Laitila

LAITILAN KAUPUNGIN TIETOTILINPÄÄTÖS 2021

Sisällys

Sisällys 1
1 Johdanto 2
2 Tietojen käsittelyyn vaikuttava lainsäädäntö 3
2.1 Tietosuojaa määritelevä keskeinen lainsäädäntö 3
2.2 Tietosuoja lainsäädännön keskeiset muutokset 3
3 Tiedonhallinnan keskeiset muutokset 2021 3
4 Rekisteröityjen oikeuksien toteutuminen 4
5 Rekisterinpitäjän vastuut ja velvoitteet 4
5.1.1 Osoitusvelvollisuus 4
5.1.2 Käsittelyn oikeusperusta 4
5.1.3 Tietosuojavastaava 5
5.1.4 Sisäänrakennettu ja oletusarvoinen tietosuoja 5
5.1.5 Ilmoitusvelvollisuus henkilötietojen tietoturvaloukkauksista 5
6 Kaupungin tietovarannot ja keskeiset tunnusluvut 5
7 Tiedon hallinta 6
7.1 Vastuun jakautuminen kunnassa 6
7.2 Dokumentaatio ja koulutus 6
7.3 Rekisterinpitäjän ja -käsittelijän väliset sopimukset 7
8 Tietosuojauksen periaatteet 7
8.1 Suurimmat uhkatekijät 7
8.2 Tapahtuneet tietoturvaloukkaukset 7
9 Kehittämiskohteet ja keskeisimmät muutokset vuonna 2022 8
10 2021 määriteltyjen kehittämiskohteiden tilannekatsaus 8

1 Johdanto

Laitilan kaupungin tietopääoman hyödyntäminen on koko ajan tärkeämpää, jotta voidaan tuottaa kansalaisille palvelut turvallisesti ja oikea-aikaisesti. Palvelut pitää pystyä toteuttamaan entistä kustannustehokkaammin ja nopeammin, mutta asioinnin turvallisuudesta ei saa tinkiä. Kansalaisten tulee voida luottaa siihen, että heidän henkilötietojaan käsitellään luottamuksellisesti ja digitaalinen turvallisuus oletusarvoisesti huomioiden.

Tietotilinpäätöksen tavoitteena on lisätä avoimuutta ja luottamusta siihen, että organisaatiossa noudatetaan organisaation luomia tietoturva- ja tietosuojaperiaatteita ja käsitellään henkilötietoja niiden mukaisesti.

Tietotilinpäätös kuvaa tietojen käsittelyn nykytilaa sekä arvioi tietosuojan ja tietoturvan toteutumista. Lisäksi se sisältää tietosuojaan ja tietoturvaan liittyviä kehittämistarpeita ja toimenpiteitä.

Tietotilinpäätöksen koonnista vastaa kaupungin tietosuojavastaava yhdessä tietopalvelu- ja työhyvinvointipäällikön kanssa.

Kaupunki julkaisee vuosittain tietotilinpäätöksen, jonka kaupunginhallitus hyväksyy.

Tietosuojasääntely koostuu tietosuoja-asetuksesta, kansallisesta tietosuojalaista sekä erityislainsäädännöstä. Suomessa tietosuojavaltuutetun toimisto valvoo tietosuojalainsäädännön noudattamista. Tietosuoja-asetuksessa (GDPR) on keskeisenä teemana tietosuojariskien hallinta ja rekisterinpitäjän tilintekokykyisyys-periaate. Osoitusvelvollisuuteen kuuluu mm. se, että organisaation sopimuksissa ja alihankinnoissa on huomioitu tietosuojan ja -turvan vaatimukset. Lisäksi rekisterinpitäjän tulee huomioida rekisteröidyn henkilötietojen käsittelyyn kohdistuvat riskit.

Tietotilinpäätös on käsitelty 14.03.2022 Laitilan kaupunginviraston johtoryhmässä sekä esitellään kaupunginhallitukselle tilinpäätöskäsittelyn 28.3.2022 yhteydessä.

