

P A L T A M O

TIETOTURVA- JA
TIETOSUOJAPOLITIIKKA

Kunnanhallitus 17.6.2025 § 158

1	TIETOTURVA- JA TIETOSUOJAPOLITIikka.....	3
1.1.	Tietoturvan ja tietosuojan määritelmä.....	3
1.2.	Tietoturva- ja tietosuojatyön tavoitteet	4
2	TIETOTURVA- JA TIETOSUOJATYÖN HALLINNOINTI, ROOLIT JA VASTUUT.....	6
2.1.	Tietosuojavastaava	6
2.2.	Tietosuojaryhmä.....	6
2.3.	Palvelualuejohtajat	6
2.4.	ICT-palveluiden vastuut	7
2.5.	Arkistotoimi	7
2.6.	Muut kunnan toimijat.....	7
2.7.	Kainuun liiton tietohallintopäällikön vastuut.....	7
2.8.	Tietosuoja- ja tietoturvaorganisaatio pähkinänkuoressa	9
3	TIETOTURVA- JA TIETOSUOJAPERIAATTEET (HALLINTAMALLI)	10
3.1.	Henkilötietojen inventaario/luettelo rekistereistä ja käsittelijöistä	10
3.2.	Tietosuoja- ja tietoturvakoulutus ja ohjeet	10
3.3.	Riskienarviointi ja hallinta.....	10
3.4.	Tietosuoja prosessit	11
4	HENKILÖTIEJOEN KÄSITTELYN PERIAATTEET	12
4.1.	Kunnan tietoturva- ja tietosuoja politiikka ja henkilöstön kouluttaminen	12
4.2.	Tietosuoja hankinnoissa sekä järjestelmä- ja sovelluskehityksessä.....	12
4.2.1	DPIA-vaikutustenarviointi	12
4.3.	Vaatimukset henkilötiedon elinkaaren ajan	13
4.4.	Viranomaisyhteistyö.....	13
4.5.	Rekisteröidyt.....	13
4.6.	Informointi	14
4.7.	Oikeus tulla unohdetuksi	14
5	TIETOTURVALLISUUSTOIMINTA	16
5.1.	Tiedon ja tietojärjestelmien käyttö.....	16
5.2.1	Tekoäly	17
5.2.	Lokitietojen kerääminen	17
6	POIKKEAMIEH HALLINTA JA ILMOITUSVELVOLLISUUS	19
6.1.	Tietosuoja poikkeamien hallintaprosessi	19
6.1.2	Hallinnolliset sakot ja seuraamukset	20

6.2.	Tietoturvapoikkeamien käsittely ja niistä tiedottaminen	21
7	SEURANTA JA VALVONTA	22
7.1.	Tietosuojan vuosikello	22
7.2.	Tietotilinpäättös	23

1 TIETOTURVA- JA TIETOSUOJAPOLITIikka

Tietoturva- ja tietosuojapolitiikka on Paltamon kunnan ylimmän johdon hyväksymä strateginen asiakirja, jonka tavoitteena on luoda yhdenmukaiset toimintaperiaatteet ja käytännöt hyvän tietosuoja- ja tietoturvaton noudattamiseksi. Tietosuoja- ja tietoturvapolitiikassa määritellään kuntaorganisaation tietosuoja- ja tietoturvatyön tavoitteet, vastuut, toimintatavat, valvonta ja seuranta. Poliitikassa määriteltyjä toimintaperiaatteita ja käytäntöjä noudatetaan kunnan kaikessa toiminnassa ja ne koskevat kaikkia kunnan palveluksessa olevia viranhaltijoita, työntekijöitä ja luottamushenkilöitä sekä niitä kunnan sidosryhmien edustajia, jotka toimeksiantojensa puitteissa käsittelevät kunnan omistamaa tai hallinnoimaa tietoa.

1.1. Tietoturvan ja tietosuojan määritelmä

Tietoturvalla tarkoitetaan laajasti erilaisia toimenpiteitä ja keinoja, joilla pyritään suojaamaan eri muodoissa olevia tietoja. Tiedot voivat olla esimerkiksi sähköisesti tallennettuja, välitettyjä tai rekisteröityjä, paperilla olevia, suullisia tai postin kuljettamia. Tietoturva kattaa niin hallinnolliset kuin tekniset näkökulmat ja on olennainen osa organisaation toimintaa sekä normaali- että poikkeusoloissa. Sen tavoitteena on varmistaa tietojen luottamuksellisuus, eheys ja saatavuus sekä vähentää riskejä, jotka voivat vaikuttaa organisaation toimintaan ja asiakkaiden tietoihin.

Hallinnolliset toimenpiteet ovat keskeinen osa tietoturvaa. Näihin kuuluu tietoturvasuunnitelman ja -politiikan laatiminen, jossa määritellään organisaation tietoturvatavoitteet, vastuut ja käytännöt. Tietoturvakäytännöt sisältävät esimerkiksi käyttäjätunnusten ja salasanojen hallinnan, käyttöoikeuksien valvonnan, tietojen säilytys- ja hävittämisohjeet sekä tietojen varmuuskopioinnin ja palauttamisen käytännöt. Lisäksi tietoturvakoulutus ja tietoisuuden lisääminen ovat osa hallinnollisia toimenpiteitä, jotta organisaation henkilöstö ymmärtää tietoturvan merkityksen ja osaa toimia sen vaatimalla tavalla.

Tekniset toimenpiteet liittyvät tietojärjestelmien ja -verkkojen suojaamiseen. Tähän kuuluu muun muassa tietojärjestelmien ja ohjelmistojen päivitysten säännöllinen seuranta ja toteuttaminen, palomuurien ja virustorjuntaohjelmistojen käyttö, salaustekniikoiden hyödyntäminen tiedonsiirrossa sekä tietojen varmuuskopioinnin ja palauttamisen järjestäminen. Lisäksi tietojärjestelmissä käytetään vahvoja käyttäjätunnistusmenetelmiä ja pääsynvalvontajärjestelmiä, jotka rajoittavat käyttöoikeuksia ja estävät luvattoman pääsyn tietoihin.

Poikkeus- ja häiriötilanteiden osalta tietoturvassa on huomioitava toiminnan jatkuvuus ja palveluiden saatavuus. Tämä edellyttää varautumista erilaisiin uhkatekijöihin, kuten luonnonkatastrofeihin, tietoverkkohyökkäyksiin tai laitteiden vikaantumiseen. Paltamon kunnassa on varautumis- ja valmiussuunnitelmat, joissa on määritelty toimenpiteet poikkeustilanteiden varalle. Näihin kuuluu esimerkiksi varajärjestelmien ja -laitteiden käyttöönotto, tietojen varmuuskopioinnin ja palauttamisen suunnittelu sekä henkilöstön ohjeistaminen toimimaan poikkeusoloissa.

Tietoturva on jatkuva prosessi, joka vaatii säännöllistä seurantaa, päivityksiä ja parannuksia vastaamaan uusia uhkia ja haasteita, joita tietoyhteiskunta ja digitaalinen toimintaympäristö tuovat mukanaan.

Tietosuojalla tarkoitetaan henkilötietojen käsittelyä koskevien vaatimusten huomioon ottamista yksityisten ihmisten yksityisyyden, oikeuksien ja oikeusturvan varmistamiseksi. Tietosuoja on perusoikeus, joka turvaa rekisteröidyn oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä. Tietosuojan tarkoituksena on osoittaa, milloin ja millä edellytyksillä henkilötietoja voidaan käsitellä. Keskeinen tietosuojaan liittyvät lainsäädäntö on EU:n tietosuoja-asetus (General Data Protection Regulation, GDPR) sekä tietosuojalaki (1050/2018). Kaikki viranomaiset sekä yritykset, jotka käsittelevät asiakkaiden henkilötietoja, ovat velvollisia noudattamaan tietosuojaan liittyvää lainsäädäntöä.

Henkilötietoja ovat kaikki tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyvät tiedot, esimerkiksi nimi, henkilötunnus, kuva tai biometrinen tieto. Henkilötietojen käsittelyn on aina perustuttava lakiin.

Tietoturva on yksi tietosuojan toteuttamisen keino. Tietoturvan tarkoituksena on suojata tietoaineisto ja tietojärjestelmät. Tieturva tarkoittaa muun muassa organisatorisia ja teknisiä toimenpiteitä, joilla varmistetaan tiedon luottamuksellisuus ja eheys, järjestelmien käytettävyys sekä rekisteröidyn oikeuksien toteutuminen.

Tietosuojakäytäntöjä ja niiden lainmukaisuutta valvovat Suomessa tietosuojaviranomaiset *tietosuojavaltuutettu* ja *tietosuojalautakunta*. Tietosuojavaltuutettu antaa ohjausta ja neuvontaa henkilötietojen käsittelyyn liittyen sekä valvoo henkilötietojen käsittelyä lain tavoitteiden toteuttamiseksi. Tietosuojalautakunta käsittelee henkilötietojen käsittelyyn liittyviä lain soveltamisalan kannalta periaatteellisesti tärkeitä kysymyksiä.

