Laitila

LAITILAN KAUPUNGIN
TIETOTILINPÄÄTÖS
2024

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 henkilöstö- ja tietopalveluasiantuntijan kanssa.

Kaupunki julkaisee vuosittain tietotilinpäätöksen, jonka kaupunginhallitus hyväksyy.

Tietotilinpäätös on käsitelty 17.3.2025 Laitilan kaupunginviraston johtoryhmässä sekä esitellään kaupunginhallitukselle tilinpäätöskäsittelyn yhteydessä 31.3.2025 ja vastaavasti kaupunginvaltuustolle 19.5.2025.

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 Tietosuoja-asioiden vastuunjako

2.1 Kaupunginhallitus

Hallintosäännön 8 luvun 1 §:n 5-kohdan mukaisesti kunnanhallitus vastaa siitä, että kunta täyttää tietosuojalainsäädännön velvoitteet ja valvoo niiden toteutumista.

2.2 Tietosuojavastaava

Tietosuoja-asetus velvoittaa kaikkia julkishallintoon kuuluvia organisaatioita nimittämään tietosuojavastaavan. Tietosuojavastaavan tehtäviin kuuluu organisaation neuvonta ja ohjaus kaikissa tietosuojakysymyksissä, tietosuoja-asetuksen noudattamisen valvonta mukaan lukien tähän liittyvät tarkastukset, yhteistyö valvontaviranomaisen kanssa ja rekisteröityjen oikeuksien toteuttamisen tukeminen.

2.3 Tietosuojaa koskevat vastuut toimialaloilla

Jokainen toimiala vastaa siitä, että tietosuoja- ja turva-asiat hoidetaan asetusten ja lakien mukaisesti omalla toimialla.

Esimiehet vastaavat siitä, että heidän alaisillaan on riittävä osaaminen, mahdollisuus riittävään koulutuksiin, ohjeistus ja asianmukaiset työkalut tietoturvan ja tietosuojan mukaiseen tietojenkäsittelyyn. Heidän tehtävänään on valvoa tietoturvan ja tietosuojan toteutumista omalla toimialallaan ja raportoida tietosuojan vaarantumiset sekä poikkeamat periaatteista tai ohjeistuksesta.

2.4 Tietoturva- ja tietosuojaryhmä

Kaupungin tietosuoja ja –tietoturvatyöryhmänä toimii johtoryhmä. Johtoryhmä käsittelee yleisiä ja koordinointia vaativia tietosuojaan, tietoturvaan, tiedonhallintaan, riskienhallintaan ja varautumiseen liittyviä asioita. Tarvittaessa johtoryhmän kokouksiin osallistuu tietohallintopäällikkö, tietosuojavastaava ja tarpeen mukaan muita asiantuntijoita eri toimialoilta. Tarvittaessa asiat viedään päätettäväksi ja hyväksyttäväksi kaupunginhallitukselle tai valiokuntiin.

2.5 Ulkoistetut kunnan ICT- palvelut

Kunnan tietohallinto vastaa yhdessä toimialojen ja ulkopuolisten järjestelmätoimittajien kanssa tietojärjestelmien toipumis-, varautumis- ja valmiussuunnitelmista.

3 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.

3.1 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.

3.2 Tietosuojaan liittyvän lainsäädännön keskeiset muutokset 2024

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.

Euroopan unionin verkko- ja tietoturvadirektiivi eli NIS2-direktiivi astui EU:ssa voimaan 14.12.2023. Hallituksen esitys HE 57/2024 eduskunnalle kyberturvallisuusdirektiivin (NIS 2 -direktiivi) täytäntöönpanoa koskevaksi lainsäädännöksi on vielä kesken. Hallituksen esityksen perusteella vaikutukset koskevat useita kansallisia lakeja, joista keskeisimpinä ovat uusi kyber-turvallisuuslaki sekä uusi tiedonhallintalain (906/2019) 4 a luku.

4 Keskeiset toimenpiteet 2024

1. Julkisten työvoimapalveluiden järjestämisvastuu siirtyi valtiolta kuntien muodostamille työllisyysalueille vuoden 2025 alusta. Laitilan kaupunki kuuluu Turun työllisyysalueeseen. Työnhakijoiden, työttömien ja muiden työvoimapalveluja tarvitsevien palvelut tuottaa lähipalveluna Laitilan kaupungin työllisyyspalvelut. Laitilan kaupungissa toimii työllisyysohjaajan asiointipäivystys. Palvelussa käytössä olevasta Työmarkkinatori järjestelmästä vastaa KEHA-keskus.

2. Tietosuoja-asetuksen 35. artikla velvoittaa tekemään vaikutuksenarvioinnit (DPIA) sellaisille prosesseille, joissa henkilötietojen käsittelyä todennäköisesti aiheuttaa korkean riskin henkilöiden oikeuksille ja vapauksille. 2024 alkuvuodesta valmistui tietosuojanvaikutuksenarviointi oppilaitosten käyttämään Google Workspace for Education ympäristöön.

