

TAMMELAN KUNTA

TIETOSUOJAPOLITIIKKA



TAMMELA

www.tammela.fi

SISÄLLYS

1	JOHDANTO	3
2	KÄSITTEET	3
3	TIETOSUOJAN TAVOITTEET	4
4	TIETOSUOJAN TOTEUTTAMINEN	5
5	ROOLIT JA VASTUUT	6
6	TIETOSUOJAN SEURANTA, YLLÄPITO JA KEHITTÄMINEN	7
LIITTEET		8
Liite 1 Lainsäädäntö ja ohjaavat asiakirjat		8



TAMMELA

www.tammela.fi

1 JOHDANTO

Tammelan kunnan toiminta ja palvelut perustuvat suurelta osin tietoon ja sen käsittelyyn. Tiedon tehokas hyödyntäminen, turvallisuus ja henkilötietojen suoja edellyttävät tiedon hallintaa ja käyttöä tukevien järjestelyjen asianmukaista toimintaa sekä kehittämistä kaikissa tilanteissa. Tämän edellytyksenä on tehokas johtaminen, luotettava tietojen käsittelyn toteutus ja osaava henkilöstö.

Tammelan kunta toimii tietosuojan toteuttamisessa kulloinkin voimassa olevan lainsäädännön, EU:n yleisen tietosuojasetuksen ja hyvän tiedonsuojaustavan mukaisesti.

Tietosuojapolitiikka määrittää Tammelan kunnan valtuuston, kunnanhallituksen ja johtoryhmän asettaman tavoitetilan tietosuojalle. Tietosuojapolitiikka sisältää ne henkilötietojen käsittelyyn liittyvät periaatteet, toimintatavat, roolit ja vastuut, joita noudatetaan Tammelan kunnan tietosuojan toteuttamisessa ja kehittämisessä. Tietosuoja on otettava huomioon kaikessa tietojen käsittelyssä jo suunnitteluvaiheessa. Tietosuojapolitiikka antaa pohjan ohjeiden ja määräysten soveltamiselle.

Tietosuojapolitiikka koskee koko Tammelan kunnan organisaatiota mukaan lukien konsernin, henkilöstöä, luottamushenkilöitä sekä niitä kunnan sidosryhmien edustajia, jotka toimeksiantojensa puitteissa käsittelevät Tammelan kunnan omistamaa tai hallinnoimaa tietoa.

Tietosuojapolitiikka on julkinen asiakirja ja se on voimassa toistaiseksi. Sitä täydennetään tai päivitetään tarpeen mukaan, esimerkiksi lainsäädännön muuttuessa.

2 KÄSITTEET

Henkilötieto

Henkilötiedolla tarkoitetaan kaikkea sellaista tietoa, jolla voidaan tunnistaa ja yksilöidä henkilöitä. Näitä tietoja ovat muun muassa nimi, osoite, henkilötunnus, sähköpostiosoite sekä verkkotunnistiedot. Henkilö on tunnistettavissa, jos tieto voidaan liittää henkilöön joko suoraan tai välillisesti.

Henkilörekisteri

Henkilötietoja sisältävä jäsennelty tietojoukko, jota käsitellään osin tai kokonaan automaattisen tietojenkäsittelyn avulla taikka joka on järjestetty kortistoksi, luetteloksi tai muulla näihin verrattavalla tavalla siten, että tiettyä henkilöä koskevat tiedot voidaan löytää helposti ja kohtuuttomitta kustannuksitta. Tietomassa voi olla keskitetty, hajautettu tai jaettu eri perustein.

Henkilötietojen käsittelijä

Henkilötietojen käsittelijä on se henkilö, viranomainen, virasto tai muu taho, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Esimerkiksi rekisterinpitäjän käyttämä palveluntarjoaja. Henkilötietojen käsittelijällä ei tarkoiteta organisaatio omia työntekijöitä.

Henkilötietojen käsittely

Henkilötietojen käsittely tarkoittaa kaikkia henkilötietoihin kohdistettavia toimia, kuten tietojen kerääminen, tallentaminen, järjestäminen, jäsentäminen, säilyttäminen, muokkaaminen tai muuttaminen, haku, kysely, käyttö, tietojen luovuttaminen siirtämällä, levittämällä tai asettamalla ne

muutoin saataville, tietojen yhteensovittaminen tai yhdistäminen, rajoittaminen, poistaminen tai tuhoaminen.