Tietosuojapolitiikan soveltaminen ja tavoitteet

Tietosuojaan kuuluvat henkilöiden yksityiselämän suoja ja yksityisyyden suojaa turvaavat muut oikeudet henkilötietoja käsiteltäessä.

Suojaamistoimet koskevat kaikkien sähköisessä, kirjallisessa tai muussa muodossa olevien henkilötietojen käsittelyä, siirtoa ja säilytystä riippumatta siitä, onko tietoihin kohdistuva uhka tahallinen tai tahaton, esimerkiksi järjestelmän vikaantuminen, tapaturma tai luonnonkatastrofi.

Kaupungin luottamushenkilöt ja henkilökunta ovat sitoutuneet tietosuojan huomioivaan toimintaan ja toimivat tässä asiakirjassa julkaistujen periaatteiden mukaisesti.

Tietosuojapolitiikan avulla pyritään turvaamaan kunnan toiminta lainsäädännön mukaisesti. Tähän kuuluu olennaisesti henkilötietojen käyttöön liittyvät asiakkaiden, työntekijöiden ja muihin sidosryhmiin kuuluvien henkilöiden oikeudet sekä tietojen käsittelijän oikeuksien ja velvollisuuksien varmistaminen ja noudattaminen henkilötietoja käsiteltäessä.

Tietosuojaa toteutettaessa kiinnitetään erityistä huomiota henkilötietojen salassapitoon ja siihen, ettei asiattomilla ole pääsyä tietoihin ja ettei tietoja käytetä henkilöä vahingoittavasti.

2 Tietojen käsittelyyn vaikuttava lainsäädäntö

2.1 Tietosuojaa määritelevä keskeinen lainsäädäntö

- EU:n yleinen tietosuoja-asetus EU 679/2016
- Tietosuojalaki 5.12.2018/1050
- Tiedonhallintalaki (906/2019)
- Laki digitaalisten palvelujen tarjoamisesta 306/2019
- Laki sähköisestä asioinnista viranomaistoiminnassa 24.1.2003/13
- Euroopan parlamentin ja neuvoston verkko- ja tietoturvadirektiivi
- Laki yksityisyyden suojasta työelämässä (759/2004)
- Laki viranomaisten toiminnan julkisuudesta 21.5.1999/621

2.2 Tietosuoja lainsäädännön keskeiset muutokset

Julkisen hallinnon tiedonhallintalaki (906/2019) astui voimaan 1.1.2020. Tiedonhallintalain tarkoituksena on varmistaa viranomaisten tietoaineistojen yhdenmukainen ja laadukas hallinta ja tietoturvallinen käsittely. Lisäksi lailla mahdollistetaan tietoaineistojen turvallinen ja tehokas hyödyntäminen sekä edistetään tietojärjestelmien ja tietovarantojen yhteen toimivuutta. Tiedonhallintalain siirtymäsäännösten mukaan toinen siirtymäaika päättyy 1.1.2022 seuraaville lain kohdille:

- Asianhallinnan ja palvelujen tiedonhallinnan järjestäminen (26 ja 27§)
- Tietoaineistojen saataville saattaminen koneluettavassa muodossa (19,2§)
- Vastaanotettujen asiakirjojen muuttamien digitaaliseen muotoon (19,1§)
- Lokitietojen kerääminen tietojärjestelmien käytöstä (17§)

3 Tiedonhallinnan keskeiset muutokset 2021

1. Tiedonhallintalain ensimmäisen- ja toisen osan toimeenpano kuntaorganisaatiossa

   Kaupunki perusti tiedonhallintaryhmän ja tiedonhallintavastuut määriteltiin kaupunginhallituksessa 31.5.2021.
   Tiedonhallintamalli ja asiakirjajulkisuuskuvaukset hyväksyttiin kaupunginhallituksessa 22.11.2021.

