Laitila

LAITILAN KAUPUNGIN
TIETOTILINPÄÄTÖS
2023

Sisällys

1 Tietotilinpäätöksen tarkoitus

Tietotilinpäätöksen tavoitteena on rakentaa 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. Julkaistavalla tietotilinpäätöksellä halutaan lisätä johdon, luottamushenkilöiden, henkilöstön ja suuren yleisön tietoisuutta tietosuojasta ja tietoturvasta sekä saada näkyvyyttä näiden asioiden eteen tehdystä työstä.

Tietotilinpäätöksen laatiminen ja julkaisu on linjassa tietosuojavaltuutetun suositusten kanssa, joiden mukaan tietotilinpäätöksen laatiminen on yksi tapa toteuttaa tietosuojalainsäädännön edellyttämää rekisterinpitäjän osoitusvelvollisuutta. Osoitusvelvollisuus tarkoittaa sitä, että organisaation pitää pystyä osoittamaan noudattavansa tietosuoja-asetusta henkilötietojen käsittelyssä sekä toteuttavansa tietosuojaperiaatteita myös käytännössä.

Tämä tietotilinpäätös on Laitilan kaupungin kuudes tietotilinpäätös. Tietotilinpäätöksen koonnista vastaa kaupungin tietosuojavastaava yhdessä tietopalvelu- ja työhyvinvointipäällikön kanssa.

Kaupunki julkaisee vuosittain tietotilinpäätöksen, jonka kaupunginhallitus hyväksyy.

Tietotilinpäätös on käsitelty 11.3.2024 Laitilan kaupunginviraston johtoryhmässä sekä esitellään kaupunginhallitukselle tilinpäätöskäsittelyn 25.3.2024 yhteydessä ja vastaavasti kaupunginvaltuustolle 10.6.2024.

Tietosuojan toteuttaminen

Tietosuojan toteuttaminen edellyttää jatkuvaa tietosuojaseikkojen huomioimista sekä koko organisaation läpäisevää tietosuojakulttuuria. Käytännön toteutuksen kannalta ensisijaisen tärkeää on johdon tuki tietosuojan edistämisessä.

Kaupungin luottamushenkilöt ja henkilökunta ovat sitoutuneet tietosuojan huomioivaan toimintaan ja noudattamaan tietosuojalain mukaisia tietosuojaperiaatteita, jonka mukaan henkilötietoja on:

- käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi
- käsiteltävä luottamuksellisesti ja turvallisesti
- kerättävä ja käsiteltävä tiettyä, nimenomaista ja laillista tarkoitusta varten
- kerättävä vain tarpeellinen määrä henkilötietojen käsittelyn tarkoitukseen nähden
- päivitettävä aina tarvittaessa
- epätarkat ja virheelliset henkilötiedot on poistettava tai oikaistava viipymättä
- säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin
- on tarpeen tietojenkäsittelyn tarkoitusten toteutumista varten.

2 Tietojen käsittelyyn vaikuttava lainsäädäntö

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.

2.1 Tietosuojaa määritelevä keskeinen lainsäädäntö

- Perustuslaki (731/1999)
- Kuntalaki (410/2015)
- Hallintolaki (434/2003)
- Laki julkisen hallinnon tiedonhallinnasta (906/2019)
- EU:n yleinen tietosuoja-asetus EU 679/2016
- Tietosuojalaki 5.12.2018/1050
- Tiedonhallintalaki (906/2019)
- Arkistolaki (831/1994)
- 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
- Työsopimuslaki (55/2001)
- Rikoslaki (39/1889)

Lisäksi on olemassa runsaasti toimialakohtaista erityislainsäädäntöä, joissa tietojen käsittelyä on säädelty.

2.2 Tietosuojaan liittyvän lainsäädännön keskeiset muutokset

Laki julkisen hallinnon tiedonhallinnasta (906/2019) astui voimaan 1.1.2020.
Yleislakina tiedonhallintalaki sisältää koko julkista hallintoa koskevat säännökset tiedonhallinnan järjestämisestä ja kuvaamisesta, tietovarantojen yhteen toimivuudesta, teknisten rajapintojen ja katseluyhteyksien toteuttamisesta sekä tietoturvallisuuden toteuttamisesta.
Tiedonhallintalain siirtymäsäännösten mukaan neljäs siirtymäaika päättyy 31.12.2023 seuraaville lain kohdille:

- Tietojen luovuttaminen teknisen rajapinnan avulla viranomaisten välillä (22 §)
- Katseluyhteyden avaaminen viranomaiselle (23§)
- Tietoaineistojen luovuttaminen teknisen rajapinnan avulla muille kuin viranomaisille (24§)

Muutokset tietosuojalakiin ja rikosasioiden tietosuojalakiin tulivat voimaan 1.1.2024.
Muutoksessa selkeytetään henkilötunnuksen käsittelyä koskevaa sääntelyä. Henkilön tunnistamiseen ei saa käyttää yksinomaan henkilötunnusta tai henkilötunnuksen ja rekisteröidyn nimen yhdistelmää.

3 Keskeiset toimenpiteet 2023

1. Laitilassa automatisoitiin tiedonkulkua uusien ja poistuvien työntekijöiden osalta vuoden 2023 aikana. Tämä selkeytti käyttäjätunnusten hallintaa, ja tällä varmistetaan esimerkiksi ohjelmistojen käyttöoikeuksien poistaminen, kun henkilön työ- tai virkasuhde Laitilassa päättyy. Lisäksi uusissa (ja osittain myös käytössä olleissa) järjestelmissä alettiin hyödyntämään ns. kertakirjautumista, jolloin erillisistä tunnus- ja salasanapari-kirjautumisista päästiin eroon.

   Nämä toimenpiteet liittyvät tiedonhallintalain kohtiin

   - Luotettavuutta edellyttävien tehtävien tunnistaminen ja luotettavuudesta varmistuminen (12§)
   - Tietojärjestelmien käyttöoikeuksien hallinta (16§)

2. Vastuu sosiaali- ja terveydenhuollon ja pelastustoimen järjestämisestä siirtyi 1.1.2023 Varsinais-Suomen hyvinvointialueelle (Varha). Siirron myötä Laitilan kaupungilta poistui 16 henkilörekisteriä.
   Potilastietojärjestelmiä siirrettiin Varhalle vielä vuoden 2023 kevään aikana (Aura, Proconsona). Samoin SOTE-käytössä olleet leasing-laitteet siirrettiin useammassa erässä Varhalle, viimeiset siirrot olivat alkusyksyllä 2023.
   Varhalle siirtyneiden työntekijöiden laitila.fi-sähköpostit puolestaan lopetettiin keväällä. Henkilöstöhallinnan palkkaohjelmasta (Personec F2) luovutettiin henkilötietoja (mm. nimi, hetu, tehtävänimike, palkka, kokemuslisä, henkilökohtaiset lisät, esihenkilö, työyksikkö) hyvin-vointialueella liikkeen luovutuksen periaattein siirtyvästä henkilöstöstä.

3. Ison haasteen 2023 aiheutti opiskeluhuollon järjestämisen kannalta välttämättömien tietojen luovuttaminen Varhalle, mikä pitkälti johtui kansallisen ohjeistuksen puutteesta. Oppilas- ja opiskelijahuollon tietojen luovuttaminen tai käyttöoikeuksien antaminen mm. Wilmaan nousivat puheenaiheeksi valtakunnallisesti. Käytännön ratkaisut olivat eriäviä kuntien kesken, tämä aiheutti hämmennystä ja epätietoisuutta aina marraskuulle 2023 saakka, jolloin OPH julkaisi ohjeistusta liittyen tietojen luovutukseen koulutuksesta opiskeluhuoltopalveluille. Ohjeistus selvensi käytänteitä, mutta ei poistanut epäselvyyksiä kaikilta osin.

4. Tietosuoja-asetuksen 35. artikla velvoittaa tekemään vaikutuksenarvioinnit (PIA/DPIA) ja ennakkokuulemiset sellaisille prosesseille, joissa henkilötietojen käsittelyyn liittyy riskejä. Kansallinen tietosuojavaltuutetun toimisto on julkaissut vuonna 2021 viralliset ohjeistukset ja työkalut vaikutuksenarvioinnin tekemiseen. 2023 alkuvuodesta valmistui Ilmoituskanavan vaikutuksenarviointi ja sitä päivitetään tarpeen mukaan.