Rekisterinpitäjä

Rekisterinpitäjä on se henkilö tai organisaatio, joka määrittelee henkilötietojen käsittelyn tarkoitukset sekä keinot tai jonka tehtäväksi henkilötietojen käsittely on lailla säädetty. Rekisterinpitäjä on vastuussa suorittamastaan henkilötietojen käsittelystä.

Rekisteröity

Rekisteröity on henkilö, jonka tietoja käsitellään.

Tietosuoja

Henkilötietojen suoja on jokaiselle kuuluva perusoikeus. Tietosuojalla tarkoitetaan kansalaisten yksityisyyden suojaamista sekä oikeuksien, etujen, vapauksien ja oikeusturvan turvaamista henkilötietoja käsiteltäessä. Tietosuoja määrittelee ne periaatteet, milloin, millä edellytyksillä ja miten henkilötietoja voidaan käsitellä.

Tietosuojavastaava

Henkilö, jonka tehtävänä on mm. seurata henkilötietojen käsittelyn lainmukaisuutta ja auttaa organisaatiota toteuttamaan lainsäädännön asettamat velvoitteet. Asema on itsenäinen ja riippumaton. Vastaava raportoi suoraan rekisterinpitäjän ylimmälle johdolle, joka on päävastuussa henkilötietojen käsittelyn lainmukaisuudesta.

Tietoturva

Tietoturvalla tarkoitetaan niitä teknisiä ja hallinnollisia toimenpiteitä, joilla pyritään mm. tietosuojan toteuttamiseen. Tietoturva on siis yksi tietosuojan toteuttamisen keino.

3 TIETOSUOJAN TAVOITTEET

Yksityisyydensuoja ja henkilötietojen suoja on jokaisen perusoikeus. Tammelan kunnassa käsitellään erilaisia henkilötietoja, taloustietoja ja hallinnon asiakirjoja. Osa tiedoista sisältää salassa pidettävää tai muutoin luottamuksellista tietoa. Tammelan kunnan tavoitteena on edistää hyvää tietojenkäsittelytapaa sekä varmistaa tietojenkäsittelyn turvallisuus, sekä tehtävien sujuva ja häiriötön toiminta kunnassa. Tietoja käsitellään niin, että osapuolet voivat luottaa käsittelyn asianmukaisuuteen.

Tammelan kunta määrittää tarvittavat suojatoimet ottamalla huomioon mm. käytettävissä olevan tekniikan, toteuttamiskustannukset, käsittelyn luonteen ja laajuuden, asiayhteyden ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat riskit.

Hyvän tietosuojan tason saavuttamiseksi jokaisen tietoa käsittelevän tulee ymmärtää tietojen käsittelyn periaatteet: mitä tietoa saa käsitellä, missä tarkoituksessa ja milloin tietoa saa käsitellä sekä mitkä ovat rekisteröidyn oikeudet.

4 TIETOSUOJAN TOTEUTTAMINEN

Hyvän tietosuojan toteuttaminen edellyttää organisaation jatkuvia toimia, joilla turvataan organisaation toiminta niin normaalioloissa, normaaliolojen häiriötilanteessa kuin poikkeusoloissakin. Toteuttaminen tapahtuu erilaisten hallinnollisten ja teknisten toimenpiteiden avulla. Tietosuoja tulee huomioida kaikessa toiminnassa niin manuaalisessa kuin sähköisessä henkilötietojen käsittelyssä sekä suullisessa ja kirjoitetussa tiedossa. Henkilöstön riittävästä osaamisesta huolehditaan järjestämällä koulutusta ja ottamalla tietosuojan toteuttaminen osaksi perehdytystä sekä seuraamalla osaamisen tasoa. Poikkeamiin ja häiriöihin varaudutaan ennakolta ylläpitämällä, harjoittelemalla ja testaamalla tarvittavia suunnitelmia.

Henkilötietojen käsittelyssä noudatetaan seuraavia tietosuoja-asetuksessa annettuja tietosuoja-periaatteita:

1) Lainmukaisuus, kohtuullisuus ja läpinäkyvyys

Henkilötietojen käsittelyssä on noudatettava EU:n tietosuoja-asetusta ja muuta henkilötietojen käsittelyä koskevaa lainsäädäntöä. Jotta henkilötietojen käsittely olisi lainmukaista, sille on oltava sopiva käsittelyperuste. Henkilötietojen käsittelyn on oltava asianmukaista ja kohtuullista. Henkilötietojen käsittelystä on kerrottava rekisteröidyille selkeällä ja ymmärrettävällä tavalla. Henkilötietojen käsittelystä kertovien tietojen on oltava helposti saatavilla.

