

PADASJOEN KUNTA TIEOTILINPÄÄTÖS 2025

Pituus: 15 sivua

Aikataulutus: Kerran vuodessa, muulloin pyydettyäessä

Tarkoitus: Osoitusvelvollisuuden toteennäyttäminen, organisaation tietojen käsittelyn kuvaus, sisäisen valvonnan työkalu, suunnittelun ja toiminnanohjauksen sekä raportoinnin ja johtamisen tuki.

Päiväys ja laatija: 24.3.2026, Markku Lahtinen ja Pia Mustisto

Hyväksyntä: Kunnanhallitus 30.3.2026

SISÄLLYS

Julkinen tiivistelmä	2
Yleiskatsaus	3
Lainsäädäntö ja muu ohjeistus	5
Keskeinen lainsäädäntö	5
Ohjeistukset ja viitekehykset	5
Toimintapolitiikat ja strategiat	5
Sertifiointit ja standardit	5
Tiedonhallinnan toteuttaminen	6
Tiedonhallinnan organisointi	6
Tietoturvan ja tietosuojan organisointi	7
Tekniset ja organisatoriset toimenpiteet	8
Riskienhallinta	9
Tarkastukset	10
Tietoturvapoikkeamien käsittely	10
Tietovarannot ja tietovirrat	10
Tiedon elinkaaren hallinta	11
Tietovarannot	11
Asianhallinta ja sähköinen asiointi	11
Asiakirjahallinto ja arkistotoimi	11
Koulutus ja kehittäminen	12
Koulutus	12
Ohjeistus	12
Kehittäminen	12
Rekisteröidyn oikeuksien toteutuminen	12
Seuranta ja mittarit	14

Tietotilinpäättös kuvaa Padasjoen kunnan henkilötietojen käsittelyn, tietoturvan ja tiedonhallinnan tilaa sekä vuoden aikana tehtyjä kehittämistoimenpiteitä. Vuosi painottui erityisesti tietosuojan, tiedonhallintamallin ja teknisten suojatoimien kehittämiseen.

Keskeisimpiä tapahtumia olivat työllisyydenhoidon vastuiden siirron myötä kasvaneet tietovirrat kuntien ja työllisyysalueen välillä sekä uuden asiakastietojärjestelmän käyttöönotto. Tietosuoja-asiakirjojen päivitystä jatkettiin ja rekisteröityjen informointia varten olevat selosteet ovat edelleen viimeistelyvaiheessa.

Tietoturvassa painopisteenä oli teknisten ja organisatoristen kontrollien kehittäminen, kuten vahva tunnistautuminen, salaukset ja Intune-laitehallinta. Vuonna 2025 ei havaittu tietoturvaloukkauksia. Henkilöstön ja luottamushenkilöiden tietoturvakoulutusten suoritusaste jäi matalaksi (50 % ja 35 %).

Kokonaisuutena kunnan tietosuoja- ja tietoturvatoiminta on perustasolla, mutta keskeisiä kehitystarpeita ovat tiedonohjaus, selosteiden valmistuminen, koulutusten läpivienti ja resurssien riittävyys.

Tietotilinpäätös tarjoaa ajantasaisen tilannekuvan organisaation henkilötietojen käsittelyn nykytilasta sekä arvion tietosuojan toteutumisesta. Tietotilinpäätöksessä kartoitetaan henkilötietojen käsittelyyn liittyviä kehittämistarpeita ja niiden edellyttämiä toimenpiteitä. Tavoitteena on tukea tietosuojatyön tekemistä ja lisätä tekemisen vaikuttavuutta. Tietotilinpäätös toimii myös yhtenä osoitusvelvollisuuden osoittamisen välineenä ja sisäisen ja ulkoisen valvonnan raporttina. Osoitusvelvollisuuteen kuuluu mm. se, että organisaation sopimuksissa ja alihankinnoissa on huomioitu tietosuojan ja -turvan vaatimukset. Lisäksi rekisterinpitäjä tulee huomioida rekisteröidyn henkilötietojen käsittelyyn kohdistuvat riskit. Rekisterinpitäjän tulee huolehtia siitä, että henkilöstöllä ja ulkopuolisilla henkilötietojen käsittelijöillä on tarvittava ohjeistus ja osaaminen.

Rekisterinpitäjän tulee myös seurata, raportoida ja valvoa tietosuojan ja -turvaan liittyviä asioita ja huolehtia siitä, että tietosuojan koskeva sääntely toteutuu organisaatiossa. Osoitusvelvollisuuteen kuuluu myös sisäänrakennetun tietosuojan vaatimus, millä tarkoitetaan sitä, että tietosuojaperiaatteet toteutuvat kaikissa käsittelyn vaiheissa. Tietosuojaperiaatteet (5 art.) ovat 1. lainmukaisuuden, kohtuullisen ja läpinäkyvyyden periaate, 2. käyttötarkoitussidonnaisuuden periaate, 3. tietojen minimoinnin periaate 4. täsmällisyyden periaate, 5. säilytyksen rajoittamisen periaate ja 6. eheyden ja luottamuksellisuuden periaate.

Tietotilinpäätöksellä voidaan lisätä luottamusta siihen, että organisaatiossa noudatetaan edellä mainittuja tietosuojaperiaatteita ja käsitellään henkilötietoja sen mukaisesti. Hyvin hoidetulla tietosuojatyöllä vaikutetaan organisaation tehokkuuteen ja kilpailukykyyn. Tietosuojasääntely koostuu tietosuoja-asetuksesta, kansallisesta tietosuojalaista sekä erityislainsäädännöstä. Suomessa tietosuojavaltuutetun toimisto valvoo tietosuojalainsäädännön noudattamista.

Padasjoen kunnan tietotilinpäätöksellä päätehtävä on laajempi tiedonhallinnan kokonaisuuden tarkastelu; organisaation tiedonhallinnan laadun ja turvallisuuden seuranta ja kehittäminen sekä osoitusvelvollisuuden huomioiminen.

Tietotilinpäätöksen valmistelee kunnan tietosuojavastaavat yhdessä asianhallinta- ja tietoturvaryhmän kanssa. Tietotilinpäätös käsitellään vuosittain kunnan johtoryhmässä sekä kunnanhallituksessa.

