LEMIN KUNTA **TIETOSUOJAPOLITIIKKA**
20.8.2018

1. Johdanto

Tieto on keskeisessä roolissa Lemin kunnan toiminnassa ja palvelutuotannossa. Jotta tieto on tehokkaasti hyödynnettävissä, tiedon hallinnan ja käsittelyn tulee toimia asianmukaisesti kaikissa tilanteissa.

Kunnan johto määrittelee tässä asiakirjassa tietoturvallisuutta ja tietosuojaa koskevat periaatteet, linjaukset, vastuut ja tavoitteet. Asiakirja toimii perustana kunnan tietoturvallisuutta ja tietosuojaa koskeville ohjeille, joiden tehtävänä on tarkentaa tämän asiakirjan sisältöä ja auttaa sen käytäntöön soveltamisessa.

Tietosuojapolitiikka koskee jokaista kunnan työntekijää ja sidosryhmän edustajaa, joka työnsä tai toimeksiantonsa puitteissa käsittelee kunnan omistamaa tai hallinnoimaa tietoa.

Tietosuojapolitiikkaa sovelletaan kaikkeen tietoon ja muuhun dataan (myöh. tieto) riippumatta sen esitystavasta, muodosta, suojaustasosta, elinkaaren vaiheesta, esiintymisympäristöstä tai siirtotiestä.

2. Vaatimustenmukaisuus ja tavoitteet

Velvoittavan lainsäädännön lisäksi kunnan tietoturvallisuudelle ja tietosuojalle asettaa vaatimuksia kunnan toimintaympäristö. Tietoturvallisuutta ja tietosuojaa ohjaavat kunnan omien ohjeiden ja määräysten lisäksi seuraavat säädöstöt ja ohjeet:

- EU:n Yleinen Tietosuoja-asetus: (EU) 2016/679 sekä sen nojalla annettava tietosuojalaki
- Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa: 681/2010, 5§
- Julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) ohjeet

Kunnan tietoturva- ja tietosuojatyön tavoitteena on:

- yhdenmukaistaa kunnan sisäisiä turvallisuuskäytäntöjä kehittämällä kunnan turvallisuuskulttuuria
- varmistaa seudullinen turvallisuuskäytäntöjen yhteensopivuus tekemällä yhteistyötä tietoverkon ylläpidossa Saimaan Talous- ja Tieto Oy:n kanssa

Tavoitteiden saavuttamiseksi toteutetut ja suunnitellut toimenpiteet kuvataan erillisissä suunnitelmissa.

3. Tietoturvallisuus ja tietosuoja

Tietoturvallisuudella tarkoitetaan kunnassa hallinnollisia, teknisiä ja muita keinoja, joilla suojataan kunnan omistamaa tai hallinnoimaa tietoa normaali- ja häiriötilanteissa sekä poikkeusoloissa. Toteutuakseen tietoturvallisuus vaatii seuraavien, painoarvoltaan tapauskohtaisesti vaihtelevien asioiden, toteutumista:

- Luottamuksellisuus: Tieto on vain tietoon oikeutettujen käytettävissä.
- Eheys: Tietoa ei ole muutettu tahallisesti tai tahattomasti, eikä tieto ole muuttunut teknisen häiriön seurauksena.
- Saatavuus: Tieto, tietojärjestelmä tai palvelu on siihen oikeutettujen henkilöiden ja järjestelmien saatavilla ja käytettävissä silloin kun sitä tarvitaan.
- Kiistämättömyys: Todisteiden keräämistä sen varmistamiseksi, ettei yksikään tietojen käsittelyn tai siirron osapuoli voi jälkikäteen kiistää osuuttaan siihen.

Tietosuojalla tarkoitetaan kunnassa velvoittavien tietosuojasäädösten mukaisia toimenpiteitä, joilla varmistetaan henkilön riittävä yksityisyyden suoja ja muut sitä turvaavat oikeudet henkilötietoja käsiteltäessä.