2) Käyttötarkoitussidonnaisuus

Henkilötietojen käsittelyn tarkoitus on suunniteltava ja määritettävä selkeästi ennen käsittelyn aloittamista. Henkilötietoja saa kerätä vain tiettyä, nimenomaista ja laillista tarkoitusta varten. Tietoja ei saa käsitellä alkuperäisten tarkoitusten kanssa yhteensopimattomalla tavalla myöhemmin.

3) Tietojen minimointi

Henkilötietoja saa käsitellä vain silloin, kun se on tarpeellista käsittelyn tarkoituksen kannalta. Käsiteltävien henkilötietojen on oltava asianmukaisia eli kerättyjen tietojen on oltava sellaisia tietoja, joilla kyetään täyttämään määritelty käyttötarkoitus. Käsiteltävien henkilötietojen on oltava olennaisia eli kerätyillä henkilötiedoilla on oltava selkeä yhteys määriteltyyn käyttötarkoitukseen. Lisäksi käsiteltävien henkilötietojen on oltava rajoitettuja eli välttämättömiä määritellyn henkilötietojen käyttötarkoituksen kannalta.

4) Tietojen täsmällisyys

Käsiteltävien henkilötietojen on oltava **täsmällisiä** ja päivitettyjä sekä rekisterinpitäjän on kohtuullisen toimenpitein varmistettava, että käsittelyn tarkoituksiin nähden epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä.

5) Säilytyksen rajoittaminen

Henkilötietoja saa säilyttää vain niin kauan kuin se on tarpeen tietojen käyttötarkoitusta varten. Rekisterinpitäjän on suunniteltava ja pystyttävä perustelemaan henkilötietojen säilytysaika. Rekisterinpitäjän on itse huomioitava laista tulevat säilytysajat. Henkilötietojen säilytysajat on myös dokumentoitava. Kun henkilötietoja ei enää tarvita, ne tulee anonymisoida tai poistaa. Tietoja voidaan säilyttää alkuperäistä käyttötarkoitusta kauemmin vain, mikäli tietoja

käsitellään ainoastaan yleisen edun mukaisia arkistointitarkoituksia varten tai tietoja käytetään historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten.

6) Luottamuksellisuus ja turvallisuus

Henkilötietojen käsittelyn on oltava luottamuksellista ja turvallista. Rekisterinpitäjän on arvioitava mahdollisia riskejä, organisaation tietosuoja- ja tietoturvaohjeistuksen tasoa sekä henkilötietojen teknistä suojausta. Suojatoimien riittävyyttä on punnittava suhteessa olosuhteisiin ja riskeihin.

5 ROOLIT JA VASTUUT

Henkilötietojen käsittelyn lainmukaisuudesta vastaa ensisijaisesti Tammelan kunnan valtuusto, kunnanhallitus ja johtoryhmä. Vastuu koskee myös ulkoistettuja toimintoja. Valtuustolla, kunnanhallituksella ja johtoryhmällä on vastuu huolehtia mm. tietosuoja- ja tietoturvatyön riittävästä resursoinnista ja tietosuojan huomioimisesta suunnittelussa.

Kunnanhallitus hyväksyy tietosuoja- ja tietoturvapoliitikan sekä vastaa tietosuojan toteuttamisen edellytyksien luomisesta asetettujen tavoitteiden saavuttamiseksi. Kunnanhallitus seuraa tietosuojan ja tietoturvan tilaa osana sisäistä valvontaa ja riskienhallintaa.

Kunnanjohtaja hyväksyy koko kuntaa koskevat operatiiviset tietosuojaohjeet ja tietoturvaohjeet sekä vastaa niiden toteuttamisen toimintaedellytyksistä ja seurannasta. Lisäksi hän vastaa kunnan turvallisuussuunnittelusta, varautumisesta sekä tietoturvallisuuden ja tietosuojan toteutumisesta henkilöstöprosessissa.

Kunnan johtoryhmä toimii tietosuojaa ja tietoturvaa koskevissa asioissa ohjausryhmänä sekä vastaa tietosuojapolitiikan toteutumisesta. Johtoryhmä varmistaa tietojen suojaamisen menetelmät, välineet ja toimenpiteet sekä työhön osoitetut resurssit.