1.2. Tietoturva- ja tietosuojatyön tavoitteet

Tietoturva- ja tietosuojatyön tavoitteiden tulee olla yhteensovitetut kunnan strategisten tavoitteiden ja lainsäädännön kanssa. Niiden on myös vastattava kunnan toimialan erityispiirteitä ja haasteita. Näiden tavoitteiden saavuttamiseksi on tärkeää luoda selkeät linjaukset, vastuut ja toimenpiteet, jotka kattavat koko organisaation ja joihin kaikki kunnan toimijat osallistuvat.

Tavoitteiden saavuttaminen kunnallisessa toiminnassa sisältää seuraavia näkökohtia:

- Tietoturvallisuuden varmistaminen: Kunnan on varmistettava, että sen tietojärjestelmät, tietoverkot ja tietokannat ovat asianmukaisesti suojattuja. Tietoturvallisuustoimenpiteitä voivat olla esimerkiksi palomuurien ja virustorjuntaohjelmistojen käyttö, salausten menetelmien hyödyntäminen sekä käyttäjien tietoturvakoulutus. Lisäksi tulisi kiinnittää huomiota vahvojen käyttäjätunusten ja salasanojen käyttöön, kaksivaiheiseen tunnistautumiseen, tietojen varmuuskopiointiin sekä tietojen käyttöoikeuksien ja käyttöoikeusvalvontamenetelmien hallintaan.
- Tietosuojan noudattaminen: Kunnan on varmistettava, että henkilötietojen käsittely ja tallentaminen tapahtuvat lainmukaisesti ja asianmukaisesti. Tämä sisältää esimerkiksi rekisteriselosteiden laatimisen ja ylläpidon, suostumusten hallinnoinnin sekä tietojen säilyttämisen vain tarvittavan ajan. Henkilötietojen käsittelyssä on noudatettava tarkoitussidonnaisuus- ja minimointiperiaatetta, eli tietoja tulee kerätä ja käyttää vain tarpeellisessa laajuudessa ja tarkoituksessa.

- Riskienhallinta: Kunnan on suoritettava säännöllisesti riskienarviointeja ja -hallintaa, jotta havaitut tietoturvariskit voidaan tunnistaa, arvioida ja minimoida. Riskienhallintaan voi sisältyä haavoittuvuuksien tunnistaminen järjestelmissä, hätäsuunnitelmien luominen ja testaaminen sekä tietoturvaan liittyvien prosessien jatkuvan seurannan varmistaminen. Jatkuva riskienhallinta sisältää myös uusien uhkien ja haavoittuvuuksien seurannan sekä tarvittavien toimenpiteiden toteuttamisen niiden minimoimiseksi.
- Henkilöstön tietoisuuden ja koulutuksen lisääminen: on tärkeää, että henkilöstö ymmärtää tietoturva- ja tietosuojakäytännöt sekä heidän roolinsa tietoturvan ylläpitämisessä. Koulutusohjelmat ja tiedotuskampanjat auttavat henkilöstöä tunnistamaan mahdolliset uhkatilanteet, raportoi-
maan tietoturvaloukkauksista ja ymmärtämään heidän vastuunsa tietojen suojaamisessa.
- Jatkuvan parantamisen periaate: organisaation tulee noudattaa jatkuvan parantamisen periaatetta tietoturva- ja tietosuojatyössä. Toimenpiteitä ja prosesseja tarkastellaan säännöllisesti, jotta voidaan havaita mahdolliset heikkoudet ja tehdä tarvittavat parannukset. Auditoinnit, tarkastukset ja seuranta auttavat varmistamaan, että tietoturvallisuus- ja tietosuojakäytännöt ovat jatkuvasti ajan tasalla ja tehokkaita. Tietoturva- ja tietosuojakäytännöt tulisi arvioida säännöllisesti muuttuvien uhkien ja vaatimusten mukaisesti.

2 TIETOTURVA- JA TIETOSUOJATYÖN HALLINNOINTI, ROOLIT JA VASTUUT

Tietosuoja eli henkilötietojen asianmukainen käsittely sekä tietoturvasta huolehtiminen on koko kunta-organisaation yhteinen asia. Tiedonhallinnan ja asiakirjahallinnon järjestämisestä määrätään Paltamon kunnan hallintosäännössä.

Kunnanhallituksen hyväksymä tietosuoja- ja tietoturvapoliittikka on tietosuojan ja tietoturvan toteuttamisen perusta. Kunnanhallitus asettaa ja nimeää tietosuojavastaavan ja määrittelee hänen tehtäväkuvansa.

2.1. Tietosuojavastaava

Tietosuojavastaavan tehtävänä on asiantuntijana auttaa ylintä johtoa velvoitteidensa toteuttamisessa rekisterinpitäjänä. Tietosuojavastaava osallistuu suunnittelutoimintaan, ohjeiden valmisteluun ja ylläpitoon sekä tietosuojakoulutuksen koordinointiin ja toteutukseen. Tietosuojavastaava seuraa ja valvoo henkilötietojen käsittelyä ja suojausmenettelyä, tukee ja ohjaa henkilökuntaa ja rekisteröityjä tietosuoja-asioissa, toimii yhdysiteenä valvontaviranomaisiin sekä raportoi tietosuojan tilasta ja kehittämistarpeista johdolle.

Tietosuojavastaavan asemasta ja tehtävistä säädetään tietosuoja-asetuksen artiklassa 38 ja 39. Tietosuojavastaavalla on oikeus suorittaa tehtävänsä ja niihin liittyvä suunnittelu, seuranta ja raportointi itsenäisesti. Tietosuojavastaavalla on oikeus organisoida henkilötietojen käsittelyn valvonta, ylläpitää käyttöloki- ja luovutuslokirekistereitä ja ryhtyä jatkotoimenpiteisiin tietosuojan ongelmatilanteissa seuranta- ja valvontasuunnitelman mukaisesti.

2.2. Tietosuojaryhmä

Tietosuojaryhmä tukee tietosuojavastaavaa tietosuojatyössä. Ryhmän tehtäviin kuuluu muun muassa tietosuoja-asetuksen edellyttämien toimenpiteiden toteuttaminen, riskienarviointien tekeminen, dokumentointiin liittyvät tehtävät sekä tietosuojaan liittyvien kysymysten selvittäminen ja raportointi. Tietosuojaryhmään kuuluu tietosuojavastaava, hänen sijaisensa, hallintojohtaja ja ICT-asiantuntija.

2.3. Palvelualuejohtajat

Palvelualuejohtajat vastaavat oman palvelualueensa tietosuojasta ja päättävät siihen kuuluvista kehittämistoiminnan tavoitteista, organisoinnista, resursseista ja toimivaltuuksista sekä tietosuojaa koskevasta sisäisestä ja ulkoisesta tiedottamisesta. Palvelualuejohtajat vastaavat palvelualueensa henkilötietoja sisältävien rekistereiden ylläpidosta, tietosuojaselosteiden olemassaolosta ja rekistereiden vastuuhenkilöiden nimeämisestä. Palvelualuejohtajat antavat henkilötietojen ja asiakirjojen käsittelystä ja menettelytavoista palvelualuekohtaisia ohjeita, jotka esimerkiksi tarkentavat kansallisia suosituksia ja ohjeita sekä alueellisesti sovittuja toimintamalleja.

2.4. ICT-palveluiden vastuut

ICT-palveluista vastaavat Paltamon kunnassa ICT-asiantuntija ja hallintojohtaja. ICT-asiantuntija hallinnoi yhdessä ICT-palveluntuottajan ja tarvittaessa muiden palveluntarjoajien kanssa esimerkiksi tietojärjestelmien toimintaan, ylläpitoon, turvallisuuteen ja käytön riittävään ohjeistukseen liittyvästä toiminnasta. Hän huolehtii tietoturvan vaatimuksista ja osallistuu aktiivisesti kunnan digitalisaation kehittämiseen sekä sen tehokkaaseen hyödyntämiseen kunnan toiminnassa.

ICT-asiantuntija toimii tietosuojavastaavan tukena teknisiin tietosuojaan ja tietoturvaan liittyvissä asioissa. Tämä sisältää esimerkiksi tietosuojan valvontaan ja riskienhallintaan liittyvien käytäntöjen kehittämisen, tietoturvaan liittyvien toimenpiteiden suunnittelun ja toteutuksen sekä tietosuoja-asetuksen vaatimusten noudattamisen varmistamisen.

