



Laitila

LAITILAN KAUPUNGIN
TIETOTILINPÄÄTÖS

2025

Sisällys

Sisällys	1
1 Tietotilinpäätöksen tarkoitus.....	2
2 Tietosuoja-asioiden vastuunjako	3
2.1 Kaupunginhallitus.....	3
2.2 Tietosuojavastaava.....	3
2.3 Tietosuoja koskevat vastuut toimialoilla.....	3
2.4 Tietoturva- ja tietosuojaryhmä	3
2.5 Ulkoistetut kunnan ICT- palvelut.....	3
3 Tietojen käsittelyyn vaikuttava lainsäädäntö.....	4
3.1 Tietosuoja määrittelevä keskeinen lainsäädäntö	4
3.2 Tietoturvaa määrittelevä lainsäädäntö	4
3.3 Tietosuojaan liittyvän lainsäädännön keskeiset muutokset 2025	4
4 Keskeiset toimenpiteet 2025	5
5 Rekisteröityjen oikeuksien toteutuminen.....	5
6 Rekisterinpitäjän vastuut ja velvoitteet	6
6.1.1 Osoitusvelvollisuus	6
6.1.2 Käsittelyn oikeusperusta	6
6.1.3 Tietosuojavastaava	6
6.1.4 Sisäänrakennettu ja oletusarvoinen tietosuoja	7
6.1.5 Ilmoitusvelvollisuus henkilötietojen tietoturvaloukkauksista.....	7
7 Kaupungin henkilötietorekisterit ja keskeiset tunnusluvut	8
7.1 Kaupungin rekisterinpitäjät	8
8 Tiedon hallinta	9
8.1 Tiedonhallintamalli ja tiedonohjaussuunnitelma	9
8.2 Asiakirjajulkisuuskuvaus.....	9
8.3 Keskeiset tietojärjestelmät.....	9
9 Dokumentaatio ja koulutus.....	10
10 Rekisterinpitäjän ja -käsittelijän väliset sopimukset	10
11 Tietoturvan periaatteet.....	11
11.1 Suurimmat uhkatekijät.....	11
11.2 Tapahtuneet tietoturvaloukkaukset.....	11
12 Kehittämiskohteet ja keskeisimmät muutokset vuonna 2026.....	12
13 2025 määriteltyjen kehittämiskohteiden tilannekatsaus	12

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 seitsemäs tietotilinpäätös. Tietotilinpäätöksen koonnista vastaa kaupungin tietosuojavastaava yhdessä henkilöstö- ja tietopalveluasiantuntijan kanssa. Tietotilinpäätöksen hyväksyy kaupunginhallitus.

Vuosittain laadittavasta tietotilinpäätöksestä on linjattu kaupungin tietosuojapolitiikassa. Tietotilinpäätös täydentää tilinpäätökseen ja toimintakertomukseen kuuluvaa raportointia, sekä toimii johdon työvälineenä.

Tietotilinpäätös on käsitelty 16.03.2026 Laitilan kaupunginviraston johtoryhmässä sekä esitellään kaupunginhallitukselle tilinpäätöskäsittelyn yhteydessä 30.03.2026 ja vastaavasti kaupunginvaltuustolle 15.06.2026.

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

kaupunginhallituksen tulee kuntalain 39 §n mukaan vastata kunnan hallinnosta ja taloudenhoidosta sekä huolehtia sisäisestä valvonnasta ja riskienhallinnan järjestämisestä. Kaupunginhallituksen yleisestä hallinnon johtamisvastuusta seuraa valvontavelvoite myös siitä, että kunnassa henkilötietojen käsittely on lainmukaisessa kunnossa. Tämä sisältää vastuun tietosuojaa koskevien toimintaperiaatteiden täytännönpäätöksen ja tarvittavien teknisten ja organisatoristen toimenpiteiden toteuttamisesta.

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 toimialoilla

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

Esihenkilöt vastaavat siitä, että henkilöstöllä on riittävä osaaminen, mahdollisuus riittävään koulutukseen, ohjeistus ja asianmukaiset työkalut tietoturvan ja tietosuojan mukaiseen tietojenkäsittelyyn. Heidän tehtävänä on valvoa tietoturvan ja tietosuojan toteutumista omalla toimialallaan ja raportoida tietosuojan vaarantumiset sekä poikkeamat periaatteista tai ohjeistuksesta.