Henkilötiedot, joita kunta rekisterinpitäjänä kerää ja käsittelee, kuvataan kunnan tietosuojasivuilla.

Tietoturvallisuus ja tietosuoja, sekä niihin liittyvät kunnan määrittelemät vaatimukset, tulee huomioida mahdollisimman varhaisessa vaiheessa toiminnan, hankintojen ja teknisten järjestelmien suunnittelua.

4. Kokonaisturvallisuus

Kokonaisturvallisuudella tarkoitetaan kunnan määrittelemiä turvallisuuden, riskienhallinnan ja varautumisen osa-alueita, jotka yhdessä tietoturvallisuuden ja tietosuojan kanssa muodostavat eheän kokonaisuuden kunnan tiedon suojaksi:

- Kyberturvallisuus: Toimenpiteet, joilla turvataan kybertoimintaympäristön luottamuksellisuus, eheys, saatavuus ja jatkuvuus.
- Fyysinen turvallisuus: Toimenpiteet, järjestelmät ja rakenteet, joiden avulla kunnan tiloja, siellä olevia ihmisiä, kuljetuksia, matkatyötä sekä tietoa ja muuta omaisuutta suojataan fyysisiltä ja kiinteistö- ja ympäristövahingoilta, vahingoittamisyrityksiltä ja oikeudettomilta henkilöiltä.
- Henkilöstöturvallisuus: Tietoturvallisuuteen vaikuttavat toimenpiteet, joita suoritetaan henkilöstöprosessissa ennen palvelussuhdetta, sen aikana ja sen päättymisen yhteydessä.
- Riskien hallinta: Järjestelmällistä toimintaa riskien hallitsemiseksi niin, että ne ovat optimisuhteessa riskien rajoittamisen kustannuksiin samalla kun kunnan toiminnalle asetetut tavoitteet voidaan saavuttaa.
- Varautuminen: Tekniset järjestelyt ja toimintatavat, joilla kunnan toimintojen ja palveluiden jatkuvuus turvataan normaalioloissa, häiriötilanteissa sekä poikkeusoloissa.
- Asianmukaisilla ja ajantasaisilla sopimuksilla varmistetaan tässä politiikassa kuvailtujen periaatteiden toteutuminen myös sidosryhmien kanssa tehtävässä yhteistyössä.

5. Organisointi, roolit ja vastuut

Tietoturvallisuuteen ja tietosuojaan liittyvät roolit vastuineen on organisoitu kunnassa seuraavasti.

Kunnanhallitus seuraa tietoturvallisuuden ja tietosuojan toteutumista kunnassa. Kunnanhallitus hyväksyy tietosuojapolitiikan. Lisäksi hallituksella on vastuu kunnan sisäisen valvonnan ja riskienhallinnan järjestämisestä.

Kunnanjohtajalla on kokonaisvastuu tietoturvallisuuden ja tietosuojan toteuttamisesta ja niiden toteutumisen raportoinnista hallitukselle. Kunnanjohtaja omistaa tietoturvapolitiikan ja hyväksyy siitä johdetut tarkentavat ohjeet ja määräykset. Lisäksi hän vastaa kunnan turvallisuussuunnittelusta ja varautumisesta.

Toimialajohtaja vastaa toimialansa tietoturvallisuuden ja tietosuojan toteutumisesta sekä omistamiensa prosessien kokonaisturvallisuudesta.

Tytäryhtiöiden hallitukset ja toimitusjohtajat vastaavat tietoturvallisuuden ja tietosuojan toteutumisesta sekä kokonaisturvallisuuden toteutumisesta omissa organisaatioissaan.

Esimies vastaa tietoturvallisuuden ja tietosuojan toteutumisesta henkilöstöprosessin kaikissa vaiheissa omalla vastuualueellaan.