3. Kaupunki otti käyttöön pilvipohjaisen tietoturvakoulutus järjestelmän. Nimblr- yrityksen toimittama järjestelmä perustuu käytännön harjoituksiin ja tietoturva uhkiin liittyvään ajankohtaiseen koulutus sisältöön.

4. Talouspalvelut ja sivistystoimi ottivat käyttöön uuden sähköisen arkistointi järjestelmän, joka helpottaa asiakirjojen arkistointia, arkistoitujen asiakirjojen hyödyntämistä sekä arkiston elinkaaren hallintaa.

5. Kaupunki otti käyttöön uuden työajanseuranta järjestelmän.

6. Tekninen toimi vaihtoi asiointipalvelussa olleen lupa- ja hakemusasia järjestelmän. Uusi järjestelmä pitää sisällään perinteisen kartantuotannon lisäksi kaavoituksen, ympäristön valvonnan, infraomaisuuden ja rakennusvalvonnan toimintokokonaisuudet.

5 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/tietosuoja

Rekisteröidyn pyyntöön vastaus toimitetaan ensisijaisesti sähköisessä muodossa. Rekisteröity voi myös noutaa pyytämänsä tiedot kaupungin virastolta tai tiedot voidaan toimittaa hänelle postitse. Asiakkaan henkilöllisyys varmennetaan ennen tietojen luovuttamista.

Kaupungin vastaanottamien tietopyyntöjen määrä 1.1.2024 – 31.12.2024 välisenä aikana.
Kaikki toimialat yhteensä

- tietosuoja-asetuksen mukaiset tietopyynnöt yhteensä 13 kpl
- julkisuuslain mukaiset tietopyynnöt 186 kpl

6 Rekisterinpitäjän vastuut ja velvoitteet

6.1.1 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.

6.1.2 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.

6.1.3 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.

6.1.4 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.

6.1.5 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. Tapauksen niin vaatiessa ilmoitus tehdään myös kyberturvallisuuskeskukselle ja poliisille.

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.

7 Kaupungin henkilötietorekisterit ja keskeiset tunnusluvut

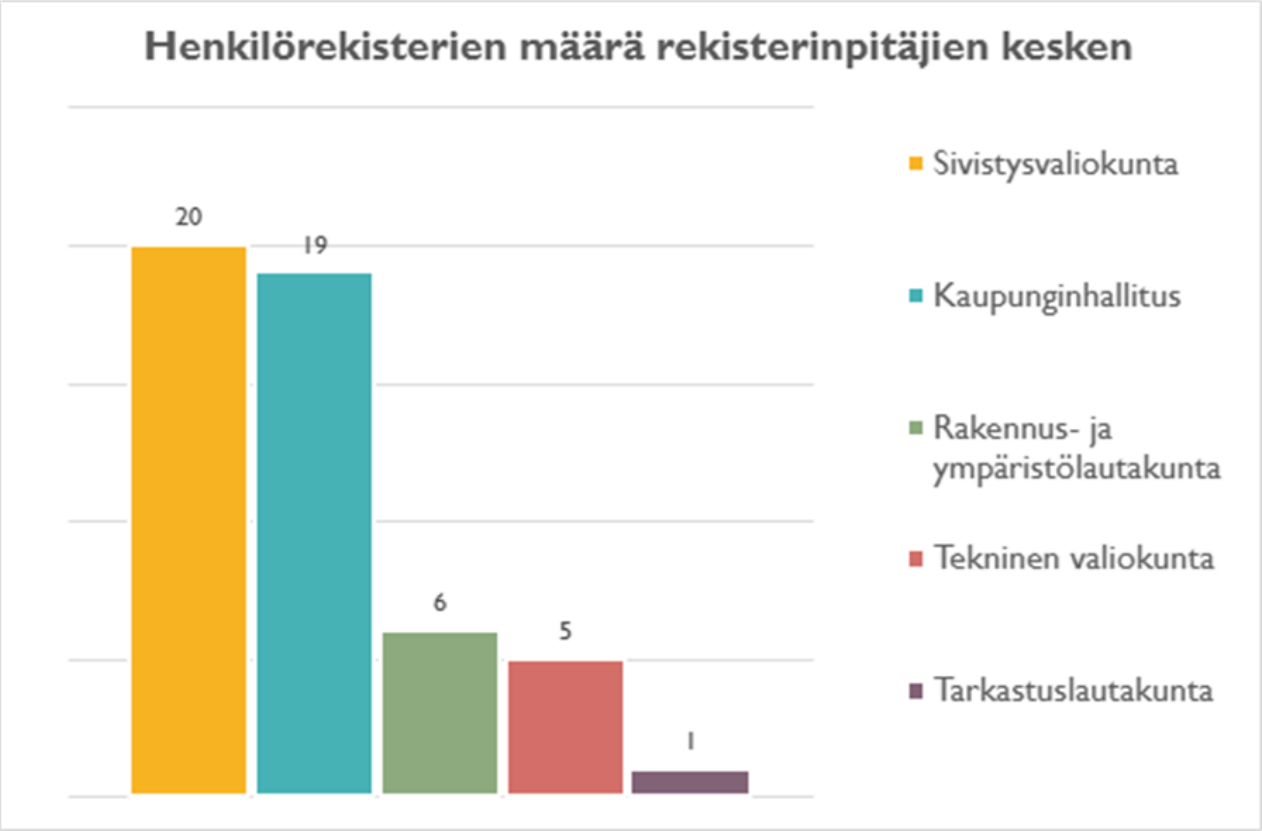
Koko kaupungin henkilötietoja sisältävien rekisterien määrä on 51.