4 Rekisteröityjen oikeuksien toteutuminen

EU:n yleinen tietosuoja-asetus sisältää useita artikloja, jotka säätävät rekisteröidylle kuuluvia oikeuksia henkilötietojen käsittelyyn liittyen. Tietosuoja-asetuksen mukaan rekisteröidyllä on oikeus:

- saada tietoa henkilötietojensa käsittelystä
- saada pääsy henkilötietoihin
- oikaista henkilötietoja
- poistaa henkilötietoja
- rajoittaa henkilötietojen käsittelyä
- siirtää henkilötiedot järjestelmästä toiseen
- vastustaa henkilötietojen käsittelyä
- olla joutumatta automaattisen päätöksenteon kohteeksi

Rekisteröityjen informointi on toteutettu kaupungin internet-sivuilla löytyvien tietosuojaselosteiden avulla.

Rekisteröity voi käyttää oikeuksiaan toimittamalla pyynnön rekisterinpitäjälle ensisijaisesti tietojenpyyntö lomakkeella, vapaamuotoisella sähköpostilla tai asioimalla henkilökohtaisesti.

Tietosuojaselosteet ja tietopyyntölomakkeet löytyvät osoitteesta:
https://www.laitila.fi/hallinto-ja-paatoksenteko/tietosuoja/

Jos rekisteröity esittää pyynnön sähköisesti, tiedot toimitetaan yleisesti käytetyssä sähköisessä muodossa, paitsi jos rekisteröity toisin pyytää. Asiakas voi tulla noutamaan pyytämänsä tiedot kaupungin virastolta. Tiedot voidaan toimittaa hänelle myös postitse.
Ennen tietojen luovutusta, tietosuojaoikeuksiaan käyttävän rekisteröidyn henkilöllisyys on pystyttävä vahvistamaan.

Kaupungin vastaanottamien tietopyyntöjen määrä 1.1.2023 – 31.12.2023 välisenä aikana.
Kaikki toimialat yhteensä

- tietosuoja-asetuksen mukaiset tietopyynnöt yhteensä 24 kpl
- julkisuuslain mukaiset tietopyynnöt 107 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

Tietosuojalainsäädäntö edellyttää, että henkilötietojen käsittelylle on aina nimetty oikeusperusta. Rekisterinpitäjän tulee huolehtia, että henkilötietoja käsitellään vain asianmukaisin edellytyksin ja että tietojenkäsittelyn tarkoitus määritellään jo ennen kuin tietoja ryhdytään käsittelemään.

Tietosuoja-asetuksessa on kuusi eri perustetta, joilla henkilötietojen käsittely on mahdollista:

- rekisteröidyn suostumus
- sopimus
- rekisterinpitäjän lakisääteinen velvoite
- elintärkeiden etujen suojaaminen
- yleistä etua koskeva tehtävä tai julkinen valta
- rekisterinpitäjän tai kolmannen osapuolen oikeutettu etu.

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 alkaen koko käsiteltävien henkilötietojen elinkaaren ajan. Jotta sisäänrakennetun ja oletusarvoisen tietosuojan velvollisuuksista voidaan huolehtia, kaupungin on toteutettava asianmukaiset tekniset ja organisatoriset toimenpiteet, joilla varmistetaan, että oletusarvoisesti käsitellään vain käsittelyn kunkin erityisen tarkoituksen kannalta tarpeellisia henkilötietoja. Tämä velvollisuus koskee kerättyjen henkilötietojen määriä, käsittelyn laajuutta, säilytysaikaa ja saatavilla oloa. Näiden toimenpiteiden avulla on varmistettava etenkin se, että henkilötietoja oletusarvoisesti ei saateta rajoittamattoman henkilömäärän saataville ilman luonnollisen henkilön myötävaikutusta.

5.1.5 Ilmoitusvelvollisuus henkilötietojen tietoturvaloukkauksista

Henkilötietojen tietoturvaloukkauksella tarkoitetaan tapahtumaa, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu, henkilötietoja luovutetaan luvattomasti tai niihin pääsee käsiksi taho, jolla ei ole käsittelyoikeutta.

Kaupunki tekee ilmoituksen henkilötietojen tietoturvaloukkauksesta tietosuojavaltuutetun toimistolle, jos loukkauksesta voi aiheutua riski luonnollisten henkilöiden oikeuksille ja vapauksille. Henkilötietojen tietoturvaloukkauksesta on ilmoitettava tietosuojavaltuutetun toimistolle ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa siitä, kun rekisterinpitäjä on tullut tietoiseksi tietoturvaloukkauksesta.