Asianhallintajärjestelmään tehtiin AD-integraatio kirjautumista ja käyttäjähallintaa varten. Toteutus tehtiin jo vuoden 2024 lopulla, mutta todellinen jalkauttaminen tapahtui vuoden 2025 alussa. Integraation toteutus onnistui kohtalaisen hyvin eikä loppuvuonna asiasta tarvinnut enää muistuttaa.

Työllisyydenhoidon vastuiden siirryttyä kunnille vuoden 2025 alusta, lisääntyi tiedonvaihto perustetun työllisyysalueen ja kunnan työllisyyspalveluiden välillä. Roolien ja tiedonvaihdon tason muututtua tehtiin päivitykset myös työllisyydenhoidon dokumenttien hallinnan ohjeistukseen. Henkilötietojen käsittelyn ja keräämisen tarkoitukseen lisättiin työ- ja työskentelykyyn sekä työllistymisen edistämiseen liittyvät henkilötiedot, joita aikaisemmasta poiketen alettiin kirjata säännönmukaisesti.

Tietojen luovutus muuttui työllistymisen ja kotoutumisen edistämispohjaiseksi, jolla perusteella asiakkaan tietoja voidaan luovuttaa aikaisempaa useammille yhteistyötahoille. Myös työllisyyspalveluiden työntekijöitä koskeva tietojen kirjaamisohje päivitettiin vastaamaan uudistuneita käytäntöjä.

Vuoden 2025 aikana käyttöön otettiin uusi asiakastietojärjestelmä, jolloin tietojen säilytyspaikkana on järjestelmän ylläpitäjän säilytyspaikka Helsingissä. Säilytyspaikkatiedon keräämisen yhteydessä tietosuojaselostetta varten selvitettiin myös tietojen mahdollinen siirtäminen EU-alueen ulkopuolelle. Tietoja ei siirretä EU:n ulkopuolelle.

Tietosuojan osalta vuoden 2025 loppupuoliskolla aloitettiin tietosuojaselosteiden kartoitus ja puuttuvien tekeminen. Osa selosteista tehtiin tietosuojaparin yhteistyöskentelynä, mutta myös muita

rekisterinpitäjiä ja vastuuhenkilöitä kontaktoitiin päivitysten merkeissä. Samalla päivitettiin ole-massa oleva mallipohja.

Tiedonhallintamallia aloitettiin päivittämään ensimmäistä kertaa noin vuoden tämän hyväksynnän jälkeen. Osa tunnistetuista prosesseista saatiin päivitettyä sekä uusia löydettyä, mutta suurin osa tiedoista eri tulosalueiden osalta jäi päivittämättä pyynnöistä huolimatta.

Tietosuojan näkökulmasta helpotusta tietojen siirtoihin EU:n ja Yhdysvaltojen välillä toi Euroopan komission heinäkuussa 2023 antama päätös tietosuojan riittävästä tasosta. Tietosuojan riittävyys-päätöksen perusteella tietoja voidaan siirtää EU- ja ETA –alueelta järjestelyyn osallistuville yhdysval-talaisille yrityksille ilman erillistä tietosuoja-asetuksen 46 artiklan mukaista siirtooperustetta. Järjes-telmään sertifioituneille ja EU:n ja Yhdysvaltojen väliseen tietosuojakehyksessä sovittuihin suojatoi-miin sitoutuneille yhdysvaltalaisille yrityksille voidaan riittävyyspäätöksen nojalla siirtää henkilötie-toja. Riittävyyspäätöstä ei voi kuitenkaan käyttää tiedonsiirtoihin julkisen sektorin toimijoiden välillä.

Tietotilinpäätös on Padasjoen kunnassa ensimmäinen laatuaan ja sisällöltään täten varmasti osittain puutteellinen. Asiakirjan laatimisessa on käytetty hyväksi tekoälyä.

LAINSÄÄDÄNTÖ JA MUU OHJEISTUS

Julkishallinnon organisaatiot noudattavat Suomen ja EU:n lainsäädäntöä. Organisaatioita ohjaavat mm. hallintolaki, julkisuuslaki, tietosuoja-asetus, tietosuoja-laki, tiedonhallintalaki, arkistolaki sekä lukuiset muut yleis- ja erityislait. Lisäksi rahoittajat (projektit, hankkeet) antavat omia ohjeistuksia henkilötietojen käsittelystä, säilyttämisestä ja arkistoinnista. Organisaatio voi toimia myös käsittelijänä toisen rekisterinpitäjän lukuun. Sen lisäksi organisaatioilla on omia käytännesääntöjä ja ohjeistuksia sekä kansallisia tai kansainvälisiä sertifikaatteja. Organisaatioissa on myös omavalvontaa, sisäisiä tarkastuksia ja auditointeja. Tässä luvussa tehtävänä käydään läpi lainsäädännöllistä ja omien ohjeistuksiin ja politiikkoihin liittyviä taustoja tietojenkäsittelyn osalta. Toisaalta tiedon laatuun ja käytettävyyteen liittyvät tekijät tulisi myös huomioida tietotilinpäätöksessä. Tässä luvussa vastataan tietosuojaperiaatteiden kysymyksiin koskien tietojenkäsittelyn lainmukaisuutta, kohtuullisuutta ja läpinäkyvyyttä.

Kunnan tietojen käsittelyä ohjaavat useat kansalliset ja EU-tason säädökset, viranomaisohjeet sekä sisäiset politiikat ja strategiat. Tietotilinpäätöksen tarkoituksena on kuvata, miten nämä vaatimukset toteutuvat käytännössä ja miten organisaatio varmistaa jatkuvan vaatimustenmukaisuuden.

Padasjoen kunnassa toteutetaan säännöllisiä sisäisiä auditointeja tietoturvan ja tietosuojan toteutumisesta, johdon katselmuksia riskienhallinnan ja vaatimustenmukaisuuden varmistamiseksi sekä tarvittaessa ulkoisia auditointeja tietosuojan ja -turvan vaatimusten täyttämiseksi.

