



Tietotilinpäätös 2024

Suomussalmen kunta



Sisällys

1. Tietosuojavastaavan katsaus	1
2. Tietotilinpäätöksen tarkoitus.....	2
3. Tietosuojavuosi 2024 pähkinäkuoressa	3
4. Tietosuoja-asioiden vastuunjako Suomussalmen kunnassa	4
4.1 Erilaiset toimijat ja niiden vastuu	4
4.2 Suomussalmen tietoturvaryhmä ja Kainuun tietoturvan ja tiedonhallinnan ohjausryhmä .	5
5. Rekisteröidyn oikeuksien toteuttaminen.....	6
5.1. Rekisteröidyn informointi	6
5.2. Tietosuojaselosteet.....	6
5.3. Rekisteröidyn oikeuksiin liittyvät pyynnöt	6
5.3.1. Tarkastuspyynnöt	7
5.3.2. Oikaisupyynnöt	7
5.3.3. Poistopyynnöt	7
5.3.4. Rajoittamisoikeus.....	8
5.3.5. Vastustamisoikeus	8
5.3.6. Riitauttamisoikeus.....	8
6. Selosteet käsittelytoimista.....	9
7. Tietoturva.....	10
8. Tietosuojaa koskevat vaikutustenarvioinnit.....	10
9. Käsiteltävät henkilötiedot ja niiden elinkaaren hallinta	10
10. Sopimukset ja hankinnat	10
11. Lainsäädäntö, koulutus ja ohjeistus	12
11.1. Henkilötietojen käsittelyä koskeva lainsäädäntö	12
11.2. Henkilötietojen käsittelyä koskeva ohjeistus	12
12. Henkilötietojen tietoturvaloukkaukset.....	13
13. Valvontaviranomaisten selvitys- ja tietopyynnöt.....	13
14. Tietosuojatyön kehittämistarpeet	13

1. Tietosuojavastaavan katsaus

Tällä tietotilinpäätöksellä osoitetaan, miten tietosuoja ja tietoturva ovat toteutuneet Suomussalmen kunnan toiminnassa vuonna 2024.

Tietosuojatyön kehittäminen on luonteeltaan jatkuvaa ja ilmenee nyt muun muassa sisäisten käytäntöjen uudistamisilla.

Tietosuojan ja tietoturvan vastuuhenkilöt sekä tietoturvaryhmä ovat kaikki osaavia ja sitoutuneita työhönsä. Kunnalla on toimivat prosessit rekisteröidyn oikeuksiin liittyviin pyyntöihin ja tietoturvaloukkauksiin. Sopimuksissa ja hankinnoissa, joissa käsitellään henkilötietoja, kunnalla on laadittuna oma tietosuoja- ja salassapitoliite. Henkilöstöä koulutetaan kattavasti tietosuoja- ja turva-asioihin käyttöönotetulla verkkopohjaisella ohjelmalla. Kunnalla on tietosuojan intranet -sivut, joilta löytyy selkeä ohjeistus tietosuojakysymyksiin.

Tietoturvatyöryhmä yhdessä johdon kanssa osallistui TAISTO24 -tietoturva- ja -suojaharjoitukseen, joka tarjoaa turvallisen tilaisuuden harjoitella, testata ja kehittää organisaation digiturvan toimintamalleja kuvitteellisten häiriötilanteiden kautta.

Kunnalla on vuonna 2022 hyväksytty voimassa oleva tietoturva ja tietosuojapolitiikka, jonka ajantasaistaminen aloitettiin vuonna 2024.

Tietosuojatyö on kunnan asukkaita varten. Heillä on oikeus luottaa siihen, että kunnassa käsitellään heidän henkilötietojaan lainsäädännön edellyttämällä tavoin. Näin ollen on tärkeää, että Suomussalmen kunta panostaa jatkossakin tietosuojatyöhön sekä jatkaa hyvää linjaansa tässä työssä kehittäen sitä kaudella ilmenneiden tarpeiden osalta. Tietosuojaan ja tiedonhallintaan liittyy monia lakisääteisiä velvoitteita, joiden hoitamisessa kunnassa ollaan menty resursseihin nähden erinomaisesti eteenpäin.