2.5. Arkistotoimi

Hallintojohtajan johdolla toimivan arkistotoimen vastuulla on varmistaa asiakirjojen käytettävyys, lainmukainen luovuttaminen sekä säilyttäminen arkistonmuodostamissuunnitelman ja lakien mukaisesti.

2.6. Muut kunnan toimijat

Jokaisella kunnan toimijalla on vastuu noudattaa tietoturva- ja tietosuojakäytäntöjä omassa toiminnassaan. Tämä koskee kaikkia työntekijöitä, virkamiehiä, luottamushenkilöitä ja muita henkilöitä, jotka käsittelevät tai ovat vastuussa henkilötiedoista. Jokaisen toimijan vastuulla ja velvollisuutena on raportoida mahdollisista tietoturvapoikkeamista, osallistua koulutuksiin ja noudattaa määriteltyä tietoturva- ja tietosuojapolitiikkaa ja muita ohjeita.

Hankintoja tekevät vastaavat siitä, että tietosuojanäkökohdat arvioidaan hankinnoissa ja tietosuojatoimet sisältyvät ostopalvelusopimuksiin.

Esihenkilöt vastaavat tietosuojan toteutumisesta, henkilörekistereiden lainmukaisesta käytöstä, ohjeiden noudattamisesta sekä tiedottamisesta ja valvonnasta omassa yksikössään. Esihenkilö huolehtii, että henkilöstö on tutustunut kunnan tietosuojapolitiikkaan, tietosuojaohjeisiin ja tehnyt asiakirjojen, tietojen ja tietojärjestelmien vaitiolo- ja salassapitosopimuksen ennen tietojärjestelmien käyttöönottoa. Lisäksi esihenkilö valvoo, että henkilöstö suorittaa tietosuojan verkkokoulutuksen tietosuojavastaavan ohjeistuksen mukaisesti.

Jokainen tietoja käsittelevä henkilö on oman toimintansa osalta vastuussa henkilötietojen asianmukaisesta käsittelystä ja annettujen ohjeiden ja määräysten noudattamisesta tehtäviensä hoidossa.

2.7. Kainuun liiton tietohallintopäällikön vastuut

Tietohallintopäällikön tehtäväkuvaan kuuluu tietohallintopalveluiden kehittäminen ja koordinointi Kainuun kunnille ja Kainuun Liitolle. Hän vastaa palveluiden tarpeiden ja tavoitteiden täyttymisestä yhdessä kuntien ICT-asiantuntijoiden kanssa. Hän hallinnoi myös ulkoistettujen ICT-palveluiden laatua ja varmistaa, että ne vastaavat sovittuja vaatimuksia ja palvelutasoja. Tietohallintopäällikkö vastaa kaikkien ICT-palveluiden toimivuudesta, luotettavuudesta ja saatavuudesta. Hän toimii myös yhteyshenkilönä ICT-

palvelujen sidosryhmille ja varmistaa, että palvelut vastaavat organisaatioiden odotuksia ja tarpeita. Tietohallintopäällikkö tukee kuntien tietosuoja- ja tietoturvapalveluita sekä tietohallintojärjestelmiä yhteistyössä kuntien ICT asiantuntijoiden ja johtajiston kanssa.

2.8. Tietosuoja- ja tietoturvaorganisaatio pähkinänkuoressa

ROOLI	VASTUU	VALVONTAVASTUU
Kunnanhallitus	Tietoturva- ja tietosuojapolitiikan hyväksyminen	Kunnanvaltuusto
	Valvoo, että rekisterinpito on lain mukaista	
	Nimeää tietosuojavastaavan ja hänen varahenkilönsä	
Kunnanjohtaja	Tietoturva- ja tietosuojapolitiikan ylläpitäminen Hyväksyy henkilöstön tietosuojaohjeet, jotka käsitellään yhteisesti johtoryhmässä	Kunnanhallitus
Hallintojohtaja	Tietoturva – ja tietosuojapolitiikan valmistelu	Kunnanjohtaja
	Tietosuojan hallinnointi, ohjeistus ja koordinointi	
	Tietosuojakoulutuksen suunnittelu yhdessä tietosuojavastaavan kanssa	
Tietosuojavastaava	Osallistuu henkilötietojen käsittelyä koskevaan suunnittelutoimintaan	Riippumaton asema
	Ohjaa, neuvoo ja tiedottaa tietosuoja-asioissa	
	Seuraa, että lakeja noudatetaan	
	Kouluttaa ja valvoo	
	Osallistuu vaikutusten arviointien tekoon	
	Raportoi johdolle tietosuojan tilasta ja kehittämistarpeista	
	On rekisteröityjen yhteyshenkilö henkilötietojen käsittelyyn liittyvissä asioissa	
	Tekee yhteistyötä valvontaviranomaisien kanssa ja toimii yhteyspisteenä valvontaviranomaisiin.	
	Tietosuojatietämyksen hankkiminen ja ajan tasalla pitäminen sekä tietämyksen jakaminen	
	Organisaation järjestelmien tietosuojan toteutumisen valvonta	
	Poikkeustilanteiden koordinointi	
Tietosuojaryhmä	Selvittää tietosuojavastaavan apuna onko tietosuojapoikkeamassa kyse tietoturvaloukkauksesta	Kunnanjohtaja
	Selvittää tietosuojavastaavan apuna voidaanko rekisteröidyn tiedot poistaa rekisteröidyn sitä pyytäessä	
	Valmistelee ja valvoo tietosuojadokumentaation ajantasaisuutta	
ICT-asiantuntija	Tietojärjestelmien toiminta, ylläpito, turvallisuus ja käytön ohjeistus	Hallintojohtaja
ICT asiantuntija Palvelualuejohtajat	Digitalisaation kehittäminen	Hallintojohtaja Kunnanjohtaja
	Tietosuojavastaavan tukeminen	
	Tietosuojan toteutuminen alaisessaan toiminnassa	
Palvelualuejohtajat Vastuualueiden ja toimintayksiköiden johtajat	Oman palvelualueen rekistereiden ylläpito, tietosuojaoselosteiden päivitys	Kunnanjohtaja Palvelualuejohtajat
	Tietosuojan toteutuminen alaisessaan toiminnassa	
Esihenkilö	Tietosuojan toteutumisen valvonta alaistensa toiminnassa	Palvelualuejohtajat/ toimintayksiköiden johtajat
	Oman yksikkönsä tietosuojakoulutukseen osallistumisesta huolehtiminen	
	Vastaa, että yksiköllä on sen oman toiminnan erityisvaatimukset huomioiden tarkennetut tietosuojatavoitteet ja periaatteet.	
	Henkilötietojen huolellinen käsitteleminen lainsäädännön ja ohjeistuksen mukaisesti	
Henkilötietojen käsittelijä (työntekijä)	Henkilötietojen huolellinen käsitteleminen lainsäädännön ja organisaation ohjeiden mukaisesti	Esihenkilö, palvelualuejohtaja
Henkilötietojen käsittelijä (ulkoistettu)	Henkilötietojen huolellinen käsitteleminen Paltamon kunnan lukuun kirjallisen sopimuksen ja rekisterinpitäjän ohjeistuksen mukaisesti	Sopimuksen valvoja
Kainuun kuntien tietohallintopäällikkö	Tietohallintopalveluiden kehittäminen yhdessä kuntien kanssa, ulkoistettujen ICT-palveluiden laadun tarkkailu ja valvonta	Kunnanjohtaja

3 TIETOTURVA- JA TIETOSUOJAPERIAATTEET (HALLINTAMALLI)

Kunnan tulee pystyä osoittamaan, että se toteuttaa EU:n tietosuoja-asetuksen ja lain velvoitteet sekä itse asettamansa tavoitteet tietojen käsittelyssä. Tässä luvussa on kuvattu tietosuojan hallinnan ja tietoturvallisuuden eri osa-alueet, jotka kunnan tulee ottaa huomioon toiminnassaan ja tietoturva- ja tietosuoja-työssä.

3.1. Henkilötietojen inventaario/luettelo rekistereistä ja käsittelijöistä

Pääosa henkilörekistereistä ylläpidetään sähköisissä tietojärjestelmissä. Joitakin henkilötietoja voi olla myös manuaalisessa muodossa, esimerkiksi vanhojen pysyvästi säilytettävien asiakirjojen osalta. Henkilötietoja sisältävät prosessit, rekisterit, tietojärjestelmät ja henkilötietojen käsittelijät on lueteltu tiedonhallintamallissa. Tiedonhallintamallin sisältämiä tietoja tarkastellaan ja päivitetään jatkuvasti. Tiedonhallintamallin ylläpidosta vastaa tietosuojavastaava, ICT-asiantuntija ja hallintojohtaja. Kaikista henkilötietoja sisältävistä rekistereistä on tehty tietosuojaselosteet, joita jokainen palvelualue päivittää omalta osaltaan. Tietosuojatyöryhmä muistuttaa ja ohjeistaa dokumentoinnin päivityksestä tietosuojan vuosikellon mukaisesti (luku 7.2).