KESKEINEN LAINSÄÄDÄNTÖ

- EU:n yleinen tietosuoja-asetus (GDPR, EU 2016/679), määrittää henkilötietojen käsittelyn periaatteet, rekisteröidyn oikeudet ja osoitusvelvollisuuden
- Tietosuoja-laki (1050/2018), täsmentää GDPR:n kansallista soveltamista Suomessa
- Tiedonhallintalaki (906/2019), ohjaa julkisen hallinnon tiedonhallintaa ja tietovarantojen hallintaa
- Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003) ja Laki julkisuusperiaatteesta (621/1999), määrittävät tiedon saatavuuden ja avoimuuden
- Asiakastietolaki (703/2021)

OHJEISTUKSET JA VIITEKEHYKSET

- VAHTI-ohjeet (Valtiovarainministeriön tietoturvaohjeistus), hyvät käytännöt tietoturvan ja tietosuojan toteuttamiseen julkisessa hallinnossa
- Tietosuojavaaltuutetun ohjeet, mm. vaikutustenarvioinnit, rekisteröidyn oikeudet ja riskienhallinta
- Kyberturvallisuuskeskuksen suositukset, tekniset ja organisatoriset tietoturvatoimet.

TOIMINTAPOLITIIKAT JA STRATEGIAT

Organisaatiolla on käytössä:

- Tietoturva- ja tietosuojapolitiikka, jotka määrittävät periaatteet ja vastuut
- Tietoturva- ja tietosuojariskienhallinta

SERTIFIOINNIT JA STANDARDIT

- ISO/IEC 27001, kansainvälinen tietoturvan hallintajärjestelmän standardi, joka erityisesti palveluntarjoajilla laajasti käytössä
- Katakri, kansallinen turvallisuusauditointikriteeristö (erityisesti julkishallinnossa)

TIEDONHALLINNAN TOTEUTTAMINEN

Tietosuoja-asetuksen (artikla 24) mukaan rekisterinpitäjä on vastuussa siitä, että se toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet, joilla osoitetaan, että henkilötietojen käsittelyssä noudatetaan tietosuoja-asetuksen vaatimuksia. Rekisterinpitäjän on huomioitava henkilötietojen käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudelta vaihtelevat riskit ja suhteuttava toimenpiteet näiden mukaisesti. Teknisillä ja organisatorisilla toimenpiteillä tarkoitetaan esimerkiksi henkilöstön koulutuksia, sisäisiä ohjeistuksia ja määräyksiä, salassapitosopimuksia ja -sitoumuksia, tila- ja käytönvalvontaa, pääsynhallinta, päivitysten ja muutosten hallintaa, fyysistä turvallisuutta, henkilöstöturvallisuutta, toimittajien ja sopimusten hallintaa, tietoturvallisuuden hallintaa, tietojen salausta, tietojen anonymisointia ja pseudonymisointia, tietojärjestelmien ja rekistereiden auditoimintoja, etäkäyttöyhteyksiä, teknisiä rajoituksia, tarkastus- ja valvontajärjestelmiä, käytännössäntöjen sekä sertifikaattien käyttöä. Tässä kappaleessa annetaan kuva siitä, miten tiedon eheys, saatavuus ja luottamuksellisuus taataan sekä myös tiedon läpinäkyvyys (5 art.).

Tiedonhallintalaki edellyttää, että tiedonhallintayksikön tulee ylläpitää sen toimintaympäristön tiedonhallintaa määrittelevää ja kuvaavaa tiedonhallintamallia, joka sisältää tiedot mm. toimintaprosesseista, tietovarannoista, tietoaaineistoista, arkistoinnista, tietojärjestelmistä ja tietoturvallisuustoimenpiteistä. Tämä tapahtuu esimerkiksi kokonaisarkkitehtuurin, tietojärjestelmäarkkitehtuurin, tietovarantokuvausten, asiakirjajulkisuuskuvausten, tiedonohjaussuunnitelmien ja erilaisten prosessikuvausten avulla. Tiedonhallintamallia ylläpidetään palvelujen, asiankäsittelyn ja tietoaaineistojen hallinnan suunnittelemiseksi ja toteuttamiseksi, tiedonsaantia koskevien oikeuksien ja rajoitusten toteuttamiseksi, moninkertaisen tietojen keruun vähentämiseksi, tietojärjestelmien ja tietovarantojen yhteen toimivuuden toteuttamiseksi sekä tietoturvallisuuden ylläpitämiseksi.

Tarkoituksena on selvittää sitä, miten tietoa hallintaa sen koko elinkaaren ajan, tiedon vireille tulosta hävittämiseen tai arkistointiin saakka. Lisäksi kuvaukset toimivat ja toteuttavat julkisuusperiaatetta sekä toimivat omien tietojen pyyntöön liittyvinä apuvälineinä. Tiedonohjaussuunnitelmilla voidaan todentaa esimerkiksi sitä, että tietojen säilytysajat on määritelty asianmukaisesti ja että niiden hävittäminen on suunnitelmallista. Tietovarantoja ja tietojenkäsittelyä saatetaan hoitaa myös organisaation ulkopuolella, esim. palkanlaskenta. Organisaatiolla on olemassa ohjeistus ja sopimukset näihin ulkoisiin tietojenkäsittelytilanteisiin. Organisaatio voi myös käsitellä tietoja käyttäen omia palvelinsalejaan tai ulkoisista pilvipalveluista.

Organisaatio voi johtaa tiedolla ja hyödyntää omaa tietopääomaansa vain, jos johdolla on tarpeeksi tietoa muun muassa omasta toiminnasta, toimintaympäristöstään, prosessien toimivuudesta, henkilökunnan osaamisesta, tietovirroista ja tietovarannoista. Tässä luvussa kuvataan muun muassa sitä, miten organisaatio toteuttaa tietosuojaperiaatteina tietojen minimointia, käytötarkoitussidonnaisuutta ja säilytyksen rajoittamista ja tiedon läpinäkyvyyttä.