Kaupungin tulee ilmoittaa rekisteröidylle, jos hänen henkilötietonsa ovat vuotaneet ulkopuolisille luvattomasti. Ilmoitus on tehtävä, jos tietoturvaloukkaus todennäköisesti aiheuttaa suuren riskin yksilön oikeuksille ja vapauksille. Kunnan on tällöin ilmoitettava asiasta ilman aiheetonta viivytystä, jotta rekisteröidyllä on mahdollisuus suojautua mahdollisia tapauksesta koituvia uhkia vastaan.

6 Kaupungin henkilötietorekisterit ja keskeiset tunnusluvut

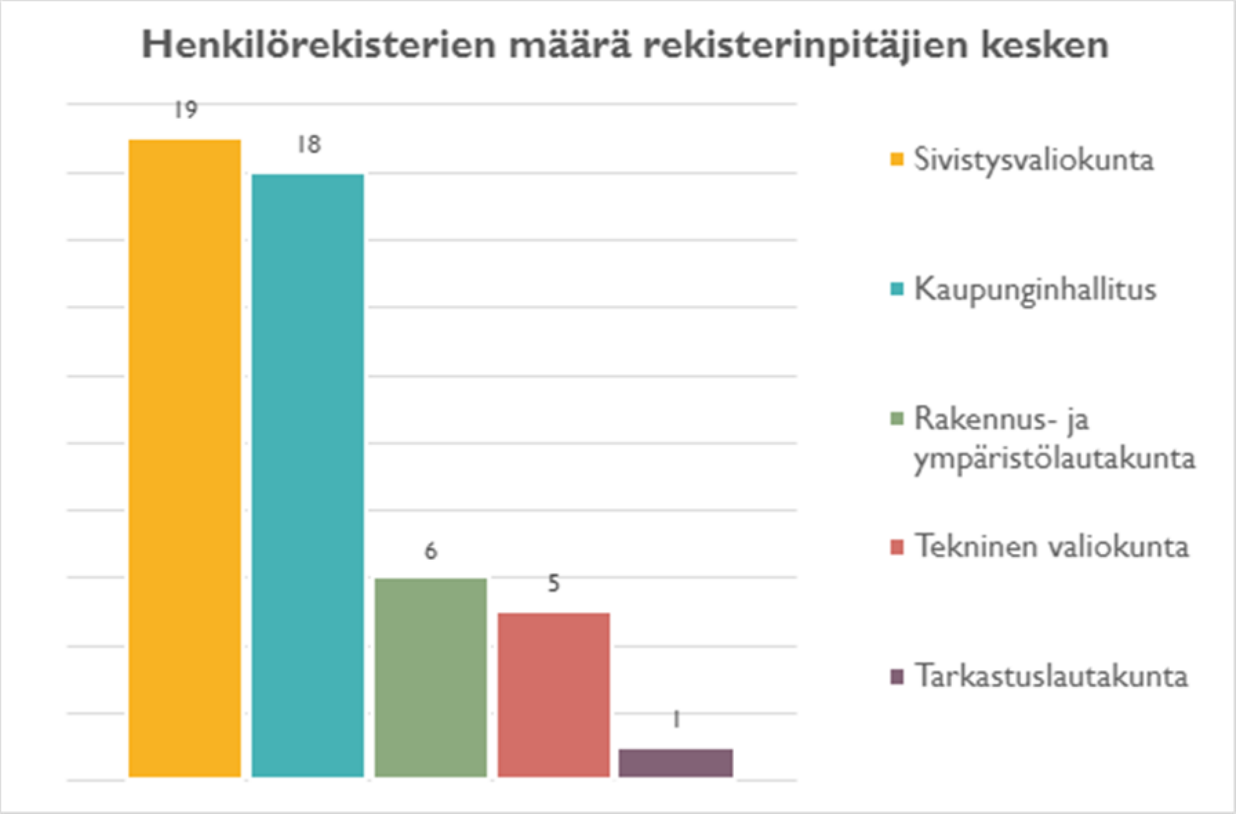
Koko kaupungin henkilötietoja sisältävien rekisterien määrä on 49.

Kaupungin henkilötietoja sisältävät tietovarannot on jaettu kolmeen eri pääryhmään.