2. Tietotilinpäätöksen tarkoitus

Tietotilinpäätös on keskeinen osa tietosuojan toteutumisen seuranta ja EU:n yleisen tietosuoja-asetuksen (EU 2016/679) määrittelemää osoitusvelvollisuutta (art. 5).

Osoitusvelvollisuus tarkoittaa sitä, että organisaation pitää pystyä osoittamaan noudattavansa tietosuoja-asetusta henkilötietojen käsittelyssä sekä toteuttavansa tietosuojaperiaatteita myös käytännössä.

Osoitusvelvollisuuden toteuttaminen edellyttää, että henkilötietojen käsittelyyn liittyvät prosessit ja tietosuojaperiaatteiden käytännön toteuttaminen dokumentoidaan. Tietotilinpäätös on osa tätä dokumentointia, ja se koostaa yhteen, mitä Suomussalmen kunnalla on käytännössä tehty tietosuojan toteuttamiseksi.

Osoitusvelvollisuuden toteuttamisen lisäksi tietotilinpäätös kuvaa tietojen käsittelyn nykytilaa, arvioi tietosuojan ja tietoturvan toteutumista, tarkastelee tietosuojan valvontaa ja esittelee kehityskohteita.

Tietotilinpäätös on kunnan johdolle tarkoitettu tietosuojan seurannan ja kehittämisen työkalu ja sitä voidaan käyttää sisäisen ja ulkoisen valvonnan apuvälineenä.

Tietotilinpäätös on suunnattu laajalle kohdeyleisölle kunnan johdosta esimiehiin, asiantuntijoihin, työntekijöihin ja kunnan asukkaisiin. Tietotilinpäätöstä laadittaessa on otettu huomioon tietosuojavaltuutetun toimiston ohjeistus tietotilinpäätöksen laatimisesta.

3. Tietosuojavuosi 2024 pähkinäkuoressa

- Jälleen kerran Tietoturvaryhmä ja viestintäsuunnittelija osallistuivat Taisto-harjoitukseen, joka on Suomen suurin digitaalisen turvallisuuden harjoitus.
- Kaikki tietosuojaselosteet päivitettiin vuonna 2024
- Tiedonhallintamallin ohjelmaan (ARC) järjestettiin koulutusta toimialoille siten, että tiedonhallintamallin seuranta ja tietosuojaselosteiden tarkastelu onnistuu ohjelmassa.
- Henkilöstön tietosuoja- ja tietoturvaohje päivitettiin
- Käyttöön otettiin Nimblr-ohjelma, joka simuloi huijausviestejä ja tarjoaa ajankohtaisia lyhyitä tietosuojakoulutuksia, jotka kaikilla on suoritettava.
- Lakisääteinen tietosuojan vaikutustenarviointi otettiin käyttöön ja vietiin käytäntöön: koulutukset toimialoille ja lomakkeiden laatiminen. Vaikutusten arviointeja on tehty tällä hetkellä 22 ja ne ovat parhaillaan viimeisteltävänä arkistointia ja hyväksyntää varten.
- 1 Tietoturvaryhmän kokous
- 4 Kainuun tietosuojan- ja tietoturvan ohjausryhmän kokousta, joissa kaikissa oli edustaja Suomussalmelta.
- Tietosuojaloukkausilmoituksia oli 9. Raportoiduista tietosuojaloukkausilmoituksista ei tietosuojaloukkauksen arvioinnin perusteella yksikään johtanut jatkotoimenpiteisiin eli tapaukset olivat rajattuja ja niiden vaikutus oli vähäinen (esimerkiksi väärälle henkilölle mennyt sähköposti, väärä tuloste tulostimesta tai ohjelmistotoimittajan laajempi virhe, joka ei koskenut Suomussalmen kuntaa, mutta tuli kuntaan tiedoksi).
- Ei yhtään henkilötietojen tarkastuspyyntöä

4. Tietosuoja-asioiden vastuunjako Suomussalmen kunnassa

4.1 Erilaiset toimijat ja niiden vastuu

Tietosuoja-asioiden vastuunjako on määritelty kunnan tietosuoja- ja tietoturvapoliitikassa.