TIEDONHALLINNAN ORGANISOINTI

Padasjoen kunnassa työskentelee noin 100 henkilöä, joista suurin osa käsittelee henkilötietoja vähintäänkin jossain määrin. Henkilötietojen käsittely kunnassa perustuu pääasiassa EU:n yleiseen tietosuoja-asetukseen (GDPR) ja Suomen tietosuojalakiin. Kunnalla on oikeus käsitellä henkilötietoja silloin, kun se on välttämätöntä lakisääteisten velvoitteiden täyttämiseksi tai julkisen vallan käyttöön ja yleistä etua koskevien tehtävien hoitamiseen. Lisäksi käsittely voi perustua sopimukseen tai rekisteröidyn antamaan suostumukseen vapaaehtoisissa palveluissa. Poikkeustilanteissa henkilötietoja voidaan käsitellä elintärkeiden etujen suojaamiseksi.

Kunnassa on keskitetty tietohallinto, jonka tehtävänä on johtaa kunnan tietohallintoa sekä IT-palveluita. Tietohallintoon sekä IT-palveluihin käytettävien resurssien, hankkeiden, määrärahojen sekä sopimusten ohjauksesta vastaa tietohallintopäällikkö. Tietohallintopalveluiden vastuualueella

on kokonaisarkkitehtuurin tietojärjestelmien ja tietoturvallisuuden ohjaus. Tietohallintapalvelut sijoittuu organisaatiossa hallinnon alaisuuteen. Asiakirjahallintoa johtava viranhaltija johtaa kunnanhallituksen alaisena asiakirjahallintoa ja vastaa kunnan pysyvästi säilytettävistä asiakirjatiedoista.

TIETOTURVAN JA TIETOSUOJAN ORGANISOINTI

KUNNANHALLITUS

Kunnanhallitus on tiedonhallintalain tarkoittama tiedonhallintayksikön johto kunnassa. Kunnanhallitus seuraa tietoturvallisuuden sekä tietosuojan toteutumista kunnassa, hyväksyy tietoturva- ja tietosuojapolitiikan sekä vastaa siitä, että tiedonhallintalain vastuut, käytännöt ja valvonta on määriteltä.

KUNNANJOHTAJA

Kunnanjohtaja vastaa omalta osaltaan tietoturvan ja tietosuojan järjestämisen toimintaedellytysten luomisesta. Kunnanjohtaja vastaa myös varautumisesta ja jatkuvuudenhallinnasta yhdessä muun kunnan johtoryhmän kanssa sekä johtaa poikkeusolojen viestintää.

TOIMIALAJOHTAJA

Toimialajohtaja vastaa oman toimialansa tietoturvallisuuden ja tietosuojan toteutumisesta. Toimialajohtajan tehtäviin kuuluu lisäksi varmistaa tietoturvaan ja tietosuojaan liittyvän lainsäädännön, linjausten, periaatteiden ja ohjeistusten noudattaminen toimialallaan.

TIETOHALLINTOPÄÄLLIKÖ

Johtaa tietohallinnon tulosaluetta sekä asianhallinta- ja tietoturvaryhmän toimintaa. Hän vastaa tietoturvallisuuden arjen toimivuudesta sekä tietoturva- ja tietosuojapolitiikan ja organisaatiotasoisesta dokumentaation valmistelusta ja kehittämisestä. Lisäksi hän johtaa ja valvoo kunnan IT-arkkitehtuuria sekä vastaa tiedonhallintamallin ylläpidosta.

ASIAKIRJAHALLINNOSTA JA ARKISTOINNISTA JOHTAVA VIRANHALTIJA

Asiakirjahallintoa johtava viranhaltija johtaa kunnanhallituksen alaisena asiakirjahallintoa ja vastaa kunnan pysyvästi säilytettävistä asiakirjatiedoista sekä lisäksi:

1. Vastaa kunnanhallituksen asiakirjahallinnon viranomaistehtävien valmistelusta ja täytäntöönpanosta.
2. Ohjaa ja kehittää asiakirjahallintoa osana kunnan tiedonhallintaa.
3. Hyväksyy tiedonkäsittelyn, säilytyksen ja arkistoinnin ohjeistuksen.
4. Vastaa keskusarkistosta ja pysyvästi säilytettävistä asiakirjatiedoista.
5. Laatii kunnan asiakirjahallinnon ohjeen ja valvoo, että tehtävät hoidetaan annettujen ohjeiden mukaisesti.
6. Huolehtii asiakirjahallintoon liittyvästä koulutuksesta ja neuvonnasta.

ASIANHALLINTA- JA TIETOTURVARYHMÄ

Asianhallinta- ja tietoturvaryhmä vastaa kunnan tiedonhallinnan ja tietoturvan kokonaisuudesta. Ryhmän tehtäviin kuuluu tietoturvallisuuden suunnittelu, ohjaus, seuranta ja kehittäminen. Se määrittelee teknisen tietoturvallisuuden minimivaatimukset ja huolehtii niiden toteutuksesta, ohjauksesta ja valvonnasta kunnan tietojärjestelmäympäristössä. Lisäksi ryhmä varmistaa tietoturvalisuuden teknisen valvonnan toteutumisen lain sallimin ja yhteistoimintamenettelyn valtuuttamin

menetelmin. Tietoturvariskien ja -poikkeamien hallinta sekä niiden koordinointi kuuluvat ryhmän vastuulle, samoin kuin tietoturvallisuuden tilan raportointi kunnan johdolle.

Asianhallintaryhmä ohjaa ja neuvoo yksiköitä arkistonmuodostuksessa sekä laatii tiedonhallinnan ohjeet ja valvoo, että tehtävät hoidetaan annettujen ohjeiden mukaisesti. Ryhmä huolehtii myös asiakirjahallintaan liittyvästä koulutuksesta ja neuvonnasta. Lisäksi sen vastuulla on kunnanarkistoon siirrettyjen asiakirjojen säilyttäminen ja niistä tietojen antaminen.

TIETOSUOJAVASTAAVA

Tietosuojavastaava sekä tietosuojavastaavan varahenkilö toimii kunnan tukena ja antaa neuvoa sekä ohjausta tietosuojan toteuttamisesta. Tietosuojavastaavan tehtävänä on auttaa kunnan johtoa toteuttamaan veloitteensa rekisterinpitäjänä. Hän tukee rekisterinpitäjää hyvän henkilötietojen käsittelytavan saavuttamisessa sekä varmistaa, että mahdollisten erityislakien edellyttämä tietosuojan taso toteutuu. Tietosuojavastaava seuraa tietosuojasääntöjen noudattamista koko organisaatiossa ja tuo esiin havaitsemansa puutteet. Lisäksi tietosuojavastaava toimii rekisteröityjen yhteyshenkilönä kaikissa henkilötietojen käsittelyyn liittyvissä asioissa. Hän on myös yhteyshenkilö valtakunnalliseen tietosuojavaikuttamiseen ja tekee tarvittaessa ilmoitukset tietosuojaloukkauksista.