Henkilöstö ja luottamushenkilöt vastaavat omalta osaltaan tietosuojan toteutumisesta tehtävissään. Henkilöstön ja luottamushenkilöiden velvollisuutena on toimia annettujen ohjeiden mukaisesti sekä ylläpitää ja kehittää osaamistaan sekä raportoida havaitsemistaan epäkohdista.

2.4 Tietoturva- ja tietosuojaryhmä

Kaupungin tietosuoja ja -tietoturvatyöryhmänä toimii johtoryhmä. Johtoryhmä käsittelee yleisiä ja koordinoivia vaatimia 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 valiokuntaan.

2.5 Ulkoistetut kunnan ICT- palvelut

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

3 Tietojen käsittelyyn vaikuttava lainsäädäntö

Tietosuojasääntely koostuu tietosuoja-asetuksesta, kansallisesta tietosuoja-laista sekä erityislainsäädännöstä. Suomessa tietosuojavaaltuutetun toimisto valvoo tietosujalainsäädännön 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 määrittelevä 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
- Tietosujalaki 5.12.2018/1050
- Tiedonhallintalaki (906/2019)
- Arkistolaki (831/1994)
- Laki digitaalisten palvelujen tarjoamisesta 306/2019
- Laki sähköisestä asiointista 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)

Näiden lisäksi tiedonhallintaa ohjaa ja velvoittaa myös kunnan eri toimintoja koskeva erityislainsäädäntö.

3.2 Tietoturvaa määrittelevä lainsäädäntö

Vuonna 2019 voimaan tullut tiedonhallintalaki (laki julkisen hallinnon tiedonhallinnasta 906/2019) on yksi keskeisemmistä laista, joka säätelee tietoturvan toteuttamisen toimenpiteistä kunnissa. Tiedonhallintalain 4 luku (pykälät 12–18) sisältävät ensisijaiset tietoturvallisuutta koskevat vaatimukset. Tietoturvallisuustoimenpiteillä tarkoitetaan tietoa-aineistojen saatavuuden, eheyden ja luottamuksellisuuden varmistamista hallinnollisilla, toiminnallisilla ja teknisillä toimenpiteillä.

3.3 Tietosuojaan liittyvän lainsäädännön keskeiset muutokset 2025

Kansallinen kyberturvallisuuslaki 124/2025, jolla toimeenpannaan, NIS2-direktiivi on tullut voimaan 8.4.2025. Suomen kansallisessa toimeenpanosäätelyssä paikallistaso eli kunnat on jätetty julkinen hallinto toimialan ulkopuolelle, eikä NIS2-sääntely koske siten peruskunnan kuten Laitilan toimintaa.

4 Keskeiset toimenpiteet 2025

1. Kaupungin tiedonhallintamallin rakeenteellinen päivitys. Päivityksessä keskityttiin tuomaan paremmin esille ohjelmistojen tietoturvaan, tietoaineistojen metatietoihin ja vastuunjakoon liittyviä asioita.
2. Kaupungin tiedonohjaussuunnitelman päivitys. Päivityksessä huomioitiin tiedonhallintalautakunnan antamat suositukset tietoaineistojen säilytysajoista.
3. Sähköisen pitkäaikaissäilytys- järjestelmän integraatiot opetuksen ja varhaiskasvatuksen järjestelmiin aloitettiin, tämä helpottaa säilytyksessä olevien asiakirjojen hyödyntämistä, elinkaaren hallintaa ja tietoaineistojen arkistoon siirtämistä.
4. Työllisyyspalveluiden vaatimien ohjelmistojen käyttöönotto ja tietoaineistojen tietoturvallisen käsittelyn toteuttaminen.
5. Talous- ohjelmistojen uusimiseen tähtäävän projektin aloitus.
6. Windows 10 ja Office 2016/2019 ohjelmistojen päivitys uusimpiin versioihin.

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.