   Tiedonhallintalain toisen osan keskeiset asiat ovat tietoaineistojen metatietojen hallinta, asiakirjojen sähköiseen muotoon muuttaminen ja tietojärjestelmissä olevien tietojen käytön ja luovutuksen seuranta sekä tietojärjestelmän teknisten virheiden selvittäminen lokitietojen avulla.

   Projektia koordinoi tiedonhallintaryhmä, mutta lain vaatimusten täytäntöönpano edellyttää toimia sen eri yksiköiltä. Tiedonhallintalain toisen osan täytäntöönpano jatkuu vuodelle 2022.

2. Koronaepidemian puhkeaminen keväällä 2020 muutti työskentelytapoja ja lisäsi huomattavasti etätyöskentelyä. Tietoturvalliseen etätyöskentelyyn kiinnitettiin entistä enemmän huomiota esimerkiksi lisäämällä koulutusta.

3. KuntaToimisto-ohjelmisto on päivitetty uuteen CaseM järjestelmään, joka on kaupungin toimialojen yhteiskäytössä oleva asianhallintajärjestelmä, jonka avulla hoidetaan vireille tulleiden asioiden kirjaaminen, käsittelyn seuranta, asioihin liittyvien sähköisten asiakirjojen sekä toimielin- ja viranhaltijapäätösten hallinta.

4 Rekisteröityjen oikeuksien toteutuminen

Rekisteröityjä informoidaan henkilötietojen käsittelystä kaupungin internet sivuilla olevilla tietosuojaselosteilla.
Rekisteröity voi käyttää oikeuksiaan toimittamalla pyynnön rekisterinpitäjälle ensisijaisesti tietojenpyyntölomakkeella tai vapaamuotoisella kirjeellä.
Tietosuojaselosteet ja tietopyyntölomakkeet löytyvät osoitteesta:
https://www.laitila.fi/hallinto-ja-paatoksenteko/tietosuoja/

Tällä hetkellä tietopyyntöprosessi toimii ainoastaan manuaalisesti.
Tietopyynnön voi toimittaa joko
1) postitse tietosuojaselosteessa mainitulle yhteyshenkilölle osoitettuna tai
2) asioimalla henkilökohtaisesti, jonka yhteydessä tarkistetaan rekisteröidyn henkilöllisyys.

Asiakas voi tulla noutamaan pyytämänsä tiedot kaupungin kirjaamosta. Tiedot voidaan toimittaa hänelle myös postitse.

Rekisteröidyiltä tulleiden pyyntöjen määrä 1.1.2021 – 31.12.2021 välisenä aikana.
• Sosiaali- ja terveystoimi
- esimiesten tai asiakkaiden pyynnöstä tehdyt lokiselvitykset 0
- tietopyynnöt 36 (25 kpl sosiaalitoimi, 11 kpl terveystoimi)

• Muut toimialat
- tietosuoja-asetuksen mukaiset tietopyynnöt yhteensä 14 kpl
- julkisuuslain mukaiset tietopyynnöt 77 kpl

5 Rekisterinpitäjän vastuut ja velvoitteet

5.1.1 Osoitusvelvollisuus

Tietosuoja-asetus velvoittaa kaupunkia osoittamaan noudattavansa tietosuoja-asetusta esimerkiksi dokumentoimalla henkilötietojen käsittelyyn liittyvät prosessit ja muut käytännön tietosuojatoimenpiteet. Osoitusvelvollisuus merkitsee käytännössä sitä, että vain riittävällä ja asianmukaisella dokumentaatiolla ja koulutuksella kunta voi osoittaa toimivansa asetuksen mukaisesti.

5.1.2 Käsittelyn oikeusperusta

Rekisterinpitäjän tulee huolehtia, että henkilötietoja käsitellään vain asianmukaisin edellytyksin ja määritellä ne tarkoitukset, joihin henkilötietoja käsitellään ja varmistua, ettei tietoja käsitellä muihin tarkoituksiin.
Asetuksen mukaan lainmukaisia käsittelyn edellytyksiä ovat muun muassa:
— Rekisteröidyn vapaaehtoinen ja informoitu suostumus. Rekisterinpitäjän velvollisuuksiin kuuluu pystyä osoittamaan jälkikäteen, että suostumus on annettu.
— Sellaisen sopimuksen täytäntöön paneminen, jossa rekisteröity on osapuolena.
— Rekisterinpitäjän lakisääteinen velvoite.