HENKILÖSTÖ JA LUOTTAMUSHENKILÖT

Henkilöstö ja luottamushenkilöt vastaavat omalta osaltaan tietoturva- ja tietosuojaohjeiden noudattamisesta. Jokaisen kunnan organisaatioon kuuluvan vastuulla on lisäksi tietoturvallisuuteen ja tietosuojaan liittyvien poikkeamien, uhkien ja riskien ilmoittaminen välittömästi kunnan tietoturva- ja tietosuojoinen mukaisesti. Jokaisella on vastuu työtehtävänsä liittyvän tietosuojan toteuttamisesta sekä tiedon ja tietojärjestelmien asianmukaisesta käytöstä. Esihenkilöasemassa toimivat vastaavat myös omien alaistensa perehdyttämisestä työtehtäviin liittyviin tietoturva- ja tietosuojavaikuttamiseen.

TEKNISET JA ORGANISATORISET TOIMENPITEET

Tietoturvaan ja tietosuojaan liittyviä riskejä pienennetään mm. seuraavilla hallintakeinoilla:

Henkilöstön käytössä on:

- Sähköinen tietoturvallisuuden ja tietosuojan oppimisympäristö
- Henkilöstön tietoturva- ja tietosuojaopas
- Kirjallinen tietoturva- ja tietosuojoinen
- Salattu sähköpostipalvelu
- Sähköinen palvelu tietoturvapoikkeamien ilmoittamiseen
- Intranet erilaisille käytännön ohjeille
- Kaksi- tai monivaiheisen tunnistautuminen käytössä kaikilla työntekijöillä sekä luottamushenkilöillä
- Päätelaitesuojaus kaikilla laitteilla

Muita hallintakeinoja:

- Hallinnon henkilökunnan työasemilta saatavilla turvallinen ja salattu VPN-etäyhteyshallinta kunnan verkkoon
- Kannettavien työasemien kiintolevyillä BitLocker
- Tietokoneissa, puhelimissa sekä tableteissa on käytössä Intune laitehallinta (mm. puhelin voidaan poistaa etänä, sovellusten jakelu keskitetysti etänä)
- Tietoturvallisuuden ja tietosuojan osalta palvelusopimuksiin pyritään luomaan kunnalle omat vakioidut malliliitteet

- Vuosittain päivitettävä tiedonhallintamalli, joka koostaa selosteen käsittelytoimista

RISKIENHALLINTA

Riskienhallinta on osa sisäistä valvontaa. Se on dynaaminen prosessi, jossa tunnistetaan tavoitteiden saavuttamiseen vaikuttavia riskejä ja arvioidaan riskien merkittävyyttä suhteessa määritettyyn riskiensietokykyyn. Riskienhallinnassa huomioidaan niin ulkoisen kuin sisäisen toimintaympäristön muutosten vaikutuksia kunnan toimintaan. Hyvällä riskienhallinnalla pyritään riskien tunnistamiseen ennalta, riskien luokitteluun ja vaikutusten arviointiin ja riskienhallintatoimenpiteiden toteuttamiseen. Tavoitteena on riskien toteutumisen ennaltaehkäisemiseen tai niiden vaikutusten minimoiminen. Riskienhallintaa ohjaavia asiakirjoja ovat hallintosääntö sekä konserniohje.

Viimeaikainen Euroopan geopoliittisen tilanteen muuttuminen on muodostanut enenevässä määrin epävarmuus ja riskitekijöitä myös tietohallinnolle. Tietohallinnon tulee näiltä osin edelleen tarkentaa varautumistaan erilaisiin tilanteisiin ja skenaarioihin liittyen. Varautumissuunnittelu vaatii ICT-palveluihin liittyvien uhka-arvioiden tuntemusta eli sitä, millaisiin häiriötilanteisiin kunnassa varaudutaan. Häiriötilanne on uhka tai tapahtuma, joka voi koskettaa sekä kunnan työntekijöitä että kuntalaisille tarjottavia palveluita. Ongelmia syntyy tai erilaisia skenaarioita voi pahentaa, mikäli esimerkiksi puhelin- sähkö- tai tietoliikenneverkkoihin kohdentuu häiriöitä.

Padasjoen kunta huolehtii korruption ja lahjonnan torjunnasta sekä ihmisoikeusasioista lainsäädännön ja hyvän hallinnon periaatteiden noudattamisen, ajantasaisen ohjeistuksen ja selkeiden toimivallan jakojen kautta. Padasjoen kunnanvaltuuston hyväksymä hallintosääntö määrittää toimielinten, luottamushenkilöiden ja viranhaltijoiden toimivallan jaot toiminnan lainmukaisuuden varmistamiseksi. Kunnanhallitus on hyväksynyt sisäisen valvonnan ja riskienhallinnan ohjeen 1.3.2021, jossa määritellään sisäisen valvonnan ja riskienhallinnan yleiset periaatteet ja toteuttamistavat. Ohjeella turvataan toiminnan lainmukaisuutta ja hyvän hallintotavan mukaan toimimista.

Kunnalla on käytössä EU:n ilmoittajansuojelulakiin perustuva eettinen väärinkäytösten ilmoituskanava. Väärinkäytösilmoitukset käsittelevät kunnanhallituksen nimeämä työpari, joka ryhtyy välittömästi ilmoituksen vastaanottamisen jälkeen tarvittaviin jatkotoimiin. Lisäksi tarkastuslautakunta ylläpitää Kuntalain mukaista sidonnaisuusrekisteriä. Ajantasainen rekisteri löytyy kunnan verkkosivuilta.