Kaupungin henkilötietoja sisältävät tietovarannot on jaettu kolmeen eri pääryhmään.

1. Kuntalaisten tietoja sisältäviä lakisääteisiä henkilötietorekistereitä kaupungilla on 38 kappaletta.
2. Kuntalaisten tietoja sisältäviä rekisteröidyn suostumukseen perustuvia henkilötietorekistereitä kaupungilla on 8 kappaletta.
3. Kaupungin henkilökuntaa koskevia henkilötietorekistereitä kaupungilla on 5 kappaletta.

7.1 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.

8 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.

8.1 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.

8.2 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 osoitteessa https://www.laitila.fi/tietosuoja

8.3 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
- Promid – kulunvalvonta- ja työajanseuranta
- Microsoft 365 – toimisto työkalut
- MultiPrimus/Wilma – oppilastietojen hallintajärjestelmä
- Google Workspace for Educations – sähköinen oppimisympäristö
- Daisy – varhaiskasvatuksen hallintajärjestelmä
- Hellevi – kansalaisopiston oppilashallintaohjelma
- Eepos – musiikkiopiston oppilashallintaohjelma
- Koha – kirjaston asiakasjärjestelmä
- PARrent – etsivä nuorisotyön asiakasjärjestelmä
- Timmi – varausjärjestelmä

- Trimble Locus Cloud – Kuntatieto- ja sähköinen asiointijärjestelmä
- Vesikanta plus – Vesihuollon asiakkaat
- Basware InvoiceReady – ostolaskujen kierrätys- ja matkalaskuohjelma
- DataCycle360 – sähköinen pitkäaikaisarkistointi
- Nimblr – henkilöstön tietoturvakoulutus

9 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.

Kaupungilla on käytössä pilvipohjainen tietoturvakoulutus järjestelmä. Nimblr yrityksen toimittama järjestelmä perustuu käytännön harjoituksiin ja tietoturva uhkiin liittyvään ajankohtaiseen koulutus sisältöön. Käyttäjät saavat sähköpostitse ilmoituksia uusista, n. 3-5 minuutin mittaisista mikrokoulutuksista, jotka liittyvät esim. tietojenkalasteluun, haittaohjelmiin ja verkossa toimimiseen. Kurssit ovat interaktiivisia ja niitä ne suoritetaan selaimessa tietokoneella tai mobiililaitteella. Lisäksi järjestelmä lähettää simuloituja hyökkäyksiä käyttäjille sähköpostitse ja mikäli käyttäjä erehtyy klikkaamaan viestin linkkiä, liitettä tms., ohjautuu hän verkkosivulle, jossa kerrotaan käyttäjän klikanneen haitallista sisältöä ja hänelle tarjotaan aiheeseen liittyvää kurssia suoritettavaksi. Järjestelmä arvioi käyttäjien osaamistasoa suoritettujen kurssien ja klikattujen simulaatioiden perusteella ja tietohallinto seuraa näitä tietoja.

Kaupungilla on käytössä lisäksi Eduhouse-koulutuspalvelu, jossa henkilöstön on mahdollista oma-aloitteisesti suorittaa eri koulutuskokonaisuuksia. Koulutuspalvelu toimii selaimella ja palvelusta löytyy tietosuojaan liittyviä koulutuksia, niin koko henkilöstölle tarkoitettuja kuin myös toimialakohtaisia (esim. henkilöstöhallinto, varhaiskasvatus). Myös näitä koulutussuoritteita seurataan.

Yleisen tietosuojakoulutuksen lisäksi Tietosuojavastaava julkaisee henkilöstölle joka toinen viikko ilmestyvän uutiskirjeen kunnan intranetissä. Uutiskirjeissä on mm. ajankohtaisia tietosuojaan ja –turvaan liittyviä asioita ja vastauksia kunnissa esiin tulleisiin konkreettisiin kysymyksiin.