Toimialajohtajat vastaavat toimialansa sisäisten toimintojen ja tuottamien palveluiden (prosessien) sekä tietojärjestelmien riskienhallinnasta, varautumisesta sekä tietoturvallisuuden ja tietosuojan toteutumisesta. Toimialajohtajat varmistavat tietosuojaan ja tietoturvaan liittyvien suunnitelmien ja ohjeistuksien käytäntöön viennistä.

Palvelualueiden esihenkilöt valvovat tietosuojan toteutumista omassa yksikössään. Esihenkilöt huolehtivat, että tietosuoja- ja tietoturvaohjeet perehdytetään henkilöstölle. Esihenkilöt huolehtivat myös siitä, että henkilöstö suorittaa tietosuojakoulutuksen. Lisäksi työntekijän palvelussuhteen päättyessä tai henkilön siirtyessä toisiin tehtäviin esihenkilöt ilmoittavat atk-suunnittelijalle tästä tiedon kunnan omaisuuden palauttamista sekä käyttöoikeuksien ja -valtuuksien poistamista varten.

Pääkäyttäjät vastaa järjestelmänsä tai sovelluksensa osalta tietoturvallisuuden ja tietosuojan toteuttamisesta toimialajohtajan ohjauksessa. Pääkäyttäjät ohjeistaa ja kouluttaa muita käyttäjiä järjestelmän tai sovelluksen käytössä.

Tietosuojavastaava toimii asiantuntijana ja yhteyshenkilönä tietosuoja-asioissa. Tietosuojavastaavan tehtäviin kuuluu myös asiantuntija-avun antaminen sekä organisaation henkilöstölle että organisaation johdolle tietosuojaan liittyvissä kysymyksissä sekä toimiminen valvontaviranomaisen yhdyshenkilönä. Tietosuojavastaava valmistelee tietosuojaan liittyviä ohjeita ja ylläpitää niitä. Tietosuojavastaavana toimii hallintopäällikkö.

ATK-suunnittelija vastaa teknisen tietoturvan kehittämisestä sekä tietojärjestelmien toiminnasta, hoidosta ja turvallisuudesta saamiensa resurssien ja toimintavaltuuksien puitteissa. Lisäksi atk-suunnittelija pyrkii varmistamaan, että kunnalla on edellytykset toimia tietosuojaan tai tietoturvaan liittyvissä häiriö- ja poikkeustilanteissa.

Tietosuojaryhmä vastaa omalta osaltaan tietosuojan tiedottamiseen, perehdyttämiseen, seurantaan, valvontaan ja kehittämiseen liittyvistä toiminnoista. Tietosuojaryhmän jäsenet toimivat tietosuojasioissa asiantuntijoina omalla toimialallaan.

Henkilöstö vastaa omalta osaltaan määräysten ja ohjeiden noudattamisesta. Jokaisen kunnan työntekijän tulee suorittaa hyväksytysti tietosuojakoulutus. Jokaisen vastuulla on lisäksi poikkeamien, uhkien ja riskien ilmoittaminen välittömästi omalle esihenkilölleen, tietosuojavastaavalle tai IT-vastuuhenkilölle.

Jokaisella Tammelan kunnan omistamaa tietoa käsittelevällä on omalta osaltaan henkilökohtainen vastuu kokonaisturvallisuudesta. Tietoa ja tietojärjestelmiä käyttävä on velvollinen noudattamaan tietosuojapolitiikan periaatteita ja tietosuojasta annettuja ohjeita sekä ilmoittamaan havaitsemistaan tietoturvallisuuden ja -suojan puutteista ohjeistetulla tavalla.

6 TIETOSUOJAN SEURANTA, YLLÄPITO JA KEHITTÄMINEN

Tietosuojatavoitteet asetetaan vuosittain laadittavaan vuosikelloon ja sen toteutumista seurataan säännöllisesti. Tällä tavoin toteutetaan myös rekisterinpitäjän osoitusvelvollisuutta sen osalta, että henkilötietoja käsitellään tietosuoja-aseuksen mukaisesti. Tietosuojapolitiikan ajantasaisuus tarkastetaan vuosittain vuosikellon mukaisesti tietosuojaryhmässä ja sitä päivitetään tarvittaessa. Päivitykset hyväksyy kunnanhallitus.

Tietosuojan seuranta on osa sisäistä valvontaa ja riskienhallintaa.