Tietosuojaan riskienhallinta on osa organisaation toimintaa. Tietosuojauhkien hallinta ei pysy uusien koko ajan lisääntyvien uhkien tasolla, jos sitä ei sisällytetä oletusarvoisesti osaksi riskienhallintaprosessia. Tietoturvan riskienhallinta liittyy oleellisesti tietosuojaan riskienhallintaan, joten riskienhallinta on oltava kunnossa, jos halutaan saavuttaa hyvä tietosuojataso organisaatiossa. Tietosuoja-asetuksen velvoitteet ja asianmukaiset suojatoimet on suhteutettava henkilötietojen käsittelystä rekisteröidyn oikeuksille ja vapauksille aiheutuvaan riskiin. Rekisterinpitäjän on tehtävä perusteellinen arvio henkilötietojen käsittelyyn liittyvistä riskeistä, jotta rekisterinpitäjä voi toteuttaa asetuksen sisäänrakennettua ja oletusarvoista tietosuojaa ja muita asetuksessa säädettyjä velvollisuuksia.

Tietosuojaan vaikutustenarviointi auttaa noudattamaan asetuksen vaatimuksia ja edesauttaa osoitusvelvollisuuden toteutumista. Vaikutustenarviointi on tehtävä, jos käsittely todennäköisesti aiheuttaa korkean riskin henkilötietojen suojalle. Padasjoen kunnalla on oma ohjeistus vaikutustenarvioinnin tekemiseen. Ohjeet pohjautuvat vahvasti tietosuojavaltuutetun toimiston tuottamiin ohjeisiin.

Tietohallinnon riskienhallintasuunnitelmassa on arvioitu keskeisimmät riskit, niiden toteutumisen todennäköisyys, vaikutukset, vakavuus ja toimenpiteet riskien pienentämiseksi.

Sisäinen valvonta ja riskienhallinta päivittäisessä toiminnassa toteutuu:

- esihenkilöiden ja henkilöstön suorittamana riskien tunnistamisena ja arviointina
- riskien hallintatoimenpiteiden toteuttamisena ja valvontana
- valtuuksien, päätösten ja ohjeiden noudattamisena
- prosessien ja tietojärjestelmien kontrolleina

TARKASTUKSET

Tietosuojan osalta on tehty sisäisiä tarkastuksia ja niihin on sisältynyt muun muassa tietosuojaselosteiden tarkastaminen sekä päätöksissä olevien henkilötietojen poistaminen verkkosivujen julkaisuista. Ulkoista auditointia tietosuojan tai tietoturvan osalta ei tehty vuonna 2025. Tarkastuslautakunta ei myöskään tuonut esille puutteita tietoturvan tai tietosuojan osalta kyseiseltä vuodelta.

TIETOTURVAPOIKKEAMIENTÄN KÄSITTELY

Tietoturvapoikkeamien käsittelyyn ja hallintaan on luotu prosessi, joka on kuvattuna Tietoturva- ja tietosuojapolitiikan liitteissä. Ilmoituksia voi tulla palvelupyynnötyjärjestelmään, puhelimitse tai tavalisella sähköpostilla. Ilmoitukset käsitellään ja ryhdytään tarvittaviin toimenpiteisiin niiden edellyttämällä tavalla.

Käsittely tehdään aina tapauskohtaisesti ja käsittelyyn osallistuu tarvittava määrä henkilöitä, kuten tietosuojavastaava ja esihenkilö. Vuonna 2025 tällaisia poikkeamia ei havaittu.

TIETOVARANNOT JA TIETOVIRRAT

Tiedonhallintalaki edellyttää, että tiedonhallintayksikön tulee ylläpitää sen toimintaympäristön tiedonhallintaa määrittelevää ja kuvaavaa tiedonhallintamallia, joka sisältää tiedot mm. toimintaprosesseista, tietovarannoista, tietoa-aineistoista, arkistoinnista, tietojärjestelmistä ja tietoturvasuojatoimenpiteistä. Tämä tapahtuu esimerkiksi kokonaisarkkitehtuurin, tietojärjestelmäarkkitehtuurin, tietovarantokuvausten, asiakirjajulkaisuuskuvauksen, tiedonohjaussuunnitelmien ja erilaisten prosessikuvausten avulla. Tiedonhallintamallia ylläpidetään palvelujen, asiankäsittelyn ja tietoa-aineistojen hallinnan suunnittelemiseksi ja toteuttamiseksi, tiedonsaantia koskevien oikeuksien ja rajoitusten toteuttamiseksi, moninkertaisen tietojen keruun vähentämiseksi, tietojärjestelmien ja tietovarantojen yhteen toimivuuden toteuttamiseksi sekä tietoturvasuojallisuuden ylläpitämiseksi.

Tarkoituksena on selvittää sitä, miten tietoa hallintaa sen koko elinkaaren ajan, tiedon vireille tulosta hävittämiseen tai arkistointiin saakka. Lisäksi kuvaukset toimivat ja toteuttavat julkisuusperiaatetta sekä toimivat omien tietojen pyyntöön liittyvinä apuvälineinä. Tiedonohjaussuunnitelmilla voidaan todentaa esimerkiksi sitä, että tietojen säilytysajat on määritelty asianmukaisesti ja että niiden hävittäminen on suunnitelmallista. Tietovarantoja ja tietojenkäsittelyä saatetaan hoitaa myös organisaation ulkopuolella, esim. palkanlaskenta. Organisaatiolla on olemassa ohjeistus ja sopimukset näihin ulkoisiin tietojenkäsittelytilanteisiin. Organisaatio voi myös käsitellä tietoja käyttäen omia palvelinsalejaan tai ulkoisista pilvipalveluista.

Organisaatio voi johtaa tiedolla ja hyödyntää omaa tietopääomaansa vain, jos johdolla on tarpeeksi tietoa muun muassa omasta toiminnasta, toimintaympäristöstään, prosessien toimivuudesta, henkilökunnan osaamisesta, tietovirroista ja tietovarannoista. Tässä luvussa kuvataan muun muassa sitä, miten organisaatio toteuttaa tietosuojaperiaatteina tietojen minimointia, käytötarkoitussidonnaisuutta ja säilytyksen rajoittamista ja tiedon läpinäkyvyyttä.