1. Rekisteröityjä koskevat lakisääteiset henkilörekisterit.
   Tämä ryhmä sisältää isoimman osat rekistereistä (36 kpl) ja kyseiset rekisterit jakautuvat useammalle kaupungin toimialalle.
2. Rekisteröidyn suostumukseen perustuvat henkilörekisterit.
   Näitä rekistereistä kunnassa on (8 kpl) ja kyseiset rekisterit jakautuvat useammalle kaupungin toimialalle.
3. Kaupungin henkilökuntaa koskevat rekisterit.
   Näitä rekistereistä kaupungilla on (5 kpl) ja kyseiset rekisterit jakautuvat useammalle kaupungin toimialalle.

6.1 Kaupungin rekisterinpitäjät

Rekisterivastuut jakautuvat kaupunginhallituksen, valiokuntien ja lautakuntien välillä seuraavasti:



Kukin rekisterinpitäjä huolehtii henkilötietojen käsittelystä EU:n tietosuoja-asetuksen ja lainsäädännön vaatimusten mukaisesti. Lisäksi kaupunginhallitus velvoittaa kaikkia rekisterinpitäjiä huolehti maan tarvittavasta tietosuojakoulutuksesta ja -ohjeistuksesta.

7 Tiedon hallinta

Tiedonhallinnalla tarkoitetaan viranomaisen tehtävien hoidossa tai sen muussa toiminnassa syntyviin tarpeisiin perustuvia toimia ja tietoturvallisuustoimenpiteitä viranomaimen tietoaineistojen, niiden käsittelyvaiheiden ja tietoaineistoihin sisältyvien tietojen hallinnoimiseksi riippumatta tietoaineistojen tallentamistavasta ja muista käsittelytavoista. Laitilassa tiedonhallintaa kuvataan ja ohjataan tiedonhallintalain vaatimusten mukaisella tiedonhallintamallilla, tiedonohjaussuunnitelmalla sekä asiakirjajulkisuuskuvauksella.

7.1 Tiedonhallintamalli ja tiedonohjaussuunnitelma

Tiedonhallintamallissamme kuvataan tiedonhallintayksikön eli Laitilan kaupungin toiminta, tietopääoma ja tietojärjestelmät.

Tiedonohjaussuunnitelmassamme kuvaamme kaupungin tehtävät ja käsittelyprosessit, tehtävien hoidossa syntyvän asiakirjallisen tiedon ohjaus- ja hallintaperiaatteet sekä tietojen säilytysajat.

Tiedonhallintamallin ja tiedonohjaussuunnitelman ylläpito on jatkuva prosessi, jota päivitetään tehtävien muuttuessa.

7.2 Asiakirjajulkisuuskuvaus

Asiakirjajulkisuuskuvauksemme antaa yleiskuvan tiedonhallinnasta ja siitä, miten ja missä laajuudessa keräämme ja käsittelemme tietoja lakisääteisissä tehtävissämme. Asiakirja julkisuuskuvaus toteuttaa julkisuusperiaatetta. Tavoitteena on auttaa asiakasta kohdistamaan tietopyyntönsä ja yksilöimään tietopyynnön sekä opastaa tietoaineistojen omatoimisessa haussa ja käytössä.
Asiakirjajulkisuuskuvaus on saatavilla https://www.laitila.fi/hallinto-ja-paatoksenteko/asiakirjajulkisuuskuvaus/

7.3 Keskeiset tietojärjestelmät

Kaupungilla on sekä keskitettyjä koko konsernin tietojärjestelmiä että toimialakohtaisia järjestelmiä, joista keskeisimmät ovat:

- CaseM – asianhallintajärjestelmä
- Personec F2 - henkilöstöhallinto
- Intime Plus – taloushallinto
- Cloudia – sopimustenhallinta
- Clausion Cloud -konserniohjelma
- Targetor Pro - riskienhallinnan ohjelmisto
- Hedsam Novitas - kulunvalvonta- ja työajanseuranta
- Microsoft 365 – toimisto työkalut
- MultiPrimus/Wilma – oppilastietojen hallintajärjestelmä
- Google Workspace for Educations – sähköinen oppimisympäristö
- Daisy – varhaiskasvatuksen hallintajärjestelmä
- Koha - kirjaston asiakasjärjestelmä
- PARrent = etsivä nuorisotyön asiakasjärjestelmä
- Timmi – varausjärjestelmä
- Facta – paikkatietojärjestelmä

- Kuntanet7 – Rakennusvalvonta
- Trimple - sähköinen lupa-asiointipalvelu
- Vesikanta plus – Vesihuollon asiakkaat
- Basware InvoiceReady – ostolaskujen kierrätys- ja matkalaskuohjelma

8 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 2023 joulukuussa koko henkilökunnalle suunnatun tietoturvan ja tietosuojan kertauskoulutuksen. Koulutuksen tavoite oli perustiedon jakaminen ja osaamisen kasvattaminen.