Rekisterinpitäjän velvollisuutena on ilmoittaa henkilötietojen tietoturvaloukkauksista valvontaviranomaiselle, jos loukkauksesta voi aiheutua riski luonnollisten henkilöiden oikeuksille ja vapauksille. Suomessa valvontaviranomaisena toimii tietosuojavaltuutetun toimisto. Henkilötietojen tietoturvaloukkauksella tarkoitetaan tapahtumaa, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu, henkilötietoja luovutetaan luvottomasti tai niihin pääsee käsiksi taho, jolla ei ole käsitteilyoikeutta. Henkilötietojen tietoturvaloukkauksia voivat olla esimerkiksi varastettu tietokone tai puhelin, hakkerointi, kyberhyökkäys tai haittaohjelmatartunta.

Henkilötietojen tietoturvaloukkauksesta on ilmoitettava tietosuojavaltuutetun toimistolle ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa siitä, kun rekisterinpitäjä on tullut tietoiseksi tietoturvaloukkauksesta. Henkilötietojen käsittelijän tulee ilmoittaa tietoturvaloukkauksesta ensin rekisterinpitäjälle, jollei ole erikseen sovittu, että käsittelijä voi ilmoittaa tietoturvaloukkauksista suoraan tietosuojavaltuutetun toimistolle. Henkilötietojen tietoturvaloukkauksesta on ilmoitettava rekisteröidylle, jos se todennäköisesti aiheuttaa korkean riskin tämän oikeuksille ja vapauksille. Rekisterinpitäjän on tällöin ilmoitettava asiasta ilman aiheetonta viivytystä, jotta rekisteröidyllä on mahdollisuus suojautua esimerkiksi sulkemalla luottokorttinsa.

Tammelan kunnan prosessin mukaan tieto tai epäily tietoturvaloukkauksesta tehdään tietosuoja-vastaavalle. Tietosuojavastaava kokoaa tarvittaessa tietosuojaryhmän koolle asian selvittämiseksi. Selvittettäviä asioita ovat:

- 1) Mitä on tapahtunut

- 2) Onko henkilötietoa levinnyt
- 3) Mistä henkilötiedosta on kyse
- 4) Minne henkilötietoa on päätynt
- 5) Milloin epäilty tietoturvaloukkaus on tapahtunut
- 6) Tapahtuman seuraukset ja riskit

Edellä olevien tietojen perusteella päätetään välittömistä toimenpiteistä.

Kunnan tietosuojavastaava tekee tarvittaessa ilmoituksen tietosuojavaltuutetun toimistolle.

LIITTEET

Liite 1 Lainsäädäntö ja ohjaavat asiakirjat

Tietosuojaan liittyvä keskeinen säädöspohja:

Arkistolaki (831/1994): Asiakirjojen laatiminen, säilyttäminen ja käyttö
Asetus viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999)
CER-direktiivi (Critical Entities Resilience Directive) (EU) 2022/2557
EU:n yleinen tietosuoja-asetus (679/2016)
Hallintolaki (434/2003)
Laki digitaalisten palvelujen tarjoamisesta (306/2019)
Laki julkisen hallinnon tiedonhallinnasta (906/2019)
Laki kunnan ja hyvinvointialueen viranhaltijasta (304/2003)
Laki sähköisen viestinnän palveluista 917/2014
Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003)
Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009)
Laki viranomaisten toiminnan julkisuudesta (621/1999)
Laki yksityisyyden suojasta työelämässä (759/2004)
NIS2-direktiivi (EU) 2022/2555
Oppilas- ja opiskelijahuoltolaki (1287/2013)
Rikoslaki (39/1889) 38 Luku Tieto- ja viestintärikoksista
Suomen perustuslaki (731/1999)
Tietosuojalaki (1050/2018)
Työsopimuslaki (55/2001)
Vahingonkorvauslaki (412/1974)
Valmiuslaki (1552/2022)
Muut eri toimialojen toimintaa ohjaavat erityislait

Muita tietosuojaa ja tietoturvaa ohjaavia suosituksia:

Tiedonhallintalautakunnan suositukset
DVV:n digiturvajulkaisut (Selvitykset ja raportit, Oppaat ja VAHTI hyvät käytännöt -tukimateriaalit,
Työkalut ja mallipohjat, Ohjeet)
Tietosuojavaltuutetun www-sivut www.tietosuoja.fi