Rekisteröidyllä on oikeuksia liittyen omiin henkilötietoihinsa ja niiden käsittelyyn. Rekisteröidyllä on muun muassa oikeus tietää, käsitelläänkö hänen henkilötietojaan ja mitä henkilötietoja käsitellään sekä pyytää häntä koskevat tiedot itselleen. Lisäksi rekisteröidyllä on oikeus vaatia virheelliset henkilötiedot oikaistavaksi. Muita rekisteröidyn oikeuksia sovelletaan eri tavoin riippuen siitä, mikä on henkilötietojen käsittelyn oikeusperuste. Esimerkiksi oikeutta tietojen poistamiseen ei sovelleta laakisääteisiin rekistereihin.

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 1.1.2025 – 31.12.2025 välisenä aikana.

Kaikki toimialat yhteensä

- tietosuoja-asetuksen mukaiset tietopyynnot yhteensä 19 kpl
- julkisuuslain mukaiset tietopyynnot 185 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 nimetty tietosuojavastaava, jonka tehtävät ja asema on määritelty tietosuoja-asetuksessa (37–39 artiklat). Tietosuojavastaavan nimenomaisiin tehtäviin kuuluu:

- Antaa tietoja ja neuvoja organisaation sisällä tietosuojalainsäädännön noudattamisesta.
- Seurata henkilötietojen käsittelyyn liittyvien vaatimusten sekä organisaation menettelytapojen noudattamista (mukaan lukien vastuunjako, tietoisuuden lisääminen ja käsittelyyn osallistuvan henkilöstön koulutus sekä tähän liittyvät tarkastukset).
- Antaa pyydettyä neuvoja tietosuojan vaikutustenarvioinnin tekemisestä ja valvoa sen toteutusta.
- Tehdä yhteistyötä tietosuojavaikuttetun toimiston kanssa sekä toimia yhteyspisteenä käsittelyyn liittyvissä kysymyksissä.

- Raportoida suoraan organisaation ylimmälle johdolle. Kunnan tulee sisäisesti määritellä raportointivelvollisuudelle selkeät prosessit.

Tietosuojavastaava ei ole henkilökohtaisesti vastuussa tietosuoja-asetuksen rikkomisesta, vaan tietosuojalainsäädännön noudattaminen on rekisterinpitäjän vastuulla.

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 tietosuojavaikuttetun toimistolle, jos loukkauksesta voi aiheutua riski luonnollisten henkilöiden oikeuksille ja vapauksille. Henkilötietojen tietoturvaloukkauksesta on ilmoitettava tietosuojavaikuttetun 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

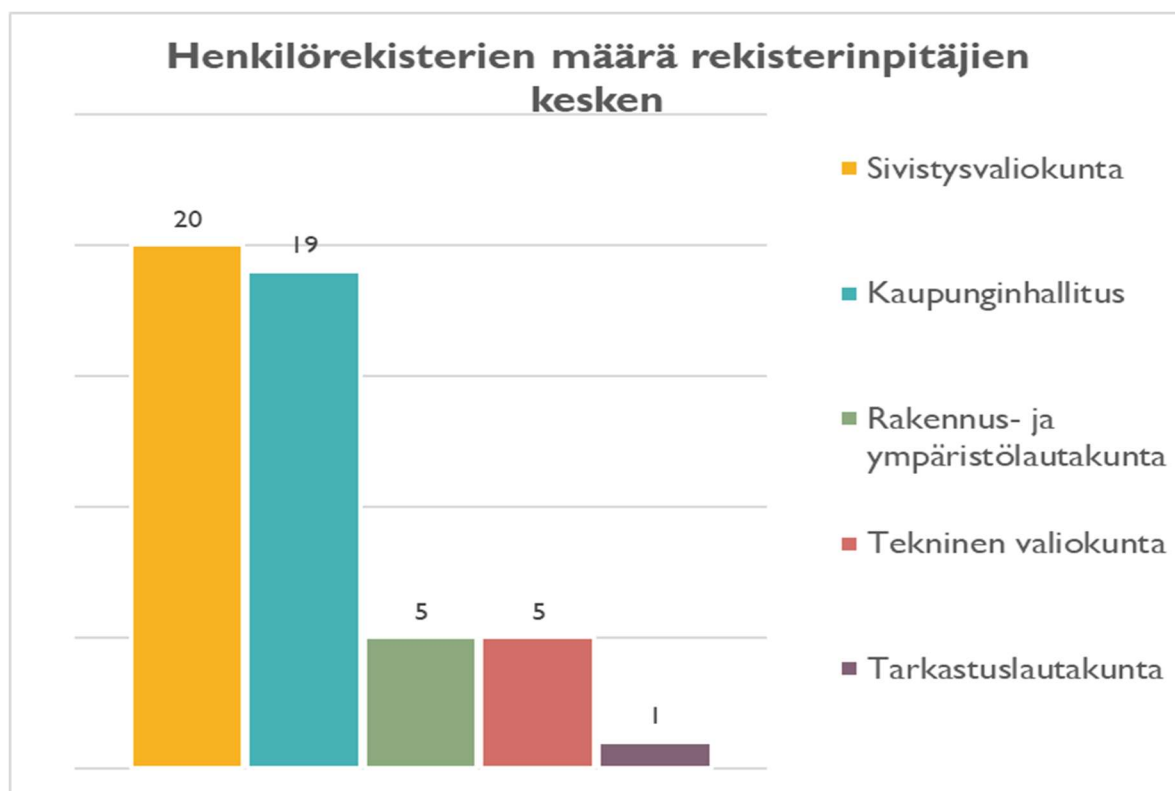
Koko kaupungin henkilötietoja sisältävien rekisterien määrä on 50.