TIEDON ELINKAAREN HALLINTA

Asianhallintajärjestelmässä olevien tietojen elinkaarta ohjaa tiedonohjaussuunnitelma, johon on määritelty asioiden, käsittelyvaiheiden ja asiakirjojen elinkaarta ohjaavia metatietoja, kuten säilytysaikatiedot ja säilytysajan perusteet. Tiedonohjaussuunnitelman runkona toimii Padasjoen kunnan tehtäväluokitus, johon on määritelty kuntien yhteisen tehtäväluokituksen pohjalta tehtävät. Vuoden 2025 aikana tiedonohjaussuunnitelmaa ei koettu tarpeen päivittää.

Tietojen säilytysajat ja -tavat merkitään kunnan arkistonmuodostussuunnitelmaan. Vuonna 2024 tiedonhallintamallin valmistumisen myötä luotiin uutta arkistonmuodostussuunnitelmaa, mutta tiedot ovat puutteellisia eikä niitä ole tarkistettu. Arkistonmuodostussuunnitelmalla ei voida ohjata tietojärjestelmissä olevien tietojen elinkaarta teknisesti. Elinkaaren vaiheiden hallinta ja tietojen tuhoaminen tietojärjestelmistä on riippuvainen tietojärjestelmien toiminnoista.

Tiedon elinkaari ja tietoaineistojen säilytysaikojen määrittely on ollut puutteellista. Kaikki sähköisesti säilytettävät aineistot asianhallintajärjestelmässä on määritelty pysyvästi säilytettäväksi. Säilytysaikoja tarkastellaan ja päivitetään mahdollisuuksien mukaan uuden asianhallintajärjestelmän käyttöönoton yhteydessä vuoden 2026 aikana.

TIETOVARANNOT

Padasjoen kunnalla on tällä hetkellä 35 tunnistettua tietovarantoa. Tiedonhallintamallin päivityksen yhteydessä on tavoite tunnistaa tietovarantojen päällekkäisyyksiä, mutta vuoden 2025 päivityksen yhteydessä sitä ei ehditty tekemään.

ASIANHALLINTA JA SÄHKÖINEN ASIOINTI

Asianhallinnan tarkoituksena on hallita ja seurata viranomaisen käsiteltäväksi saapuneita ja otettuja asioita sekä niiden käsittelyvaiheita ja niihin liittyviä asiakirjoja. Käytössä olevasta asianhallintajärjestelmästä on tulossa uusi versio 2.0, mihin Padasjoen kunta ilmoittautui pilottikunnaksi. Asia ei kuitenkaan edennyt vuoden 2025 aikana.

Asianhallintajärjestelmäkokonaisuuteen kuuluvaa sähköisen asiointipalvelun käyttöä suunniteltiin otettavaksi käyttöön, mutta käyttöönotto siirtyi vuoden 2026 alkupuoliskolle.

ASIAKIRJAHALLINTO JA ARKISTOTOIMI

Kunnan arkistosta on siirretty sosiaali- ja terveydenhuollon tietoaaineistoja Päijät-Hämeen hyvinvointialueelle yhteistyössä hyvinvointialueen kanssa. Tietoaaineistojen siirrosta tehtiin luovutus sopimus Päijät-Hämeen hyvinvointialueen arkistopalveluiden kanssa. Tietoaaineistojen siirrosta siirrettiin Padasjoen terveysaseman päätearkistosta työterveyshuollon potilasasiakirjoja ajalta 1971–2010.

Arkiston osalta vuoden 2025 aikana tehtiin jonkin verran aineistojen hävittämistä sekä uudelleenjärjestelyitä arkistotilan tehostamiseksi. Tämä työ jatkuu vielä vuoden 2026 puolelle. Sähköisesti Lupapisteen kautta haettavat lupapyynnöt arkistoituvat Lupapisteen Onkaloon. Kunnan rakenusvalvonnan paperiarkistosta Onkaloon viedään materiaalia sitä mukaan, kun niitä tarvitsi asiakkailla digitoida.

KOULUTUS JA KEHITTÄMINEN

KOULUTUS

Padasjoen kunnalla on käytössä sähköinen tietoturvan ja tietosuojan oppimisympäristö, jossa jokaisen kunnan viranhaltijan, työntekijän sekä luottamushenkilön tulee suorittaa koulutus vuosittain. Tietoturvaan ja tietosuojaan liittyvää koulutusta uudistettiin vuonna 2025 ja palveluun saatiin erilaisia rooli- ja toimialakohtaisia koulutuksia.

OHJEISTUS

Kunnan intranetissä on julkaistu kunnan laatimia ohjeita sekä muut tärkeimmät asiat, mitkä tulee ottaa huomioon ennen palvelussuhteen alkua, loppua, palvelussuhteen aikana tai muussa muutostilanteessa. Näitä ovat esimerkiksi työajanseurantaan liittyvät asiat, tietoturva- ja tietosuojakoulutus, laitteiden ja sovellusten käyttöohjeita sekä muita työntekoon liittyviä ohjeistuksia. Näitä päivitetään sekä laaditaan uusia aina tarpeen mukaan.

Intranetissä on erillinen paikka tietohallinnon asioille ja ohjeille, mistä löytää esimerkiksi ajantasaisen tietoturva- ja tietosuojapolitiikan sekä muita tietoturvallisuuteen ja tietosuojaan liittyviä ohjeita. Tänne myös julkaistaan 3–5 kertaa vuodessa uutisena tietosuojavastaavan ajankohtaiskatsaus.

KEHITTÄMINEN

TIEDOLLA JOHTAMINEN

Tiedolla johtamista on pyritty kehittämään osallistumalla Heinolan kaupungin hallinnoimaan ”Päijät-Häme digitiedolla tulevaisuuteen” -hankkeen toteuttamiseen. Tavoitteena on maakunnan kuntien tiedolla johtamisen kehittäminen. Hanke on tarkoitus toteuttaa vuosina 2025–2027 ja sille haetaan EAKR-rahoitusta.