3.2. Tietosuoja- ja tietoturvakoulutus ja ohjeet

Paltamon kunnassa on käytössä tietosuojan ja tietoturvan verkkokoulutus, jonka suorittamista edellytetään koko henkilöstöltä vuosittain. Koulutuksessa on erilaisia moduuleita, joista voidaan määrittää oikeat koulutusmoduulit kullekin henkilöstöryhmälle.

Organisaation tietosuoja- ja tietoturvaohjeistuksia ylläpidetään Intranetissä.

3.3. Riskienarviointi ja hallinta

Tietosuoja-asetus velvoittaa rekisterinpitäjän arvioimaan henkilötietojen käsittelyyn liittyviä riskejä aina kun se ryhtyy käsittelemään henkilötietoja, käytännössä jatkuvasti. Riskianalyysin avulla on mahdollista tunnistaa jo suunnitteluvaiheessa toimenpiteet, joita riskien hallitseminen ja henkilötietojen asianmukainen käsittely edellyttää. Rekisterinpitäjän tulee varmistaa tietosuojaperiaatteiden tehokas toteutuminen ja vaadittavat resurssit suhteessa käsittelyyn liittyvään riskiin. Toisaalta on arvioitava myös käytettävien resurssien ja tietoturvakeinojen kohtuullisuutta verrattuna arvioituun riskiin.

Riskiarvio on tehtävä rekisteröidyn näkökulmasta, eli rekisterinpitäjän on arvioitava, mitä rekisteröidyn vapauksia ja oikeuksia käsittely voi vaarantaa ja mitä vahinkoja rekisteröidylle voi aiheutua henkilötietojen käsittelystä. Vahinko voi tarkoittaa esimerkiksi riskiä joutua petoksen kohteeksi tai riskiä sosiaaliseen vahinkoon, kuten maineen menetykseen.

Riskien arviointi on jatkuvaa toimintaa, ja riskejä on arvioitava esimerkiksi aina kun uusia tietoteknisiä järjestelmiä otetaan käyttöön. Tietotekniikan kehittyminen on otettava huomioon ja arvioitava, täyttävätkö vanhemmat laitteet tai järjestelmät tietoturvavaatimuksia.

3.4. Tietosuojaprosessit

Paltamon kunnan tietosuojaprosesseja on kuvattu tarkemmin tämän dokumentin muissa luvuissa. Tietosuojaprosessien ytimessä ovat:

- Henkilötietojen käsittelyn periaatteet (luku 4)
- Poikkeamien hallinta ja käsittely (luku 6)
- Seuranta ja valvonta (luku 7)

4 HENKILÖTIETOJEN KÄSITTELYN PERIAATTEET

4.1. Kunnan tietoturva- ja tietosuojapolitiikka ja henkilöstön kouluttaminen

Paltamon kunnan tietoturva- ja tietosuojapolitiikka on keskeinen osa kunnan toimintaa ja sen tavoitteena on varmistaa henkilötietojen suojaaminen ja tietojärjestelmien turvallisuus. Poliitiikka määrittelee ohjeistuksen ja vaatimukset, joiden mukaan henkilöstön tulee toimia tietoturvan ja tietosuojan osalta.

Kunnan henkilöstölle järjestetään säännöllisesti koulutuksia, joiden avulla heidät varustetaan tarvittavalla osaamisella ja tiedolla tietoturva- ja tietosuoja-asioista. Koulutuksissa käsitellään muun muassa tietoturvariskejä, tietosuoja säännöksiä ja käytäntöjä, sekä henkilötietojen asianmukaista käsittelyä. Henkilöstön kouluttaminen on keskeinen osa kunnan pyrkimystä luoda tietoturvakulttuuria, jossa kaikki ymmärtävät oman roolinsa henkilötietojen turvaamisessa.

4.2. Tietosuoja hankinnoissa sekä järjestelmä- ja sovelluskehityksessä

Tietosuoja otetaan huomioon kaikissa hankinnoissa sekä järjestelmä- ja sovelluskehityksessä. Ennen hankintojen tekemistä ja uusien järjestelmien tai sovellusten käyttöönottoa arvioidaan huolellisesti niiden tietosuojaominaisuudet ja -vaatimukset.

Kunnan hankintaprosessissa on vahvat tietosuojanäkökulmat ja tarjouspyynnöissä asetetaan vaatimuksia tietosuojasta huolehtimiselle. Hankittavilta palveluntarjoajilta edellytetään tietosuoja- ja tietoturva-menettelyjen noudattamista sekä sopimuksellisia sitoumuksia henkilötietojen asianmukaisesta käsittelystä.

Järjestelmä- ja sovelluskehityksessä tietosuoja otetaan huomioon jo suunnitteluvaiheessa. Tietosuojan periaatteet sisällytetään kehitysprosessiin, ja käytetään turvallisia suunnittelun ja toteutuksen menetelmiä. Tämä varmistaa, että uudet järjestelmät ja sovellukset täyttävät tietosuojan vaatimukset ja tarjoavat asianmukaisen suojan henkilötiedoille.

4.2.1 DPIA-vaikutustenarviointi

Paltamon kunnassa tulee suorittaa tietosuojaa koskeva vaikutustenarviointi (DPIA) varmistaakseen henkilötietojen käsittelyn lainmukaisuuden ja asianmukaisen riskienhallinnan. DPIA auttaa tunnistamaan mahdolliset riskit ja tarjoaa konkreettisia toimenpide-ehdotuksia niiden hallitsemiseksi. Vaikutustenarviointi on erityisen tärkeää tehdä silloin, kun käsitellään korkean riskin henkilötietoja tai kun käsittelyyn liittyy profilointia, automaattista päätöksentekoa tai esimerkiksi paikannustietoja.

DPIA vaikutustenarvioinnin avulla voidaan varmistaa tietosuojan korkea taso ja noudattaa tietosuoja-asetuksen vaatimuksia. DPIA auttaa ymmärtämään henkilötietojen käsittelyyn liittyvät riskit ja kehittämään asianmukaiset hallintakeinot. Tämä varmistaa, että kuntalaiset voivat luottaa siihen, että heidän henkilötietojensa käsitellään turvallisesti ja lainmukaisesti.

On suositeltavaa hyödyntää tietosuojan asiantuntijoita ja käyttää kattavaa DPIA-menetelmää, jotta varmistetaan arvioinnin perusteellisuus ja tulosten luotettavuus. Paltamon kunnan tulisi dokumentoida ja

seurata DPIA-arvioinnin tuloksia ja toteuttaa tarvittavat toimenpiteet riskien hallitsemiseksi ja tietosuojan parantamiseksi. DPIA-arviointi on jatkuva prosessi, jota tulee päivittää tasaisin väliajoin eri järjestelmiin.

4.3. Vaatimukset henkilötiedon elinkaaren ajan

Organisaatio on asettanut selkeät vaatimukset henkilötiedon elinkaaren eri vaiheille. Näihin vaatimuksiin sisältyy henkilötietojen kerääminen ja tallentaminen, niiden käyttö ja käsittely, säilyttäminen ja poistaminen.

Henkilötietoja kerätään ja tallennetaan ainoastaan tarkoituksiin, jotka on selkeästi määritelty ja perusteltu. Kerättyjä tietoja käytetään ainoastaan niihin tarkoituksiin, joita varten ne on kerätty. Henkilötietoja säilytetään vain niin kauan kuin on tarpeen, ja niiden säilyttämistä koskevat tiedonohjaussuunnitelman mukaiset säilytysajat ja -käytännöt.

Henkilötiedot poistetaan asianmukaisesti ja turvallisesti niiden käytön tarkoituksen päätyttyä tai kun niiden säilyttämiselle ei enää ole tarvetta. Paltamon kunta varmistaa, että henkilötiedot poistetaan pysyvästi ja että tietojen hävittämisessä noudatetaan asianmukaisia turvallisuus- ja tietosuojakäytäntöjä.

4.4. Viranomaisyhteistyö

Paltamon kunta tekee tiivistä yhteistyötä viranomaisten kanssa tietoturva- ja tietosuoja-asioiden osalta. Tämä yhteistyö varmistaa, että kunnan toiminta noudattaa voimassa olevia lakeja, säädöksiä ja määräyksiä.

