilaan. Poikkeamasta laaditaan raportti, jonka havaintojen perusteella kehitetään käsittelykykyä ja varautumista, jotta poikkeaman toistuminen voitaisiin jatkossa estää.
Kaupungin tulee varmistaa tarvittaessa ulkopuolisen avun saaminen, erityisesti laajavaikutteisissa poikkeamissa. Henkilötietoihin liittyvistä poikkeamatilanteista tulee myös dokumentoida tutkintaan ja toipumiseen tehdyt toimenpiteet sekä huolehtia tarvittavien todistusaineistojen säilyttämisestä. Valvontaviranomainen voi pyytää dokumentaatiota auditoitavaksi.

6.2. Ilmoituksen tekeminen

Kaupungin tulee tehdä ilmoitus valvontaviranomaiselle henkilötietojen tietoturvaloukkauksesta 72 tunnin kuluessa siitä, kun loukkaus on havaittu.
Valvontaviranomaiselle suunnattavassa ilmoituksessa tulee kertoa vähintään seuraavassa kappaleessa listatut kohdat. Ilmoitusvelvollisuus huomioidaan myös kriisi- ja häiriötilanneviestinnässä niin prosessin kuin ohjeistuksen osalta.

Ilmoituksen sisältö:

1. Kuvaus mitä on tapahtunut.
2. Mikäli mahdollista, niiden rekisteröityjen ryhmät ja lukumäärät, joita loukkaus koskettaa.
3. Tietosuojavastaavan nimi ja yhteystiedot tai muu yhteyspiste, josta valvontaviranomainen voi kysyä lisätietoja.
4. Millaisia vaikutuksia henkilötietojen tietoturvaloukkauksella voi todennäköisesti olla rekisteröidyille.
5. Kuvaus niistä toimenpiteistä, joita kaupunki aikoo toteuttaa tai jotka se on jo toteuttanut haittavaikutusten lieventämiseksi ja tilanteen ratkaisemiseksi.
6. Jos ilmoitusta valvontaviranomaiselle ei ole mahdollista tehdä 72 tunnin kuluessa tietoturvaloukkauksen ilmitulosta, on ilmoitukseen liitettävä perusteltu selvitys viivästyksen syistä valvontaviranomaiselle. Tarvittaessa tietoja voidaan antaa vaiheittain.

Edellä mainittujen tehtävien suorittamiseksi tehdään prosessimäärittely tiedonohjaussuunnitelmaan: Tietosuojapoikkeamista ilmoittaminen, johon kuuluvat selkeät roolit ja vastuut. Tyypillisesti prosessi integroidaan osaksi tapahtumien hallintaa. Mikäli Kiuruveden kaupunki ei hallinnoi itse työasema- ja järjestelmäympäristöä, tulee poikkeamien hallinta ja ilmoitusvelvollisuus sisällyttää toimittajasopimuksiin. Myös tällöin tarvitaan prosessimäärittely, jossa kuvataan millaisista tilanteista ilmoitetaan rekisterinpitäjälle, mitä kanavia käyttäen ja miten tilanteen selvittämiseen ja ilmoitusvelvollisuuden täyttämiseen liittyvät vastuut jakautuvat.
Henkilöstöä, luottamushenkilöitä ja sidosryhmiä varten Kiuruveden kaupungin poikkeamailmoittamiseen on tehty keskitetty ilmoituslomake osoitteeseen: http://www.kiuruvesi.fi/Suomeksi/Hallinto-ja-paatoksenteko/Tietohallinto/Tietoturva. Kaikista ilmoituksista tulee tulla tieto kaupungin tietosuoja- ja tietoturvavastaavalle.

6.3. Hallinnolliset sakot ja seuraamukset

Tietosuoja-asetus tuo valvontaviranomaisille uutena oikeuden määrätä rekisterinpitäjälle ja/tai henkilötietojen käsittelijälle sakkoja tai hallinnollisia seuraamuksia tietosuoja-asetuksen velvoitteiden laiminlyönnistä. Sakon suuruus määräytyy rikkomuksen luonteen perusteella kolmeen luokkaan. Sakon enimmäismäärä on 20 miljoonaa euroa tai 4 % organisaation edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta. Niiden tietosuoja-asetuksen vaatimusten laiminlyöntien osalta, joihin ei sovelleta hallinnollisia sakkoja, voi valvontaviranomainen määrätä muita varoittavia seuraamuksia. Näitä voivat olla esimerkiksi käsittelyn kieltäminen, kunnes tarvittavat velvollisuudet on täytetty. Valvontaviranomaisella on oikeus auditoida rekisterinpitäjän tietosuojan toteutusta. Suomessa julkishallinnon osalta käytettävä menettely tarkentuu osana lainsäädäntötyön etenemistä.