Tietoturvallisuuteen liittyvät roolit vastuineen on organisoitu kunnan sääntöjen mukaisesti.

Kunnanhallitus seuraa tietoturvallisuuden toteutumista kunnassa. Kunnanhallitus hyväksyy tietoturvapoliitikan ja siihen ehdotetut muutokset. Kunnanhallituksella on vastuu kunnan sisäisen valvonnan ja riskienhallinnan järjestämisestä.

Kunnanjohtajalla on kokonaisvastuu tietoturvallisuuden toteuttamisesta ja tietoturvallisuuden toteutumisen raportoinnista kunnanhallitukselle. Kunnanjohtaja omistaa tietoturvapoliitikan ja esittelee muutokset kunnanhallitukselle. Kunnanjohtaja hyväksyy kuntatasoiset ohjeet ja linjaukset.

Kunnanjohtajan tukena tietoturvallisuusasioissa on kunnan **tietoturva- ja tietosuojayöryhmä**, jota koordinoi **hallintojohtaja**, joka yhdessä tietosuojavastaavan kanssa vastaa ohjeistusten ja asiakirjojen laatimisesta. Ryhmään kuuluu kunnanjohtajan ja hallintojohtajan lisäksi tietosuojavastaava ja mahdollisuuksien mukaan myös ICT-palvelutarjoaja sekä johtoryhmän muut jäsenet.

Toimialajohtajat vastaavat toimialansa riskienhallinnasta ja varautumisesta sekä tietoturvallisuuden ja tietosuojan toteutumisesta. **Johtoryhmä** varmistaa toimintaan kuuluvien tietojen turvaamisen ja suojaamisen menetelmät, välineet ja toimenpiteet, työhön osoitetut resurssit ja välineistöntietoturvaominaisuudet.

Esimies vastaa tietoturvallisuuden toteutumisesta omalla vastualueellaan. Esimiehen keskeisimpinä tehtävinä on huolehtia:

- oman organisaationsa perehdyttämisestä kunnan tietoturvaohjeisiin sekä jokaisen työntekijän työtehtäviin liittyviin tietoturvavastuisiin.

- työntekijän palvelussuhteen päättyessä tai henkilön siirtyessä toisiin tehtäviin:

o kunnan tiedon ja muun omaisuuden palauttamisesta

o työntekijän käyttöoikeuksien ja -valtuuksien poistamisesta.

Jokainen Suomussalmen kunnan työntekijä ja luottamushenkilö vastaa tietoturvan ja -suojan toteuttamisesta omalta osaltaan. Jokaisen on edesautettava omalla tekemisellään turvallisuuden tavoitteiden toteutumista mm. noudattamalla tietosuojaa ja tietoturvaa koskevia ohjeita. Jokaisen velvollisuus on tuoda esille mahdolliset turvallisuuspoikkeamat, epäkohdat sekä havaitsemansa uhkat ja riskit ja raportoida niistä välittömästi Atean asiakastukeen ja omalle esimiehelleen. Henkilöstö on velvollinen pyytämään apua tietoturvaa ja -suojaa koskevissa kysymyksissä sitä tarvitessaan.

Tietoturvatavoitteet saavutetaan vain, jos kaikki noudattavat yhteisesti sovittuja periaatteita.

Tietosuojavastaava valvoo ja seuraa tietosuojan toteutumista tietosuojan valvontasuunnitelman mukaisesti ja raportoi puutteista ja esittää parannusehdotuksia johtoryhmälle.

Tiedon omistaja vastaa tiedon elinkaaren hallinnasta, tiedon luokittelusta (julkisuuden ja salassapidonmäärittely), eheyden varmistamisesta sekä tallentamisesta luokituksen edellyttämään ympäristöön. Tiedon omistaja on se, joka tiedon tuottaa ja joka vastaa sen oikeellisuudesta.