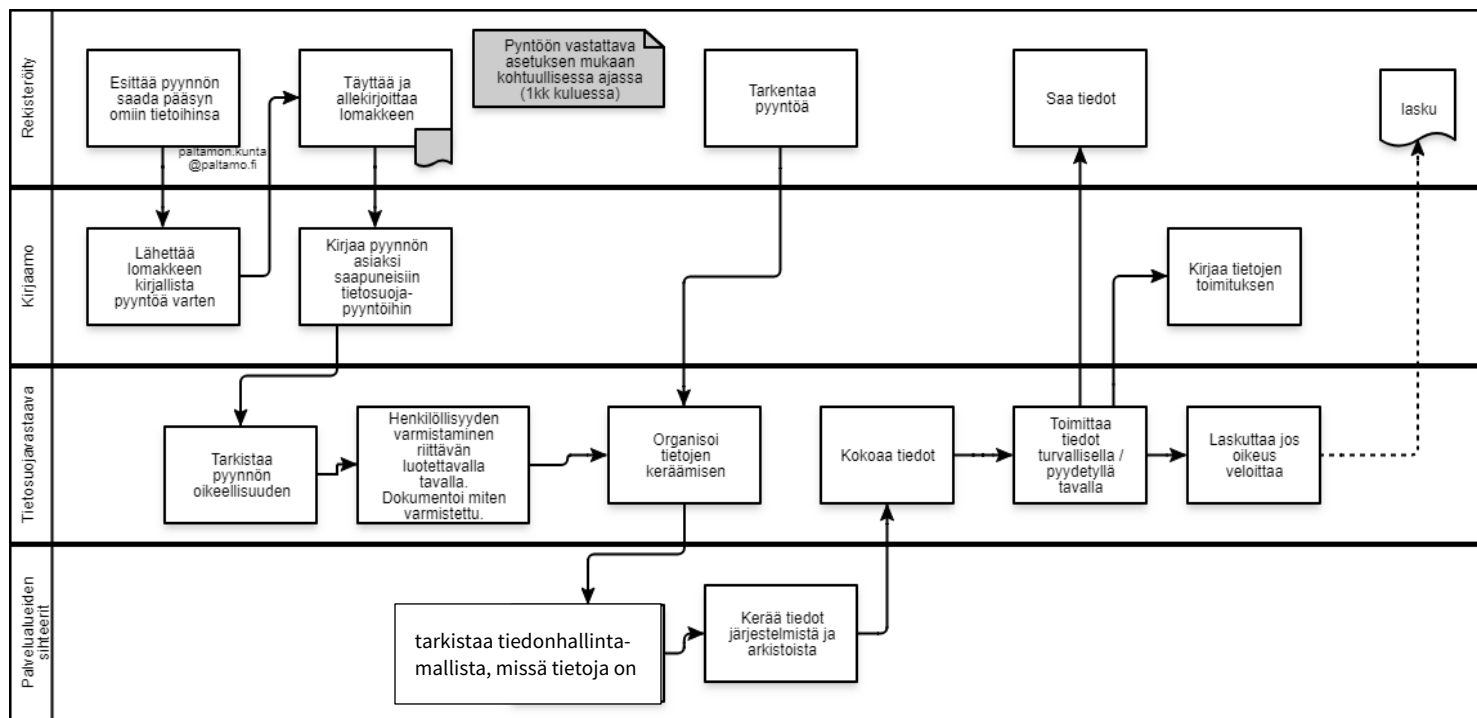
Kunta osallistuu aktiivisesti viranomaisten järjestämiin tietoturva- ja tietosuoja-alan koulutuksiin ja tapahtumiin. Lisäksi kunta ylläpitää jatkuvaa vuoropuhelua viranomaisten kanssa ja seuraa tarkasti alan kehitystä ja muutoksia. Tämä mahdollistaa nopean reagoinnin ja tarvittavien toimenpiteiden toteuttamisen, jos tietoturva- tai tietosuojaan liittyviä riskejä tai haasteita ilmenee.

4.5. Rekisteröidyt

Rekisteröity henkilö tarkoittaa yksilöä, jonka henkilötietoja käsitellään tai tallennetaan. Rekisteröitynä henkilönä voi olla esimerkiksi kuntalainen, asiakas, työntekijä tai muu henkilö, jonka henkilötietoja käsitellään organisaation toimesta.

Rekisteröityyn henkilöön liittyy myös tietosuojaan ja tietoturvaan liittyviä velvollisuuksia organisaatiolle, joka käsittelee hänen henkilötietojaan. Organisaation tulee huolehtia siitä, että rekisteröidyn oikeudet toteutuvat ja että hänen henkilötietojensa käsittely tapahtuu lainmukaisesti, turvallisesti ja asianmukaisesti.

Rekisteröidyllä on oikeus tietää, käsitelläänkö hänen henkilötietojaan vai ei ja mitä häntä koskevia tietoja on tallennettu (TSA artikla 15). Rekisteröidyllä on myös oikeus oikaista virheelliset tiedot, ja rekisterinpitäjän velvollisuus on oikaista tiedot viivytyksettä (artikla 16). Tarkistusoikeuden käyttäminen on lähtökohtaisesti maksutonta. Alla on kuvattu Paltamon kunnan toimintaprosessi rekisteröidyn käyttäessä oikeuttaan saada pääsy henkilötietoihinsa.



4.6. Informointi

Paltamon kunnan tietosuojapolitiikan mukaisesti rekisteröidylle henkilölle tiedotetaan selkeästi ja läpinäkyvästi hänen henkilötietojensa käsittelystä. Tämä informointi tapahtuu pääsääntöisesti tietosuojaselosteen muodossa. Tietosuojaseloste sisältää kattavat tiedot käsittelytarkoituksista, käytetyistä henkilötietoryhmistä, käsittelyn oikeusperusteista ja muista olennaisista tiedoista.

Rekisteröidylle henkilölle kerrotaan myös hänen oikeuksistaan, kuten oikeudesta tarkastaa omat henkilötietonsa, oikeudesta vaatia virheellisten tietojen korjaamista tai poistamista sekä oikeudesta vastustaa tietojen käsittelyä tietyissä tilanteissa.

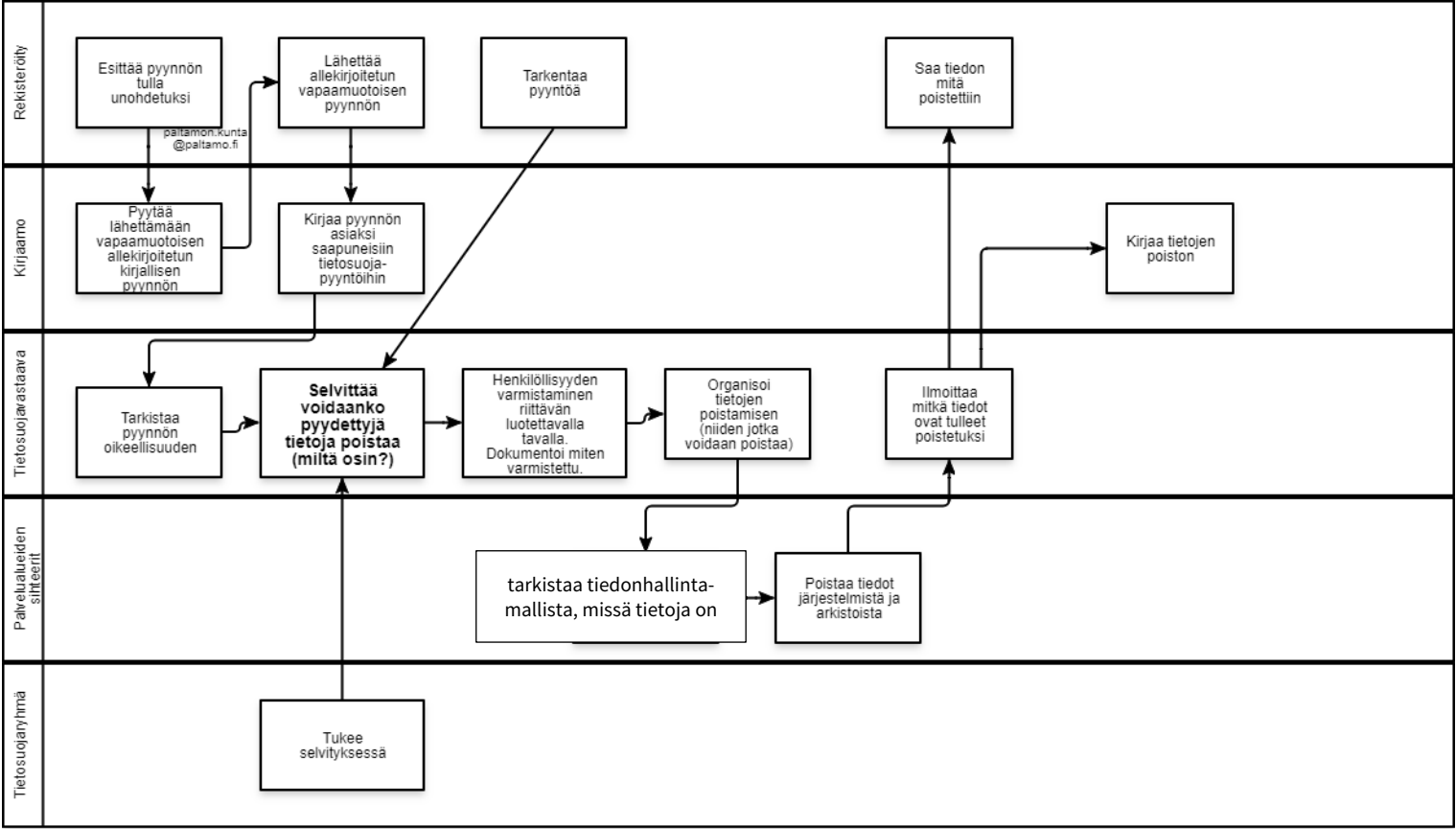
Paltamon kunnan henkilörekisterien tietosuojaselosteet ja rekisteröidyn oikeudet löytyvät kunnan palveluvuorosta osoitteesta <https://www.paltamo.fi/kunta-ja-hallinto/tietosuoja>.