Kaupungin henkilötietoja sisältävät tietovarannot on jaettu kolmeen eri pääryhmään.

1. Kuntalaisten tietoja sisältäviä lakisääteisiä henkilötietorekistereitä kaupungilla on 37 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 tietoturvaluustoimenpiteitä viranomaisen tietoaaineistojen, niiden käsittelyvaiheiden ja tietoaaineistoihin sisältyvien tietojen hallinnoimiseksi riippumatta tietoaaineistojen tallentamistavasta ja muista käsittelytavoista. Laitilassa tiedonhallintaa kuvataan ja ohjataan tiedonhallintalain vaatimusten mukaisella tiedonhallintamallilla, tiedonohjaussuunnitelmalla sekä asiakirjajulkisuuskuvauksella.

8.1 Tiedonhallintamalli ja tiedonohjaussuunnitelma

Tiedonhallintamalli on tiedonhallintalain (906/2019) edellyttämä kuvaus siitä, miten Laitilan kaupungin tiedonhallinta on järjestetty. Tiedonhallintamalli kokoaa yhteen tiedonhallinnan dokumentit ja auttaa hahmottamaan mm. mitä tietoa kaupungilla on, missä se sijaitsee ja kuka sitä käsittelee. Vastuu tiedonhallintamallin tietojen ajantasaisuudesta on jaettu toimialueittain toimialajohtajille

Tiedonohjaussuunnitelma TOS on kaupungin asiakirjojen ja tietoaaineistojen rekisteröinnin, käsittelyn ja säilyttämisen ohjeisto, joka ohjaa tiedon syntyä ja elinkaarta. Tiedonohjaussuunnitelma sisältää tiedot kaupungin asiakirjoista ja tiedoista, sekä niiden säilytysajoista ja julkisuudesta. Vastuu tiedonohjaussuunnitelman ajantasaisuudesta on jaettu toimialueittain toimialajohtajille

8.2 Asiakirjajulkisuuskuvaukset

Asiakirjajulkisuuskuvauksemme antaa yleiskuvan tiedonhallinnasta ja siitä, miten ja missä laajuudessa keräämme ja käsittelemme tietoja lakisäätöisissä tehtävissämme. Asiakirja julkisuuskuvaukset toteuttaa julkisuusperiaatetta. Tavoitteena on auttaa asiakasta kohdistamaan tietopyyntönsä ja yksilöimään tietopyynnön sekä opastaa tietoaaineistojen omatoimisessa haussa ja käytössä.

Asiakirjajulkisuuskuvaukset on saatavilla osoitteessa <https://www.laitila.fi/tietosuoja>

8.3 Keskeiset tietojärjestelmät

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

- CaseM – asianhallintajärjestelmä
- Personec F2 – henkilöstöhallinto
- Intime Plus – taloushallinto
- Cloudia – sopimustenhallinta
- Clausion Cloud – konserniohjelmisto
- 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
- 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 uhyihin 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, liitetä 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 ilmentyvän 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 tietosuoja 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 Tietoturvan periaatteet

Tietoturvallisuuden hallinnalla tarkoitetaan kaikkia hallinnollisia, toiminnallisia ja teknisiä toimenpiteitä, joilla varmistetaan tietojen ja tietoaineistojen saatavuus, eheys ja luottamuksellisuus niiden elinkaaren aikana.