10 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.

11 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.

11.1 Suurimmat uhkatekijät

Käyttäjätunnuksien kalasteluun tähtäävien viestine määrä on edelleen kasvanut. Tavat, joilla käyttäjätunnuksia yritetään saada haltuun ovat monipuolistuneet ja huijausviestejä tulee sähköpostien, sosiaalisenmedian ja puheluiden kautta. Uhkaa lisää rikollisten lisääntyvä tekoälyn käyttö, jota voidaan käyttää hyökkäysten automatisointiin ja vakuuttavampien kalastelukampanjoiden luomiseen.

Helmikuussa 2024 nähtiin Suomessa joukko palvelunestohyökkäyksiä, joiden kohteina olivat kotimaiset organisaatiot. Totutusta poiketen mukana oli uusia kohteita esimerkiksi kunta- ja koulutussektorilta. Palvelunestohyökkäykset saattavat hidastaa tai väliaikaisesti estää sähköisten palveluiden käytön. Kaupungin tulee huomioida tämä uusi kuntiin kohdistuva uhka ja varautua palvelunestohyökkäyksiin.

Verkon reunalla sijaitsevien laitteiden haavoittuvuudet, puutteet prosesseissa ja konfiguraatiovirheet altistavat organisaatiot hyökkääjille. Rikolliset havaitsevat ja hyödyntävät haavoittuvuuksia yhä nopeammin. Esimerkiksi etätyön mahdollistava VPN-ratkaisu on yksi kriittisimmistä palveluista, joka kiinnostaa myös rikollisia. Tärkeää onkin huolehtia näiden laitteidentietoturvasta ja pitää päivitykset ajan tasalla.

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.

11.2 Tapahtuneet tietoturvaloukkaukset

Vuoden 2024 aikana tapahtui kaksi tietosuojaloukkausta, joista tehtiin ilmoitus tietosuojavaltuutetun toimistolle.

Vuoden 2024 aikana tapahtui yksi tietosuojarikkomusta, josta on laadittu sisäinen tietosuojarikkomus dokumentti.

12 Kehittämiskohteet ja keskeisimmät muutokset vuonna 2025

Vuoden 2025 kehittämiskohteiksi on tunnistettu seuraavat osa-alueet:

1. Tiedonhallinnan osa-alueiden kehittäminen. Painopisteinä ovat metatietojen oikeellisuus, tietojen säilytysajat ja tiedonhallintalain tietoturvallisuuden vähimmäisvaatimukset.
2. Monivaiheisen tunnistautumisen käyttöönoton laajentaminen järjestelmissä, jotka tätä toimintoa tukevat.
3. Kaupunki seuraa NIS2-direktiivin kansallista toteutusta. Hallituksen esityksen ja Kuntaliiton asiantuntijalausunnon mukaan kaupungin ei kriittiset toiminnot ovat rajattu direktiivissä julkishallinnon ulkopuolelle. NIS2-direktiivi tulee vaikuttamaan hallituksen esityksen perusteella kansallisesti useihin lakeihin, joista keskeisimpinä ovat uusi kyberturvallisuuslaki sekä uusi tiedonhallintalain (906/2019) 4 a luku.
4. Jatkuvana kehittämiskohteena henkilöstökoulutukset ja tietoisuuden kasvattaminen painopisteenä henkilöstön tietoturva- ja tietosuojatietoisuuden ja osaamisen kasvattaminen.

13 2024 määriteltyjen kehittämiskohteiden tilannekatsaus

Viime vuoden tietotilinpäätöksessä, 2024 kehittämiskohteiksi listattiin 4 osa-aluetta.

Toimenpiteet, jotka tehtiin kehittämiskohteiden osalta, olivat seuraavat:

1. Kaupungin uudet kotisivut julkaistiin maaliskuussa 2024.
2. Talouspalvelut ja sivistystoimi ottivat käyttöön uuden sähköisenarkistointijärjestelmän.
3. Tietoturva- ja tietosuojatietoisuuden ja osaamisen kasvattamisen edistämiseksi kaupunki otti käyttöön pilvipohjaisen tietoturvakoulutus järjestelmän. Nimblr yrityksen toimittama järjestelmä perustuu käytännön harjoituksiin ja tietoturva uhkiin liittyvään ajankohtaiseen koulutus sisältöön. Tämän lisäksi käyttöön otettiin Eduhouse-koulutuspalvelu, jossa henkilöstön on mahdollista oma-aloitteisesti suorittaa eri koulutuskokonaisuuksia.
4. Monivaiheisen tunnistautumisen käyttöönotto on toteutettu vaiheittain ja kaikilla kaupungintyöntekijöillä on nyt mahdollisuus ottaa monivaiheinen tunnistautuminen käyttöön.