Yleisen tietosuojakoulutuksen lisäksi Tietosuojavastaava julkaisee henkilöstölle joka toinen viikko ilmestyvän uutiskirjeen intranetissä.

9 Rekisterinpitäjän ja -käsittelijän väliset sopimukset

Tietosuoja-asetus asettaa velvoitteita sopimusehtojen kannalta, lähtökohdaksi on otettava asetuksen asettama velvollisuus sopia henkilötietojen käsittelystä sopimuksella, kun joku muu (kuten kaupungin palveluntuottaja) käsittelee tietoja rekisterinpitäjän (kaupunki) puolesta. Se kohdistuu sekä rekisterinpitäjään että henkilötietojen käsittelijään. Tietosuoja-asetuksessa säädetään sopimisvelvoitteen lisäksi tietosuojaa koskevan sopimuksen minimisisältö eli ne kohdat, joista ainakin tulee sopia.

Rekisterinpitäjän ja -käsittelijän välisellä sopimuksella (DPA) varmistetaan, että käsittelijä käsittelee henkilötietoja ainoastaan sopimuksessa sovittujen ehtojen mukaisesti.

10 Tietosuojauksen periaatteet

Laitilan kaupunki suhtautuu asiakkaidensa tietojen suojaamiseen sekä tietoturvaan vakavasti.

Tiedon luottamuksellisuus, virheettömyys ja käytettävyys varmistetaan huolellisella käsittelyllä. Henkilötiedot suojataan asianmukaisia teknisiä ja organisatorisia suojakeinoja käyttämällä. Tällaisia keinoja ovat muun muassa palomuurien, salaustekniikoiden ja turvallisten laitetilojen sekä kulunvalvonnan ja turvallisuusjärjestelmien käyttö. Suojakeinoja ovat lisäksi hallittu käyttöoikeuksien myöntäminen ja seuranta, henkilötietojen käsittelyyn osallistuvan henkilöstön osaamisen varmistaminen sekä alihankkijoiden huolellinen valinta.

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

10.1 Suurimmat uhkatekijät

Helmikuussa 2024 nähtiin Suomessa joukko palvelunestohyökkäyksiä, joiden kohteina olivat kotimaiset organisaatiot. Totutusta poiketen mukana oli uusia kohteita esimerkiksi kunta- ja koulutussektorilta. Palvelunestohyökkäykset eivät yleensä riko mitään, mutta kunnan verkkosivusto voi olla hetkellisesti saavuttamattomissa. Kunnan tulee huomioida tämä uusi kuntiin kohdistuva uhka ja varautua palvelunestohyökkäyksiin.

Erilaiset käyttäjätunnuksien kalastelu viestit tulevat pysymään myös vuoden 2024 yhtenä suurimpana jatkuvana uhkana. Uhkaa lisää rikollisten lisääntyvä tekoälyn käyttö, jota voidaan käyttää hyökkäysten automatisointiin ja vakuuttavampien phishing-kampanjoiden luomiseen.

Etätyöskentely on tullut jäädäkseen, vaikka huippulukemat ovatkin jo takanapäin. Rikolliset kohdistavat hyökkäyksiään etätyöinfrastruktuureihin hyödyntämällä VPN:ien ja pilvipalveluiden haavoittuvuuksia. Tyypillisesti nämä hyökkäykset johtavat luvattomaan pääsyyn arkaluonteisiin yritysverkkoihin ja -tietoihin ja toimivat siten ransomware-hyökkäysten ensimmäisinä vaiheina. Työntekijöiden ohjeistus tietosuojasta ja tietoturvasta huolehtimiseen tulee pysymään tärkeässä roolissa.

Laitilan kaupunki on myös kriittisen infrastruktuurin toimija ja siten alttiina myös sellaiselle häirinnälle ja hyökkäyksille, joiden taustalla on taloudellisten motiivien lisäksi mahdollisesti geopoliittiset konfliktit tai poliittiset motiivit.