5.1.3 Tietosuojavastaava

Kaupungilla on nimettynä tietosuojavastaavat, joiden tehtävänkuvaan kuuluu seurata organisaation tietojenkäsittelyyn liittyviä toimintatapoja ja huolehtia, että ne vastaavat asetuksessa tai muualla erityislainsäädännössä säädettyä. He myös ohjaavat ja auttavat organisaatiota tietosuojaperiaatteiden ja vaatimusten toteuttamisessa. Lisäksi tietosuojavastaavat toimivat kontaktipisteenä sekä valvontaviranomaiseen että rekisteröityihin.

5.1.4 Sisäänrakennettu ja oletusarvoinen tietosuoja

Tietosuoja-asetuksen vaatimusten toteutuminen tulee taata määrittelyvaiheesta koko käsiteltävien henkilötietojen elinkaaren ajan. Jotta sisäänrakennetun ja oletusarvoisen tietosuojan velvollisuuksista voidaan huolehtia, pitää tietosuojavaatimukset analysoida ja toteuttaa aikaisessa vaiheessa. Käytännössä tämä tarkoittaa tietosuojan sisällyttämistä järjestelmien ja sovellusten hankintoihin sekä projektinhallintaan.

5.1.5 Ilmoitusvelvollisuus henkilötietojen tietoturvaloukkauksista

Rekisterinpitäjillä on velvollisuus ilmoittaa henkilötietojen tietoturvaloukkauksesta henkilökohtaisesti niille rekisteröidyille, joiden tietoja loukkaus koskettaa. Oikeus astuu voimaan, jos loukkaus todennäköisesti aiheuttaa suuren riskin yksilön oikeuksille ja vapauksille, esimerkiksi identiteettivarkauksien, maksuvälinepetosten tai muun rikollisen toiminnan muodossa.

6 Kaupungin tietovarannot ja keskeiset tunnusluvut

Koko kaupungin henkilötietoja sisältävien rekisterien määrä on 50.