Tiedon luottamuksellisuus, virheettömyys ja käytettävyys varmistetaan huolellisella käsittelyllä. Tiedot 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.

11.1 Suurimmat uhkatekijät

Käyttäjätunnuksien kalasteluun tähtäävät viestit pysyvät myös vuoden 2025 suurimpana uhkatekijänä. Tavat, joilla käyttäjätunnuksia yritetään saada haltuun ovat monipuolistuneet ja huijausviestejä tulee sähköpostien, sosiaalisen median ja puheluiden kautta. Uhkaa lisää rikollisten paremmat kyvykkyudet, esimerkiksi kiertää kaksivaiheinen tunnistautuminen.

Nopeasti muuttuva kuntien toimintaympäristö ja kasvava teknologinen monimutkaisuus lisäävät riskiä, että puutteellinen osaaminen ja resurssit altistavat kunnan tietojärjestelmät verkkorikollisten jatkuville hyökkäysyrityksille.

Rikolliset hyödyntävät yhä nopeammin tietoteknisen ympäristön haavoittuvuuksia, minkä vuoksi kaupungin on varmistettava järjestelmien ajantasaiset päivitykset ja haavoittuvuuksien hallinta, säännöllinen ja testattu varmuuskopiointi, monivaiheinen tunnistautuminen myös ylläpidossa, riittävä tekninen valvonta ja lokien hallinta sekä henkilöstön jatkuva koulutus ja viestintä.

Laitilan kaupunki on myös kriittisen infrastruktuurin toimija ja siten alttiina myös sellaiselle häirinnälle ja hyökkäyksille, joiden taustalla on taloudellisten motiivien lisäksi mahdollisesti geopolittiset 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 2025 aikana tapahtui yksi tietosuojaloukkaus, josta tehtiin ilmoitus tietosuojavaltuutetun toimistolle.

Vuoden 2025 aikana tapahtui yksi tietosuojarikkomus, josta on laadittu sisäinen tietosuojarikkomus dokumentti.

12 Kehittämiskohteet ja keskeisimmät muutokset vuonna 2026

Vuoden 2026 kehittämiskohteiksi on tunnistettu seuraavat osa-alueet:

1. Uusien tunnistautumiseen liittyvien mekanismien käyttöönotto riskiarvioiden perusteella.
2. Uusien taloushallinnon ohjelmistojen käyttöönotto ja siihen liittyvien tietoturva-, tietosuoja- ja tiedonhallinta dokumenttien päivitys ja käytänteiden jalkauttaminen organisaatiossa.
3. Jatkuvana kehittämiskohteena henkilöstökoulutukset ja tietoisuuden kasvattaminen painopisteenä henkilöstön tietoturva- ja tietosuojatietoisuuden ja osaamisen kasvattaminen.

13 2025 määriteltyjen kehittämiskohteiden tilannekatsaus

Viime vuoden tietotilinpäätöksessä, 2024 kehittämiskohteiksi listattiin 3 osa-aluetta.

Toimenpiteet, jotka tehtiin kehittämiskohteiden osalta, olivat seuraavat:

1. Tiedonhallintamallin ja tiedonohjaussuunnitelman läpikäyminen ja siinä havaittujen puuteiden implementointi oli osa tiedonhallinnan osa-alueiden kehittämistä.
2. Kansallinen kyberturvallisuuslaki 124/2025, jolla toimeenpannaan, NIS2-direktiivi on tullut voimaan 8.4.2025. Suomen kansallisessa toimeenpanosäätelyssä paikallistaso eli kunnat on jätetty julkinen hallinto toimialan ulkopuolelle, eikä NIS2-sääntely koske siten peruskunnan kuten Laitilan toimintaa.
3. Monivaiheisen tunnistautumisen käyttöönotto on toteutettu ja uudempien tunnistautumis- mekanismien käyttöönotto tapahtuu riskiarvioiden perusteella.