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

10.2 Tapahtuneet tietoturvaloukkaukset

Vuoden 2023 aikana ei tapahtunut yhtään tietosuojaloukkausta, joka olisi vaatinut raportointia tietosuojavaltuutetun toimistolle.

Vuoden 2023 aikana tapahtui yksi tietosuojarikkomusta, josta on laadittu sisäinen tietosuojarikkomus dokumentti.

11 Kehittämiskohteet ja keskeisimmät muutokset vuonna 2024

Vuoden 2024 kehittämiskohteiksi on tunnistettu seuraavat osa-alueet:

1. Järjestelmien salassapidon ja suojattavuuden määrittelyn tulee jatkua kuluvan vuoden aikana. Järjestelmien omistajien tulee olla tietoisia järjestelmänsä tietosisällön tärkeydestä ja niistä toimista, joilla osoitetaan niiden olevan riittävästi suojattu. Lisäksi henkilökunnan tulee olla riittävästi koulutettu tietojen turvalliseen käsittelyyn.

2. Kaupungin kotisivujen uusinta aloitettiin syksyllä 2023. Tarkoituksena oli uudistaa täysin Laitilan kaupungin nykyiset, teknisesti ja osittain myös sisällöllisesti vanhentuneet kotisivut. Uuden kotisivuston toimittajaksi valikoitui Poutapilvi Oy ja ne rakennetaan WordPress-julkaisualustalle, joka

tarjoaa paremmat työkalut sisällönhallintaan ja monipuolisemmat toiminnallisuudet kuntalaisnäkökulmasta katsoen. Lisäksi uusien sivujen saavutettavuus on paremmin varmistettu. Sivusto on tarkoitus julkaista vuoden 2024 alkupuoliskon aikana.

3. Sähköisen pysyväisarkistointiohjelman käyttöönotto aloitettiin keväällä.

4. TE-palvelut 2024-uudistus, jossa työllisyyspalvelut siirtyvät kuntien hoidettaviksi uudistuksen sisällön mukaisesti 1.1.2025 lukien. Tämä uudistus tuo tullessaan merkittäviä tiedonhallinnan kysymyksiä.

5. Kaupunki seuraa NIS2-direktiivin kansallista toteutusta. Julkishallinnon osalta soveltamisalaan kuulumista tullaan tarkentamaan tiedonhallintalaissa. NIS2-direktiivi on EU:n laajuinen kyberturvallisuutta koskeva lainsäädäntö. Siinä esimerkiksi kiinnitetään huomiota hallinnolliseen tietoturvaan sekä organisaation tietoturvakäytäntöihin ja politiikoihin, kuten kunnan henkilökunnalle suunnattuihin tietoturvaohjeistuksiin ja käytäntöihin. NIS2-direktiivin soveltaminen alkaa 18.10.2024.

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

12 2023 määriteltyjen kehittämiskohteiden tilannekatsaus

Viime vuoden tietotilinpäätöksessä, 2023 kehittämiskohteiksi listattiin 3 osa-aluetta, joista alla listaus toteutuneine toimenpiteineen:

1. Henkilöstökoulutukset ja tietoisuuden kasvattaminen painopisteenä henkilöstön tietoturva- ja tietosuojatietoisuuden ja osaamisen kasvattaminen.
   - Kaupunki järjesti joulukuussa 2023 koko henkilökunnalle suunnatun tietoturvan- ja tietosuojan kertauskoulutuksen.

2. Windows serverien päivitys uudempaan käyttöjärjestelmäversioon ennen kuin Microsoftin tuki niissä päättyy, jotta pystytään varmistamaan ohjelmistojen tietoturvallisuus ja päivitysten piirissä pysyminen.
   - Tuen piiristä poistuneet Windows Server 2012 -palvelimet päivitettiin osittain uudempaan käyttöjärjestelmäversioon ja osittain palvelimilla olleet palvelut siirrettiin toisille palvelimille.

3. Kalasteluviestit ja muut kirjautumiseen liittyvät uhat ovat kasvaneet, ja tämän vuoksi kaupunki vahvistaa kirjautumiskäytäntöjä ja yhtenä toimena on monivaiheisen kirjautumisen (MFA) yleisimpi käyttöönotto.
   - Monivaiheisen kirjautumisen käyttöönotto on toteutettu vaiheittain ja viimeiset käyttöönotot saadaan valmiiksi vuoden 2024 aikana.