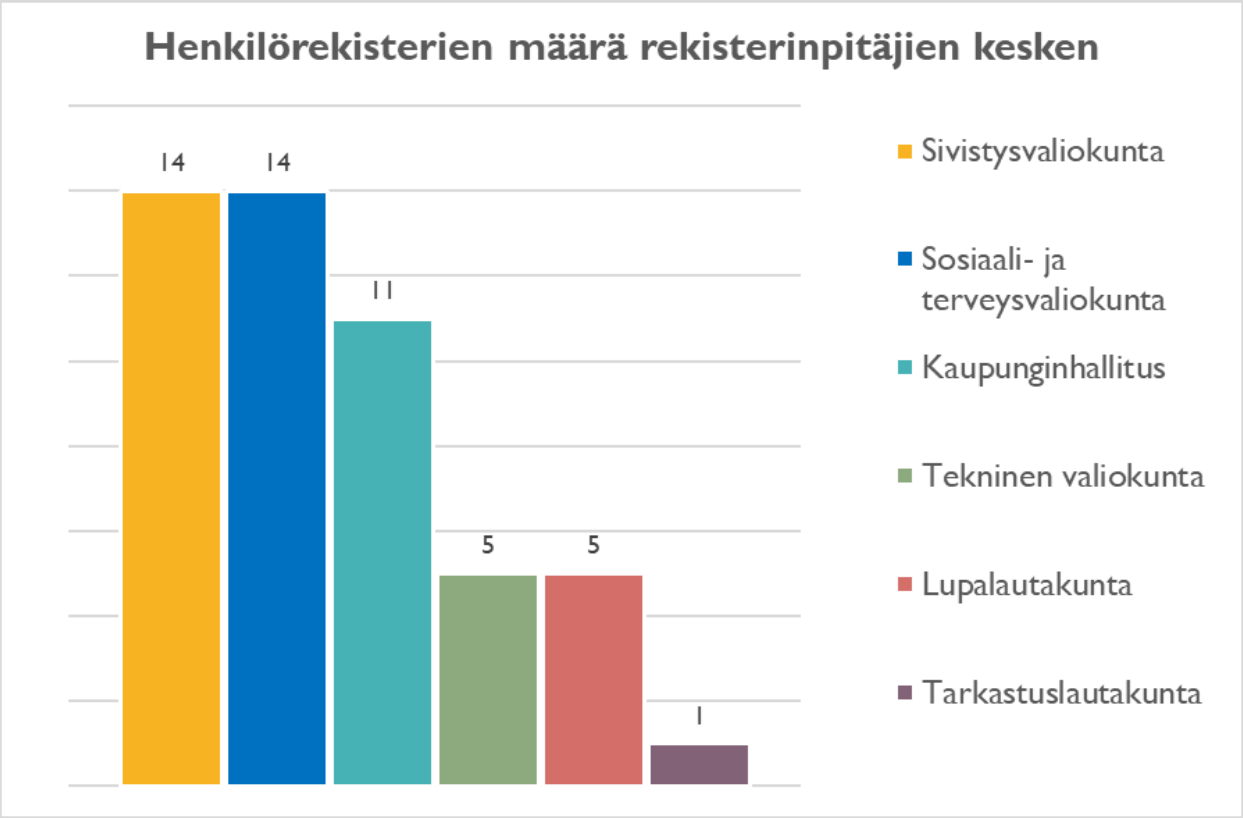
Kaupungin henkilötietoja sisältävät tietovarannot on jaettu kolmeen eri pääryhmään.

1. Rekisteröityjä koskevat lakisääteiset henkilörekisterit.
   Tämä ryhmä sisältää isoimman osat rekistereistä (35 kpl) ja kyseiset rekisterit jakautuvat useammalle kaupungin toimialalle.
2. Rekisteröityjä koskevat rekisteröidyn suostumukseen perustuvat henkilörekisterit.
   Näitä rekistereistä kunnassa on (9 kpl) ja kyseiset rekisterit jakautuvat useammalle kaupungin toimialalle.
3. Kaupungin henkilökuntaa koskevat rekisterit.
   Näitä rekistereistä kaupungilla on (6 kpl) ja kyseiset rekisterit jakautuvat useammalle kaupungin toimialalle.

7 Tiedon hallinta

7.1 Vastuun jakautuminen kunnassa

Laitilan kaupungilla on yhteensä 50 rekisteriä, jotka sisältävät henkilötietoja. Rekisterinpitäjän vastuu henkilörekistereistä jakautuu kaupunginhallituksen, valiokuntien ja lautakuntien välillä seuraavasti:



7.2 Dokumentaatio ja koulutus

Kaupungilla on laadittuna tietosuojakäsikirja, jota päivitetään säännöllisesti tietosuojavastaavan toimesta. Käsikirja sisältää esimerkiksi kaupungin tietosuojapolitiikan, rekisterikuvaukset, kriisiviestinnän ohjeet, tietosuojaselosteet ja tietosuojavastaavan tehtävänkuvan.

Kaupungin uudet työntekijät perehdytetään kunnan tietosuojakäytänteisiin koulutuksella. Kaupungissa palveluksessa työskenteleville työntekijöille järjestetään tarpeen mukaan lisäkoulutusta.

Kaupunki järjesti keväällä 2021 koko henkilökunnalle suunnatun tietosuojankertauskoulutuksen ja syksyllä 2021 järjestettiin opettajille kohdennettu tietosuojakoulutus.