4.7. Oikeus tulla unohdetuksi

Rekisteröidyn oikeudesta tulla unohdetuksi säädetään tietosuoja-asetuksen artiklassa 17. Rekisteröidyllä on oikeus pyytää rekisterin pitäjää poistamaan rekisteröityä koskevat henkilötiedot silloin, kun henkilötietoja ei enää tarvita niihin tarkoituksiin, joita varten ne on kerätty tai rekisterinpitäjällä ei ole enää lakiin perustuvaa tarvetta tietojen säilyttämiselle ja käsittelylle. Tietojen säilyttämisessä ja poistamisessa

noudatetaan kunnan arkistonmuodostussuunnitelmia ja lainsäädännön velvoittamia tietojen säilytysai-koja.

Paltamon kunnassa on määritelty alla oleva toimintaprosessi liittyen rekisteröidyn oikeuteen tulla unoh-detuksi. Tämän prosessin mukaista toimintatapaa noudatetaan silloin, kun rekisteröity haluaa käyttää oikeuttaan tulla unohdetuksi.



5 TIETOTURVALLISUUSTOIMINTA

Tietoturvallisuustoiminta on kokonaisvaltainen prosessi, joka sisältää useita osa-alueita Paltamon kunnan toiminnassa. Se edellyttää tietoturvan suunnittelua, toteutusta, seuranta ja jatkuvaa kehittämistä. Tietoturvallisuustoiminnan tavoitteena on varmistaa, että organisaation tiedot, tietojärjestelmät ja palvelut ovat suojattuja ulkoisilta uhilta, kuten tietomurroilta, haittaohjelmilta ja tietovuodoilta.

Tietoturvallisuustoimintaan kuuluu riskienhallinta, joka sisältää riskien tunnistamisen, arvioinnin ja hallintatoimenpiteiden suunnittelun. Organisaatio tunnistaa mahdolliset tietoturvauhat ja arvioi niiden vaikutukset organisaation toimintaan. Tämän perusteella suunnitellaan ja toteutetaan tarvittavat toimenpiteet riskien hallitsemiseksi ja niiden vaikutusten minimoimiseksi. Riskienhallinta on jatkuvaa ja sisältää myös säännölliset tietoturvatestaukset ja haavoittuvuusarvioinnit.

Toinen tärkeä osa-alue tietoturvallisuustoiminnassa on tietojärjestelmien ja verkkojen valvonta. Paltamon kunnassa käytetään edistynyttä automatisoitua valvontatekniikkaa, joka mahdollistaa tietoturvatapahtumien havaitsemisen, analysoinnin ja reagoinnin niihin nopeasti. Tietoverkkojen liikennettä seurataan jatkuvasti, ja epäilyttäviin tai poikkeaviin tapahtumiin reagoidaan lain edellyttämässä ajassa. Tietoturvapoikkeamien ja -häiriöiden hallintaprosessit on määritelty, ja kriittisissä tilanteissa kunta toimii yhteistyössä alan asiantuntijoiden kanssa.

5.1. Tiedon ja tietojärjestelmien käyttö

Paltamon kunnassa tiedon ja tietojärjestelmien käyttö perustuu vahvaan käytäntöjen ja ohjeistuksen noudattamiseen. Henkilöstön tulee olla tietoinen tietojärjestelmien ja tietojen luottamuksellisuudesta ja noudattaa sovittuja käytäntöjä tietoturvan varmistamiseksi. Käyttäjien tunnistaminen ja oikeuksien hallinta ovat keskeisiä osa-alueita tiedon ja tietojärjestelmien käytössä. Tarkempia tietoturvaan ja -suojaan liittyviä toimintaohjeita ylläpidetään omilla Intra-sivuillaan.

Paltamon kunnassa on käytössä tunnistautumis- ja käyttöoikeushallintajärjestelmä, joka mahdollistaa käyttäjien tunnistamisen ja heille sopivien käyttöoikeuksien myöntämisen. Jokaisella käyttäjällä on yksilöllinen käyttäjätunnus ja salasana, ja käyttäjätunnukset ovat henkilökohtaisia eikä niitä saa jakaa tai luovuttaa toisille henkilöille. Salasanat vaativat vahvan monimutkaisuuden, ja niitä tulee vaihtaa säännöllisesti. Eri palvelujen järjestelmissä voi olla näiden järjestelmien vaatimusten mukaisia muunlaisia tunnus- ja salasanakäytäntöjä.

Pilvipalveluiden käytössä tulee noudattaa tietoturvaohjeita. Tietojen suojaaminen pilvipalveluissa on varmistettava käyttämällä vahvoja salausmenetelmiä ja valitsemalla luotettavia pilvipalveluntarjoajia, jotka täyttävät tietoturva-vaatimukset. Pilvipalveluiden käsittelemä data tulisi olla EU/ETA-alueella erityisesti henkilötietoja käsitteilyssä.

Tietojen salaus on keskeinen osa tiedon ja tietojärjestelmien käyttöä Paltamon kunnassa. Henkilöstöä ohjeistetaan salauksen käytöstä ja tärkeydestä, erityisesti silloin kun käsitellään arkaluonteista tai

henkilötietoja sisältävää tietoa. Salausmenetelmiä käytetään tiedon siirrossa sekä tallennettujen tietojen suojaamisessa.

Tietoturvakoulutus on tärkeä osa tiedon ja tietojärjestelmien käyttöä koskevaa politiikkaa. Paltamon kunnassa on käytössä tietosuoja ja tietoturvan verkkokoulutus, jonka suorittamista edellytetään koko henkilöstöltä vuosittain. Lisäksi organisaatiossa tuetaan lisäkouluttautumista esimerkiksi tietoturva-uhkiin, tietosuojaan, salausmenetelmiin, tietojen luottamuksellisuuteen ja muihin tietoturvaan liittyviin aiheisiin.

Tietoturvallisuustoimintaan kuuluu myös tietojen varmuuskopiointi ja palauttamisprosessit, tietojen salausmenetelmien käyttö sekä tietojärjestelmien jatkuvuuden varmistaminen häiriötilanteissa. Kunta seuraa jatkuvasti tietoturvallisuustoimenpiteiden tehokkuutta ja kehittää niitä tarvittaessa vastaamaan muuttuvia uhkia ja vaatimuksia. Tietoturvallisuustoiminnan päivittämisestä ja seurannasta vastaa ICT-asiantuntija yhdessä organisaation johdon kanssa.

5.2.1 Tekoäly

Tekoälytekniologioiden käyttö Paltamon kunnan toiminnassa edellyttää erityistä huomiota tietoturvaan ja tietosuojaan. Tekoälyjärjestelmien kehittämisessä ja käytössä tulee noudattaa seuraavia periaatteita:

- **Läpinäkyvyys:** Tekoälyjärjestelmien toiminnan tulee olla läpinäkyvää ja selitettävää. Käyttäjille tulee tarjota riittävästi tietoa tekoälyn toiminnasta ja sen päätöksenteon perusteista.
- **Tietojen anonymisointi:** Tekoälyjärjestelmissä käytettävät henkilötiedot tulee anonymisoida aina kun mahdollista, jotta yksityisyyden suoja voidaan varmistaa.
- **Eettisyys:** Tekoälyn käyttöön liittyvät eettiset kysymykset tulee huomioida ja varmistaa, että tekoälyjärjestelmät toimivat oikeudenmukaisesti ja syrjimättömästi.
- **Riskienhallinta:** Tekoälyjärjestelmien käyttöön liittyvät riskit tulee arvioida ja hallita huolellisesti. Tämä sisältää mahdollisten tietoturva-uhkien tunnistamisen ja niihin varautumisen.
- **Jatkuva seuranta ja arviointi:** Tekoälyjärjestelmien toimintaa tulee seurata ja arvioida jatkuvasti, jotta voidaan varmistaa niiden tietoturvallisuus ja tietosuoja.