Esimiehen keskeisimmät tehtävät ovat huolehtia:

- oman organisaationsa perehdyttämisestä kunnan tietoturva- ja tietosuojaohjeisiin sekä jokaisen työntekijän työtehtäviin liittyviin tietoturva- ja tietosuojavastuisiin.
- työntekijän palvelussuhteen päättyessä tai henkilön siirtyessä toisiin tehtäviin:
  - kunnan tiedon ja muun omaisuuden palauttamisesta
  - ilmoittamisesta atk-tukihenkilölle työntekijän käyttöoikeuksien ja -valtuuksien poistamiseksi.

Henkilöstö vastaa omalta osaltaan määräysten ja ohjeiden noudattamisesta. Jokaisen vastuulla on lisäksi poikkeamien, uhkien ja riskien ilmoittaminen välittömästi omalle esimiehelleen, tietosuojavastaavalle tai atk-tukihenkilölle.

Tietojärjestelmän tai muun teknisen kokonaisuuden **omistaja** vastaa järjestelmänsä ja sen sisältämän tiedon riskienhallinnasta ja varautumisesta sekä tietoturvallisuuden ja tietosuojan toteutumisesta.

Pääkäyttäjä vastaa järjestelmänsä osalta tietoturvallisuuden ja tietosuojan toteuttamisesta tietojärjestelmän omistajan ohjauksessa.

Tiedon omistaja vastaa tiedon luokittelusta (julkisuuden ja salassapidon määrittely) ja eheyden varmistamisesta sekä tallentamisesta luokituksen edellyttämään ympäristöön.

Tietosuojavastaava edistää tietoturvallisuuden ja tietosuojan toteutumista kunnassa. Tietosuojavastaava on riippumaton toimija, joka seuraa tietosuojaa ohjaavan lainsäädännön noudattamista kunnassa. Lisäksi tietosuojavastaava tekee yhteistyötä valvonta- ja muiden viranomaisten kanssa sekä tukee ja neuvoo tietoturva- ja tietosuoja -asioissa. Tietosuojavastaava raportoi tietoturvallisuuden ja tietosuojan toteutumisesta kunnanjohtajalle sekä vastaa tietoturvallisuuteen ja tietosuojaan liittyvästä viestinnästä yhdessä talous- ja hallintojohtajan kanssa.

Tietosuojaryhmä toimii tietosuojavastaavan tukena. Tietosuojaryhmä seuraa tietoturvallisuuden ja tietosuojan yleistä kehittymistä, uhkia ja riskejä sekä tietoturvallisuuden ja tietosuojan toteutumista kunnassa. Ryhmä analysoi ja arvioi em. kokonaisuutta ja tekee siihen perustuen kehitysehdotuksia kunnan tietoturvallisuuden ja tietotuojan parantamiseksi. Lisäksi ryhmä toimii, yhdessä tietosuojavastaavan kanssa, kunnan tukena tietoturva- ja tietosuoja -asioissa. Tietosuojaryhmän nimeää kunnanjohtaja.

Sisäinen tarkastus vastaa tietoturvallisuuden toteutumisen asianmukaisuudesta ja riittävyyden arvioinnista sekä tarkastamisesta.

Johtoryhmä vastaa kunnan turvallisuussuunnittelusta ja varautumisesta.

Ulkoiset **sidosryhmät** vastaavat omalta osaltaan tietoturvallisuuden ja tietosuojan toteuttamisesta, sopimuksissa kuvattujen kunnan asettamien vaatimusten mukaisesti.

6. Tiedon ja tietojärjestelmien käyttö

Kunnan tietojärjestelmäympäristössä käytetään talous- ja hallintojohtajan hyväksymiä tietojärjestelmiä, laitteita ja ohjelmistoja, jotka on tarkoitettu työtehtävien hoitamista varten. Kunnan tietojärjestelmäympäristöön saa tehdä muutoksia vain talous- ja hallintojohtaja tai hänen valtuuttamansa.

Pääsyoikeudet kunnan tietoverkkoon ja -järjestelmiin sekä käyttöoikeudet kunnan omistamaan ja hallinnoimaan tietoon myönnetään työtehtävien hoitoon tarvittavassa laajuudessa.