7.3 Rekisterinpitäjän ja -käsittelijän väliset sopimukset

Henkilötietojen käsittelijä on taho, joka käsittelee henkilötietoja rekisterinpitäjän (kaupungin) lukuun ja rekisterinpitäjän määrittelemien ohjeiden mukaisesti. Rekisterinpitäjän ja -käsittelijän välisellä sopimuksella varmistetaan, että käsittelijä käsittelee henkilötietoja ainoastaan sopimuksessa sovittujen ehtojen mukaisesti.

8 Tietosuojauksen periaatteet

Tietoturvallisuuden keskeinen ohjausdokumentti on kaupungin tietosuojakäsikirja, jossa on kuvattu muun muassa vastuut, tietosuojavastaavan rooli, henkilörekisterit tietosuojaselosteineen, toimintaympäristö, rekisteröidyn oikeuksien toteuttaminen ja rekisterinpitäjän sopimusasiat.

Kaupungin toiminnassa pyritään siihen, että käsiteltävät dokumentit ovat tarpeen mukaan saatavilla ja niiden eheys on kunnossa.

Kaupunki informoi henkilöstöään tietosuojaan liittyvistä ajankohtaisista asioista joka toinen viikko ilmestyvällä tietosuojavastaavan uutiskirjeellä

8.1 Suurimmat uhkatekijät

Erilaiset käyttäjätunnuksien kalastelu viestit pysyivät myös vuoden 2021 yhtenä suurimpana jatkuvana uhkana.

Etätyöskentely on johtanut siihen, että yhä useampi laite toimii etäyhteyksin ja työntekijä joutuu ottamaan suurempaa vastuuta tietoturvan ja tietosuojan osalta. Työntekijöiden ohjeistus tietosuojasta ja tietoturvasta huolehtimiseen onkin etätöissä tärkeämpää kuin koskaan.

Riskien osalta yhtenä haavoittuvuutena on poikkeamat, jotka johtunut inhimillisestä virheestä joko järjestelmäasetuksissa, prosessissa tai yksittäisen henkilön työtehtävissä.

8.2 Tapahtuneet tietoturvaloukkaukset

Tietosuojaloukkauksia, jotka ovat vaatineet raportointia tietosuojavaltuutetun toimistolle on tapahtunut vuoden 2021 aikana yhteensä 4 kpl. Näistä kahdessa tapauksessa tehtiin myös ilmoitus poliisille.

1. Anonyymisti palautettujen lomakkeiden ohjeiden vastainen käsittely (SOTE)
2. Koulun O365 oppilastilin hakkerointi
3. Koulun Wilma tunnusten hakkerointi
4. Palkanlaskuun liittyvien tietojen hakkerointi (tietomurto tapahtui tietojenkäsittelijän taholla)

Vähäisempiä tietosuojaloukkauksia, joista on kirjattu tietosuojarikkomus, on tapahtunut vuoden 2021 aikana yhteensä 5 kpl.

1. Henkilötietoja sisältävien lomakkeiden jakaminen vääriin osoitteisiin
2. Henkilötietoja sisältävien viranhaltijapäätösten jakaminen vääriin osoitteisiin
3. Office 365 Käyttäjätunnusten päätyminen vääriin käsiin
4. Työntekijän henkilötietojen lähettäminen väärälle taholle
5. Työvuorosuunnittelun listassa oli julkaistuna listaan kuulumattomia henkilötietoja

9 Kehittämiskohteet ja keskeisimmät muutokset vuonna 2022

Vuoden 2022 kehittämiskohteiksi on tunnistettu seuraavat osa-alueet:

- SOTE-alueisiin liittyvän tiedon kerääminen alkoi loppuvuonna 2021 ja jatkuu 2022. SOTE-alueisiin liittyvä tiedonkeruu on koskenut esim. henkilöstöä, irtaimistoa ja sopimuksia ja kerättävää tietoa on suuri määrä.