Paltamon kunta laatii yhdessä muiden Kainuun kuntien sekä Kainuun liiton kanssa erillisen tekoälypolitiikan dokumentaation.

5.2. Lokitietojen kerääminen

Paltamon kunnassa toteutetaan aktiivista lokitietojen keräämistä ja valvontaa tietoturvallisuuden varmistamiseksi. Lokitietoja kerätään tietojärjestelmien ja verkkojen tapahtumista, kuten sisäänkirjautumisista, tiedostojen käytöstä ja muista merkittävistä tapahtumista. Lokitietojen avulla voidaan havaita ja reagoida mahdollisiin tietoturvaloukkauksiin ja väärinkäytöksiin sekä suorittaa jälkikäteistarkastuksia. Lokitiedot ovat myös henkilötietoja, joten niiden käsittelyssä tulee huomioida tiedonhallintalainsäädännön mukainen tarpeellisuusarviointi sekä tietosuojalainsäädäntö.

Lokien keräämiselle tulee olla peruste ja käsittelytavat sekä vastuut määritelty. Lokeihin tallentuvien tietojen tyypit ja suojaustarpeet tulee tunnistaa ja määritellä. Pääsyä lokitietoihin tulee kontrolloida pääsy-oikeushallinnalla ja lähtökohtaisesti käyttäjien pääsy tulee olla eväty, silloin kun henkilön työtehtävät eivät pääsyä edellytä. Luottamuksen säilyttämiseksi lokeja ei tule oikeudettomasti muuttaa tai tuhota.

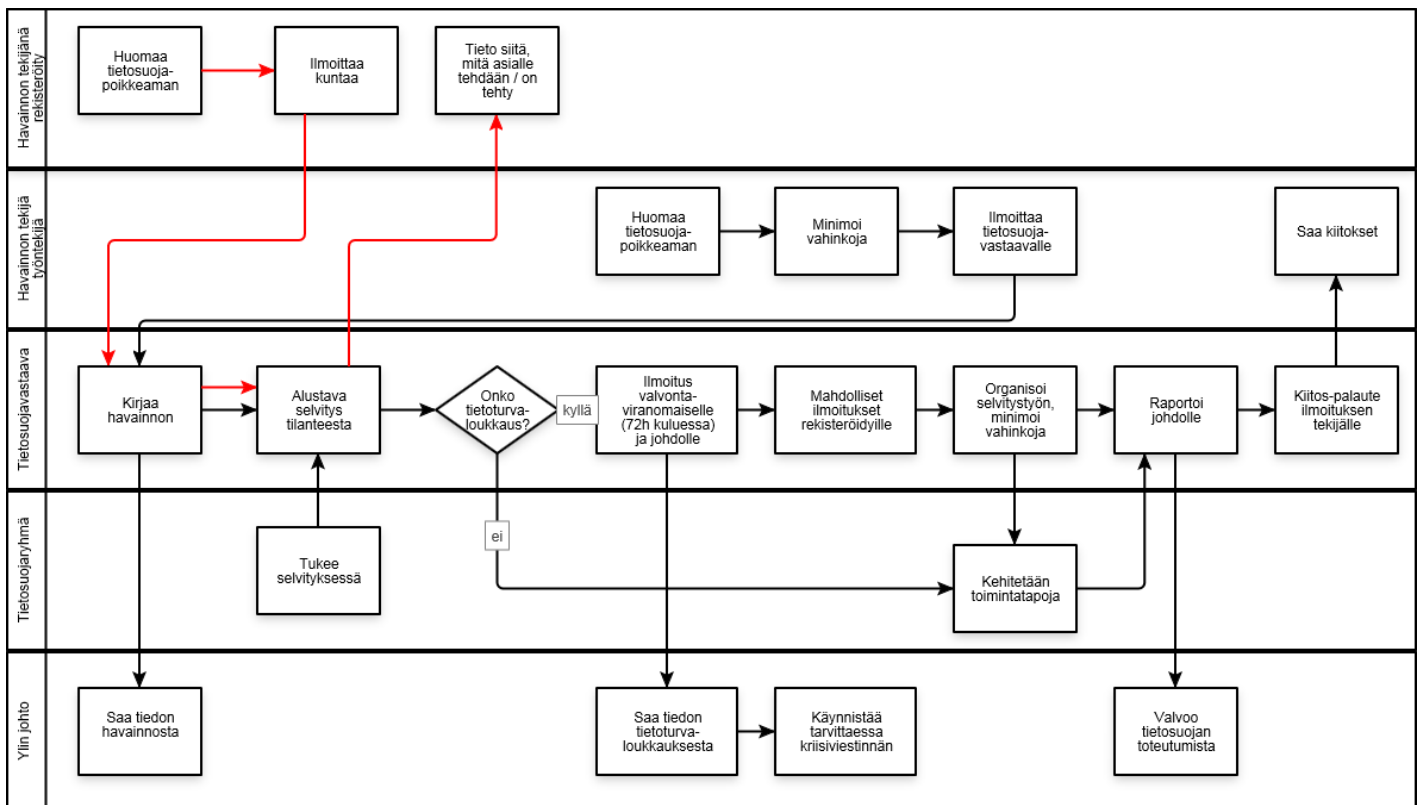
6 POIKKEAMIEN HALLINTA JA ILMOITUSVELVOLLISUUS

6.1. Tietosuojapoikkeamien hallintaprosessi

Paltamon kunnassa on määritelty alla oleva toimintaprosessi tietosuojapoikkeamien hallintaan ja käsittelyyn. Prosessia noudatetaan tietosuojapoikkeamien sattuessa.

Tapahtuneista poikkeamista pidetään luetteloa ja jokaisen poikkeaman käsittelyprosessi dokumentoidaan. Rekisterinpitäjä arvioi, minkä tasoinen riski tietoturvaloukkauksesta aiheutuu sen kohteina olleille henkilöille, ja riskin taso määrittää ne toimenpiteet, joihin rekisterinpitäjän on ryhdyttävä.

Tietosuojapoikkeaman sattuessa Paltamon kunnalla on rekisterinpitäjänä ilmoitusvelvollisuus valvontaviranomaiselle (tietosuoja-valtuutettu) sekä rekisteröidylle, jota poikkeama koskee ja jonka henkilötiedot ovat mahdollisesti vaarantuneet. Valvontaviranomaiselle tehdään ilmoitus tietosuoja-asetuksen mukaisesti 72 tunnin kuluessa siitä, kun poikkeama on tullut ilmi. Rekisteröidylle tietosuojapoikkeamasta ilmoitetaan ilman aiheetonta viivytystä.



6.1.2 Hallinnolliset sakot ja seuraamukset

Tietosuojapoikkeamat ja -rikkomukset käsitellään aina tapauskohtaisesti. Mahdollisiin seuraamuksiin sovelletaan alla olevaa tietosuojarikkomusten seuraamustaulukkoa. Rikkomuksissa arvioidaan teon tahallisuuden astetta ja rikkomuksen vakavuutta.

TEON TAHALLISUUDEN ASTE			
	Tietämättömyys Osaamattomuus Huolimattomuus Vahinko Tahattomuus	Piittaamattomuus Törkeä huolimattomuus Välinpitämättömyys Tahallisuus Toistuvuus	Rikoksentekotarkoitus (vahingonteko, luvaton käyttö, vakoilu, salassapitorikos, aseman/väärinkäyttö) Hyötymistarkoitus
Vakava rikkomus/rikos Liikesalaisuuden luvaton käsittely ja luovuttaminen Hakkerointi, tunkeutuminen Rikoslain alaisen materiaalin oikeudeton käsittely Tekijänoikeuslain alaisen materiaalin laiton levittäminen Virusten tahallinen levittäminen Tahallinen huolimattomuus henkilötietojen käsittelyssä	Työnantaja käynnistää palvelussuhteen päättämisenmenettelyn Tutkintapyyntöä poliisille harkitaan Kirjallinen varoitus	Työnantaja käynnistää palvelussuhteen päättämisenmenettelyn Tutkintapyyntö poliisille Kirjallinen varoitus	Työnantaja käynnistää palvelussuhteen päättämisenmenettelyn Tutkintapyyntö poliisille
Rikkomus (vakava väärinkäyttö tai turvallisuuden vaarantaminen) Ohjelmien ja pelien luvaton kopiointi Luvattomien ohjelmien asentaminen Ylläpitäjän työkalujen luvaton hallussapito Palvelun luvaton pystytys Tunnuksen luovuttaminen Tiedon luottamuksellisuuden vaarantaminen Huolimattomuus henkilötietojen käsittelyssä	Kirjallinen varoitus Huomautus	Työnantaja käynnistää palvelussuhteen päättämisenmenettelyn Käyttöoikeuden peruminen Kirjallinen varoitus	Työnantaja käynnistää palvelussuhteen päättämisenmenettelyn Tutkintapyyntö poliisille Kirjallinen varoitus
Lievä rikkomus (väärinkäytös) Henkilökohtaisen tietoturvan laiminlyönti Epäasiallinen käytös Haitan aiheuttaminen Resurssien tuhlaus Virustorjunnan laiminlyönti Luvaton kaupallinen tai poliittinen toiminta Kulunvalvontasääntöjen rikkominen Tahaton huolimattomuus henkilötietojen käsittelyssä	Huomautus Opastus Puheeksi ottaminen	Kirjallinen varoitus Opastus Huomautus Puheeksi ottaminen	Tutkintapyyntöä poliisille harkitaan Kirjallinen varoitus

Tietosuojavaltuutetun toimisto voi rikkomusten vakavuudesta riippuen määrätä rekisterinpitäjälle tai henkilötietojen käsittelijälle seuraamuksia, kuten varoituksen, huomautuksen tai vakavissa tapauksissa seuraamusmaksun.