7. Tietoturvallisuuden ja tietosuojan toteuttaminen

Tietoturvallisuutta ja tietosuojaa toteutetaan jatkuvaan parantamiseen tähtäävillä johtamis- ja muilla käytännöillä. Keskeistä toteuttamisessa on, että kunnalla on riittävät kyvyt ylläpitää turvallisuuskulttuuriaan mm. seuraavasti:

- Tietoturvallisuutta ja tietosuojaa johdetaan järjestelmällisesti
- Henkilöstön osaamisesta huolehditaan jatkuvalla koulutuksella
- Toimintaympäristön tilaa seurataan aktiivisesti
- Uhka- ja riskiympäristöä arvioidaan säännöllisesti ja reagoidaan tilanteen edellyttämällä tavalla
- Poikkeamiin ja häiriöihin varaudutaan ennakolta ylläpitämällä, harjoittelemalla ja testaamalla tarvittavia jatkuvuus- ja muita suunnitelmia.

8. Lemin kunnan tietosuojakäytännöt henkilötietojen käsittelyssä

Henkilötietojen käsittely kunnan toimivaltaan kuuluvissa asioissa

Kunnassa voi saada asian vireille kirjallisesti, sähköpostitse tai poikkeustapauksissa suullisesti. Vireillä oleviin asioihin liittyvät asiakirjat ovat valmistelijan tai päättäjän hallussa, kunnes asia on ratkaisu, jolloin ne siirtyvät kunnan arkistoon.

Tietojen käyttötarkoitus on vireille saatettujen asioiden käsittely lainsäädännön edellyttämällä tavalla, viranomaistoiminnan ja muun toiminnan suunnittelu ja toteuttaminen.

Teknistä asianhallintajärjestelmää ei ole käytössä.

Kunnassa käsiteltäviin vireille saatettuihin asioihin liittyvien henkilötietojen säilyttämisajat määräytyvät arkistolain (831/1994), arkistolaitoksen määräyksen (AL 16465/07.01.01.03.02/2016) ja kunnan tiedonohjaussuunnitelman mukaisesti.

Mitä tietoja kunnassa käsitellään

Kunnassa vireille saatettu asia annetaan asian valmistelijan tai päättäjän haltuun ja hän säilyttää sitä lukitussa tilassa, kunnes on ratkaissut asian tai siirtänyt sen edelleen.

Käsiteltävien tietojen laajuus riippuu asian luonteesta ja siitä, mitä asiaan liittyviä tietoja kuntaan on toimitettu.

Tavanomaisesti käsitellään ainakin seuraavia tietoja:

- vireillesaattajan nimi
- vireillesaattajan ne yhteystiedot, jotka hän on kuntaan antanut, esimerkiksi puhelinnumero, sähköpostiosoite ja/tai postiosoite
- asian kuvaus
- asian käsittelyvaiheita koskevat tiedot

Mihin tietojen käsittely kunnassa perustuu

Käsittelemme henkilötietoja yleistä etua koskevan tehtävän suorittamiseksi ja kunnalle kuuluvan julkisen vallan käyttämiseksi:

- Tietosuoja-asetuksen (EU 2016/679) 6 artikla

Käsittelemme erityisiä henkilötietoryhmiä yleisen edun perusteella kansallisen lainsäädännön nojalla:
- Tietosuoja-asetuksen (EU 2016/679) 9 artiklan 2 kohta
- Henkilötietolain (523/1999) 12 § 1 mom. 5 kohta

Kunnan asemasta, tehtävistä ja toimivallasta säädetään:
- KuntaL 410/2015

Tietojen luovuttaminen

Tietoja ei luovuteta säännönmukaisesti.

Tietoja luovutetaan niitä pyytävälle viranomaisten toiminnan julkisuudesta annetun lain mukaisesti. Tiedot ja asiakirjat ovat julkisia, ellei niitä ole nimenomaisesti lailla säädetty salassa pidettäväksi.
- JulkL 621/1999

Henkilötietojen käsittelyyn liittyvät tietosuojaoikeudet

Oikeus saada informaatiota henkilötietojen käsittelystä

- Asiakkaalla on oikeus saada tietää, mihin tarkoituksiin ja millä tavoilla käsittelemme hänen henkilötietojaan.