TIETOTURVALLISUUDEN JA TIETOSUOJAN KEHITTÄMINEN

Asianhallinta- ja tietoturvaryhmä nimettiin uudelleen. Ryhmä kokoontuu 3–5 kertaa vuodessa ja puheenjohtajana toimii tietohallintopäällikkö. Ryhmän tarkoituksena on seurata ja kehittää tietoturvallisuutta, määritellä tietoturvallisuuden minimivaatimukset, raportoida tietoturvan tilasta kunnan johdolle, koordinoida asiakirjahallintoon liittyvää koulutusta sekä huolehtia kunnanarkistoon siirretyistä asiakirjoista.

Tietosuojatyöskentelyä on kehitetty tietosuojaparityöskentelyä korostamalla, mikä on parantanut asioiden seuranta ja osaamista. Lisäksi henkilöstö on jatkanut osaamisen kehittämistä vuosittaisen tietosuoja- ja tietoturvakoulutuksen avulla.

Tietosuojan kehittäminen on pyritty tekemään säännölliseksi, rutiininomaiseksi toiminnaksi, mikä vahvistaa tietosuojavastaavan ja hänen varahenkilönsä osaamista ja asian ymmärtämistä. Resurssipula on kuitenkin tiedossa oleva riski laajemman tietosuojaosaamisen ylläpidolle ja ajantasaisuudelle.

REKISTERÖIDYN OIKEUKSIEN TOTEUTUMINEN

Jokaisella on oikeus henkilötietojensa suojaan. Tietosuoja on perusoikeus, jonka tarkoituksena on turvata rekisteröidyn oikeuksien ja vapauksien toteutuminen henkilötietojen käsittelyssä. Tietosuojan tarkoituksena on osoittaa milloin ja millä edellytyksillä henkilötietoja voidaan käsitellä. Rekisterinpitäjän velvollisuus on huolehtia rekisteröidyn oikeuksien toteutumisesta. Näitä ovat muun muassa rekisteröidyn oikeus saada tietoa henkilötietojen käsittelystä, oikeus saada pääsy tietoihin

ja oikeus oikaista virheellisiä tietoja. Lisäksi rekisteröidyillä on oikeus tietyillä rajauksilla saada tieto sosiaali- ja terveydenhuollon käyttö ja -luovutustiedoista. Rekisterinpitäjän tulee informoida rekisteröityjä henkilötietojen käytöstä avoimesti ja selkeästi. Rekisterinpitäjän tulee myös varautua mahdollisiin henkilötietojen tietoturvaloukkauksiin ja harjoitella niihin varautumista käytännössä. Henkilötietojen tietoturvaloukkauksia ovat mm., että tiedot lähetetty väärälle vastaanottajalle, suojaamaton tiedonsiirtoväline on hävinnyt esim. USB-tikku, haittaohjelmatartunta, kyberhyökkäys ja hakkerointi. Rekisterinpitäjän tulee tilastoida henkilötietojen tietoturvaloukkaukset ja ilmoittaa niistä tietosuojavaltuutetun toimistolle ja tietyn edellytyksin myös rekisteröidyille. Henkilötietojen käsittelijöillä on velvollisuus puolestaan ilmoittaa henkilötietojen tietoturvaloukkauksista rekisterinpitäjälle. Tässä luvussa kuvataan tietosuojaperiaatteina erityisesti läpinäkyvyyttä ja kohtuullisuutta.

Kuntalaisten informointiin tarkoitetut julkiset tietosuojaselosteet ovat olleet päivityksessä eikä niitä olla saatu vietyä kunnan verkkosivuille. Kunnalla on käytössä yleisen tietosuoja-asetuksen vaatimukset täyttävä tietosuojaselostepohja, jonka sisällöstä vastaa rekisterinpitäjä tai hänen nimeämänsä vastuuhenkilö.

SEURANTA JA MITTARIT

Organisaatiolla on veloitteita kuvata erilaisilla mittareilla toimintaansa. Osa mittaristosta palvelee organisaation omaa tarvetta ja osa mittareita ovat sellaisia, joita joudutaan raportoimaan muualla. Ilman mittareita on vaikea tietää, miten organisaatio on kehittynyt ja mitä osa-alueita tulee vielä kehittää. Alla on kuvattu yleisimpiä tiedonhallintaan, tietosuojaan, tietoturvaan ja riskienhallintaan liittyviä mittareita. Organisaatio valitsee omien tarpeidensa mukaan käytettävät mittarit ja voi myös seurata muita asioita, mitkä koetaan tarpeelliseksi ja omaa toimintaa kuvaavaksi. Tarvittaessa mittareiden toteumat voi jaotella organisaation toiminnan kannalta tarkoituksenmukaisesti, kuten esim. kunnassa toimialakohtaisesti (omiin sarakkeisiin sote/ muut toimialat). Mittarit on ryhmitelty kuuteen eri osioon. Näitä ovat tietohallinto, riskien arviointi ja tarkastukset, tietovarannot, asianhallinta, osaaminen ja ohjeistus sekä rekisteröidyn oikeudet.

Tunnusluku	Toteuma 2025
Käyttäjien (AD-tunnuksia), sis. oppilaat	456 kpl
IT-tukipyynnöt	162 kpl
Mobiililaitteita	162 kpl
Tietokoneita	273 kpl
Tietohallinnon henkilöstö	1 htv
Tietosuoja-tietoturva hlöstö	0,5 htv
Tehdyt vaikutustenarvioinnit	2 kpl
Tehdyt auditoinnit, sisäiset	1 kpl
Tietovarannot	35 kpl
Tiedonhallintamallin valmiusaste	100 %
Tietojärjestelmät	57 kpl
Henkilöstön tietoturvakoulutukset, suoritus %	50 %
Luottamushenkilöiden tietoturvakoulutukset, suoritus %	35 %
Aineistojen digitointi, valmiusaste (arvio)	10 %
Tietosuojaselosteet ja muu informointi valmiusaste (arvio)	70 %
Henkilötietojen tietoturvaloukkaukset	0 kpl
Henkilötietojen tietoturvaloukkaukset ilmoitukset/ TSV	0 kpl
Henkilötietojen tietoturvaloukkaukset ilmoitukset/ rekisteröidyille	0 kpl
Esille tulleet tietosuojarikkomukset	2 kpl
Epäillyt tietosuojarikkomukset	2 kpl
Palveluestohyökkäykset	0 kpl
Virushavainnot	0 kpl