6.2. Tietoturvapoikkeamien käsittely ja niistä tiedottaminen

Tietoturva- ja tietosuojaohjeiden noudattamista valvotaan säännöllisin rutiinein, automaattisesti sekä pistokokein. Väärinkäyttöihin puututaan.

Sekä odottamattomista että ennalta tiedetyistä palvelukatkoksista ja muista tietojärjestelmien käytön häiriöistä tiedotetaan Paltamon kunnan tavanomaisia tiedotuskanavia hyödyntäen. Järjestelmän omistaja tiedottaa käyttöhäiriöistä niiden edellyttämässä laajuudessa.

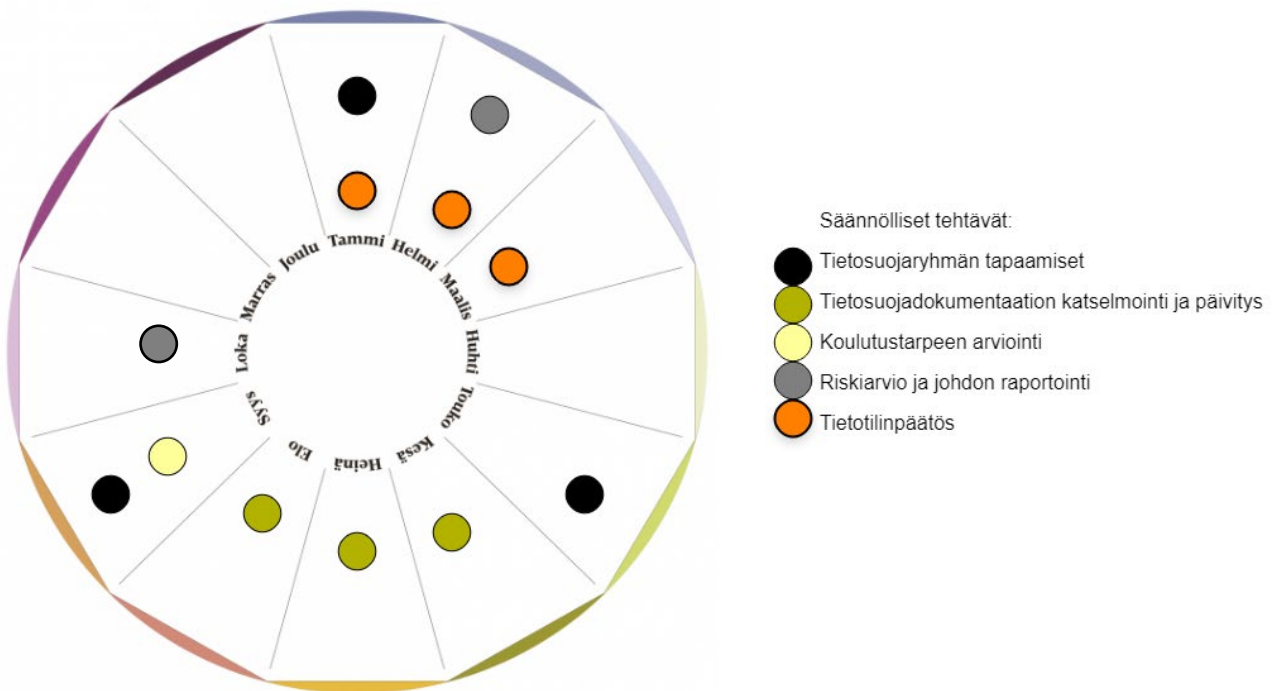
Tietoturvapoikkeamat käsitellään ja niistä raportoidaan johdolle erikseen ohjeistetulla tavalla. Muulle organisaatiolle havaituista poikkeamista tiedotetaan niiden luonteen ja laajuuden edellyttämällä tavalla.

Tietoturvaloukkauksissa noudatetaan EU:n yleisen tietosuoja-asetuksen määräyksiä henkilötietojen tietoturvaloukkauksen ilmoittamisesta valvontaviranomaiselle ja rekisteröidylle artiklojen 33 ja 34 mukaisesti.

7 SEURANTA JA VALVONTA

7.1. Tietosuoja vuosikello

Tietosuoja vuosikellossa on määritelty kuukausitasolla ajankohdat säännöllisille, vuosittain toistuville tietosuoja toimenpiteille. Tietosuojaryhmä kokoontuu aina tarvittaessa, mutta vähintään kolme kertaa vuodessa.



Tapaamisten aiheita ovat

- uusien ohjeistusten tai oikeuskäytännön muutosten seuranta
- tärkeimpien järjestelmähankkeiden ja muutosten tilanne
- rekisteröidyltä ja valvontaviranomaisilta tulleet yhteydenotot
- tietoturvatapahtumien käsittely
- yleisesti tietosuojaan liittyvät havaitut puutteet ja tarpeet
- vaikutustenarvioinnit

Tapaamisissa käsitellään myös kulloinkin ajankohtaiset, tämän tietoturva- ja tietosuojapolitiikan mukaiset dokumentaatiot, raportoinnit ja toimenpiteet:

- Tammikuun tapaamisessa valmistellaan tietotilinpäätöstä ja johdon raportointia edellisen vuoden osalta.
- Toukokuun tapaamisessa käydään läpi tietosuojadokumentaation tilannetta ja jaetaan päivitysvastuut. Vastuu henkilötietorekistereiden tietosuojaselosteiden päivityksestä on palvelualueilla, ja tietosuojatyöryhmä muistuttaa, ohjeistaa ja seuraa päivityksiä.
- Syyskuun tapaamisessa arvioidaan koulutustarpeita ja tarkastetaan henkilöstön tietosuojakoulutuksen suorituserät. Tarvittaessa muistutetaan ja opastetaan tietosuojakoulutuksen

suorittamisessa.

Tietosuojaryhmä, johon kuuluvat tietosuojavastaava, hänen varahenkilönsä, hallintojohtaja ja ICT-asiantuntija, voi kutsua tapaamisiin tarvittaessa mukaan esimerkiksi kunnanjohtajan, palvelualuejohtajia tai esihenkilöitä, mikäli heidän asiantuntijuuttaan tarvitaan jonkin asian käsittelyssä.

7.2. Tietotilinpäätös

Tietotilinpäätös on kerran vuodessa tehtävä sisäisen tietojohdamisen raportti, joka laaditaan kunnan tietotilinpäätöksen ja toimintakertomuksen liitteeksi. Tietotilinpäätös antaa kokonaiskuvan tietojenkäsittelyn tilasta ja kehittämistoimenpiteistä. Dokumentilla on rooli osoitusvelvollisuuden, läpinäkyvyyden ja avoimuuden osoittajana.

Tietotilinpäätöksen on tarkoitus antaa tilannekuva henkilötietojen käsittelyn, tiedonhallinnan ja tietoturvan tilasta. Raporttiin koostetaan myös vuoden aikana tehdyt kehittämistoimenpiteet ja arvioidaan seuraavat muutos- ja kehittämistarpeet. Tietotilinpäätökseen voidaan kerätä myös tilastotietoa esimerkiksi suoritettujen tietoturvakoulutusten määrästä, rekisteröityjen yhteydenotoista ja tietosuojapoikkeamista.

Esimerkki tietotilinpäätöksen sisällöstä

1. Johdanto
2. Tietosuojan ja tietoturvallisuuden toteuttaminen
3. Tiedonhallinta, tietovarannot ja tietovirrat
4. Lainsäädäntö ja muu ohjeistus
5. Rekisteröidyn oikeuksien toteutuminen
6. Arviointi, kehittäminen ja tiedon hyödyntäminen
7. Suunnitelma tuleville vuosille
8. Seuranta ja mittarit