-Tietosuojan vaikutustenarviointien tekeminen (DPIA Data Protection Impact Assessment) on tietosuoja-asetuksen vaatimus. Tietosuoja-asetuksen mukaisesti rekisterinpitäjän tulee tietyissä tilanteissa tehdä vaikutustenarviointi, joka on osa henkilötietojen käsittelyn riskiperusteista lähestymistapaa ja toisaalta tukee osoitusvelvollisuuden toteutumista.

-Julkisen hallinnon tiedonhallintalaki (906/2019) astui voimaan 1.1.2020. Tiedonhallintalain tarkoituksena on varmistaa viranomaisten tietoaineistojen yhdenmukainen ja laadukas hallinta ja tietoturvallinen käsittely. Lisäksi lailla mahdollistetaan tietoaineistojen turvallinen ja tehokas hyödyntäminen sekä edistetään tietojärjestelmien ja tietovarantojen yhteen toimivuutta.
Tiedonhallintalain siirtymäsäännösten mukaan siirtymäaika päättyy 1.1.2022 seuraaville lain kohdille:

- Asianhallinnan ja palvelujen tiedonhallinnan järjestäminen (26 ja 27§)
- Tietoaineistojen saataville saattaminen koneluettavassa muodossa (19,2§)
- Vastaanotettujen asiakirjojen muuttamien digitaaliseen muotoon (19,1§)
- Lokitietojen kerääminen tietojärjestelmien käytöstä (17§)

- Varautuminen tietomurtoja ja kyberiskuja vastaan. Tiedonhallintalain siirtymäsäännösten mukaan kolmas siirtymäaika päättyy 1.1.2023, johon mennessä on saatettava tietoturvallisuusvaatimukset (12 -17§) lain vaatimalle tasolle.

-Jatkuvana kehittämiskohteena henkilöstökoulutukset ja tietoisuuden kasvattaminen painopisteenä henkilöstön tietoturva- ja tietosuojatietoisuuden ja osaamisen kasvattaminen.

10 2021 määriteltyjen kehittämiskohteiden tilannekatsaus

Viime vuoden tietotilinpäätöksessä, 2020 kehittämiskohteiksi listattiin 5 osa-aluetta, joista alla listaus toteutuneine toimenpiteineen:

1. Henkilöstökoulutukset ja tietoisuuden kasvattaminen painopisteenä henkilöstön tietoturva- ja tietosuojatietoisuuden ja osaamisen kasvattaminen.
   - Kaupunki järjesti keväällä 2021 koko henkilökunnalle suunnatun tietosuojankertauskoulutuksen ja syksyllä 2021 järjestettiin opettajille kohdennettu tietosuojakoulutus.

2. Järjestelmien kirjautumissivun turvallisuutta parannetaan, esimerkiksi estämään niin sanottujen kalasteluviestien läpimeno.
   - Kaupunki päivitti 2021 kirjautumissivut tietoturvallisemmaksi.

3. Kaupungin riskienhallinnan osalta yhdeksi tehtäväksi 2021 jäi tietojen säilyvyyden varmistus.
    - Tietojen säilyvyyttä parannettiin uusimalla toinen varmuuskopiointipalvelimista, jossa on enemmän levykapasiteettia ja siten mahdollisuus säilyttää tietoja pidempään. Toisen varmuuskopiointipalvelimen osalta laitteen korjaustakuu ulkoistettiin 3. osapuolelle ja varmistusaikatauluja muutettiin siten, että palautus pidemmälle aikavälille on mahdollista. Palvelimen uusimisen ajankohta on vielä auki.

4. Rekisterinpitäjän (Kaupunki) ja käsittelijöiden välisten sopimusten läpikäyminen ja päivittäminen kaikkien kaupungin toimialojen osalta.
    - Tämä tehtävä on siirretty vuodelle 2022

5. Uusien luottamushenkilöiden tietoisuuden lisääminen ja kouluttaminen tietosuojan- ja tietoturvan osalta.
    - Tietosuojaan ja tietoturvaan liittyvää ohjeistusta tullaan lisäämään vuoden 2022 aikana.