Oikeus saada pääsy tietoihin

- Asiakkaalla on oikeus saada tietää, käsittelemmekö häntä koskevia henkilötietoja. Jos käsittelemme, asiakkaalla on oikeus saada jäljennös näistä tiedoista, ellei kunnalla ole lainmukaista perustetta kieltäytyä oikeuden toteuttamisesta

Oikeus oikaista tietoja

- Jos asiakasta koskevat henkilötiedot, joita käsittelemme, ovat virheellisiä, voi asiakas pyytää kuntaa oikaisemaan tiedot
- Jos kunta oikaisee tietoja asiakkaan pyynnön perusteella, on kunta velvollinen mahdollisuuksien mukaan ilmoittamaan oikaisusta kaikille niille, joille tietoja on aikaisemmin luovutettu

Oikeus rajoittaa tietojen käsittelyä

- Jos kunnan käsittelemät asiakasta koskevat tiedot ovat asiakkaan mielestä virheellisiä, niitä käsitellään lainvastaisesti tai asiakas on vastustanut tietojensa käsittelyä, voi hän pyytää kuntaa rajoittamaan tietojensa käsittelyä.

Tällöin kunta voi käsitellä asiakkaan tietoja vain
- asiakkaan suostumuksella
- jos kunta tarvitsee tietoja oikeusvaateen laatimisen, esittämisen tai puolustamisen takia
- yleisen edun vuoksi, tai
- jonkun toisen henkilön oikeuksien suojaamiseksi
- jos kunta rajoittaa tietojen käsittelyä asiakkaan pyynnön perusteella, on kunta velvollinen mahdollisuuksien mukaan ilmoittamaan rajoituksesta kaikille niille,

joille tietoja on aikaisemmin luovutettu

Oikeus vastustaa tietojen käsittelyä

Joissakin tilanteissa asiakas voi myös vastustaa henkilötietojensa käsittelyä eli pyytää, että tietoja ei käsiteltäisi ollenkaan.

Vastustaminen on mahdollista, jos rekisterinpitäjä käsittelee asiakkaan tietoja yleisen edun tai julkisen vallan vuoksi tai oikeutetun etunsa perusteella. Asiakas voi vastustaa tietojensa käsittelyä, jos hänellä on siihen jokin henkilökohtaiseen tilanteeseesi liittyvä erityinen syy.

Tietosuojaoikeuksia koskeva pyyntö on esitettävä kuntaan sähköpostilla (leminkunta@lemi.fi) tai postitse (Lemin kunta, Toukkalantie 2, 54710 Lemi).

Pyynnössä tulee kertoa

- haluaako asiakas rajoittaa vai vastustaa henkilötietojensa käsittelyä
- perustelut käsittelyn rajoittamiselle tai vastustamiselle
- asiakkaan nimi
- asiakkaan yhteystiedot (esimerkiksi sähköpostiosoite tai puhelinnumero).

Pyyntö käsitellään kunnassa ja siitä tehdään viranhaltijapäätös.

Kunta ei tee profilointia käsittelemiensä henkilötietojen perusteella.

Kaikki henkilötietoja koskevat tietopyynnöt ja oikaisut toimitetaan Lemin kunnan tietosuojavastaavalle sähköpostilla leminkunta@lemi.fi tai postitse osoitteella: Lemin kunta / Tietosuojavastaava, Toukkalantie 2, 54710 Lemi

9. Dokumentin ylläpito

Tämän asiakirjan säännöllisestä arvioinnista ja päivittämisestä vastaa kunnanjohtaja tai hänen nimeämänsä taho. Asiakirja on julkisesti saatavilla osoitteessa www.lemi.fi. Kunnan tietoturva- ja tietosuojadokumentaatiota kokonaisuudessaan pidetään henkilöstön saatavilla kunnan sisäisissä informaatiokanavissa työtehtävien edellyttämässä laajuudessa.