7. SEURANTA JA VALVONTA

7.1. Tietotilinpäätös

Seurannan keskiössä on vuosittain tietosuojavastaavan kokoama tietotilinpäätös, joka esitellään kaupunginhallituksessa tilinpäätöksen yhteydessä aina maaliskuussa. Tietotilinpäätös on raportti, joka syntyy Kiuruveden kaupungin sisäisen tarkastelun ja arvioinnin tuloksena. Lisäksi se on myös työkalu EU:n tietosuoja-asetuksen rekisterinpitäjän velvollisuuksien osoitusvelvollisuuden todentamiseen sekä osa kunnan sisäänrakennettua tietosuojaa eli riskien jatkuvaa seurantaa.

Tietotilinpäätös voidaan jakaa julkiseen osaan ja ei-julkiseen. Julkaisemalla tietotilinpäätöksen kaupunki osoittaa, että se noudattaa lainsäädäntöä ja, että tietoja käsitellään asianmukaisesti ja luottamuksellisesti. Samalla minimoidaan valvontaviranomaisten ja asiakkaiden tiedustelu ja kyselytarve, kun kaupunki raportoi ja tiedottaa oma-aloitteisesti ja ennakoiden.

Tietotilinpäätös on lisäksi johdon ja sisäisen sekä ulkoisen valvonnan työväline. Se nostaa esille tietojen käsittelyyn liittyviä kehittämiskohteita ja antaa kokonaiskuvan kunnan tietojen käsittelyn ja tiedonhallinnan nykytilasta. Se toimii ennen kaikkea luottamuksen rakentajana Kiuruveden kaupungin menettelytapoihin.

Tietotilinpäätökseen voidaan sisällyttää mm. seuraavia mittareita:

- keskeiset tietovarantojen tunnusluvut
- tietoturva- ja tietosuojapoikkeamat
- tietojärjestelmien käyttökatkot ja niiden vaikutukset
- käytönvalvontasuunnitelman toteutuminen
- tietoturvan ja tietosuojan omavalvontasuunnitelman toteutuminen
- tietosuoja- ja tietoturvarikkomukset

- rekisteröityjen informoinnin ajantasaisuus ja tulleet pyynnöt
- mahdolliset viranomaisten selvityspyynnöt
- lakimuutokset ja niiden jalkautukset
- tietosuoja- ja tietoturvakoulutukset
- uudet ohjeistukset

7.2. Tietosuojaperiaatteiden päivittäminen

Tietoturva- ja tietosuojapolitiikassa esitellyt tietosuojaperiaatteet ovat tämän hetken käytännön mukaiset. Periaatteita päivitetään säännöllisesti ja muutoksista tiedotetaan yhteistyökumppaneita. Tietosuojapolitiikkaa tarkastellaan valtuustokausittain.

LÄHTEET

Tietoturva- ja tietosuojatyötä ohjaavat keskeiset VAHTI-ohjeet:
2/2015 Ohje salauskäytännöistä
2/2016 Toiminnan jatkuvuuden hallinta -ohje julkaistu.
8/2017 Tietoturvapoikkeamatilanteiden hallinta
22/2017 Ohje riskienhallintaan
25/2017 Sähköisen asioinnin tietoturvaohje
Saatavilla:
https://www.vahtiohje.fi/web/guest;jsessionid=11419FB178DBD29F9DDAD5F833E5F25A9638F166DCD7ACCB359F51DE7010B51C7D3237A58BB8ADE471DCC1
Luettu 16.4.2018.

LIITTEET

Liite 1. Ohje henkilötietojen käsittelijöille
Liite 2. Henkilöstön lyhyet tietoturva- ja tietosuojaperiaatteet
Liite 3. Luottamushenkilön lyhyet tietoturva- ja tietosuojaperiaatteet