Tietojärjestelmän omistaja vastaa tietojärjestelmänsä ja sen sisältämän tiedon riskienhallinnasta ja varautumisesta sekä tietoturvallisuuden toteutumisesta. Käyttöoikeudet tietojärjestelmään hyväksyy henkilön esimiehen hakemuksen perusteella tietojärjestelmän omistaja tai hänen valtuuttamansa taho.

Tietojärjestelmän omistaja on tietojärjestelmästä vastaava toimialan tulosalueen tai toimintayksikön esimies.

Prosessin omistaja vastaa prosessinsa riskienhallinnasta ja varautumisesta sekä tietoturvallisuuden toteutumisesta. Lisäksi hän vastaa prosessin riippuvaisuuksien tunnistamisesta ja kriittisyyden arvioinnista.

Palveluntuottajat vastaavat tietoturvallisuuden ja teknisen valvonnan toteutumisesta ICT-ympäristössä ja tietojärjestelmissä lain sallimin ja yhteistoimintamenettelyn valtuuttamin menetelmin. Milloin tietosuojalainsäädäntö edellyttää tietosuojan vaikutusten arvioinnin (dpia) tekemistä, vastaa palveluntuottaja vaikutusten arviointiprosessiin osallistumisesta omalta osaltaan. Palveluntuottajat noudattavat kunnan tietoturvapoliittikkaa sekä sopimusten tietoturva- ja tietosuojaliitteitä.

4.2 Suomussalmen tietoturvaryhmä ja Kainuun tietoturvan ja tiedonhallinnan ohjausryhmä

Suomussalmen kunnassa on tietoturvaryhmä, joka seuraa tietoturvan ja tietosuojan tilaa, linjaa niiden kehittämistä sekä omalta osaltaan jalkauttaa kunnan yhteisiä toimintatapoja toimialoille.

Vuoden 2024 aikana tietoturvaryhmä kokoontui kerran.

Suomussalmen kunta osallistuu Kainuun tietoturvan ja tiedonhallinnan ohjausryhmän kokouksiin. Vuoden 2024 aikana ohjausryhmällä oli neljä kokousta.

5. Rekisteröidyn oikeuksien toteuttaminen

5.1. Rekisteröidyn informointi

Suomussalmen kunta antaa rekisteröidylle tarvittavan informaation kunnan internetsivuilla osoitteessa suomussalmi.fi/kunta-ja-hallinto/tietosuoja. Sivuilla annetaan yleisinformaatiota henkilötietojen käsittelystä Suomussalmen kunnassa sekä kerrotaan rekisteröidyn oikeuksista ja niiden toteuttamisesta.

Lisäksi sivuilla on tietosuojaselosteet, joissa kerrotaan henkilötietojen käsittelystä tietovarantokohtaisesti.

Sivuilla kerrotaan myös Suomussalmen kunnan tietosuojavastaavan yhteystiedot.

5.2. Tietosuojaselosteet

Suomussalmen kunta kerää henkilötietoja eri käyttötarkoituksiin. Kunnan rekisterinpitäjillä on velvollisuus

informoida rekisteröityjä henkilötietojen käsittelystä. Suomussalmen kunnan käsittelemistä henkilötiedoista on laadittu tietosuojaselosteet, jotka muodostavat yhden osuuden tästä informoinnista.

Tietosuojaselosteet on julkaistu kunnan verkkosivuilla osoitteessa <https://suomussalmi.fi/fi/kunta-ja-hallinto/tietosuoja>

Tietosuojaselosteista ilmenee seuraavat tiedot:

- rekisterinpitäjän ja tämän edustajan yhteystiedot
- tieto siitä, mitä henkilötietoja käsitellään
- henkilötietojen käsittelyn tarkoitukset sekä käsittelyn oikeusperuste
- tieto henkilötietojen säännönmukaisista luovutuksista
- henkilötietojen säilytysaika tai jos se ei ole mahdollista, tämän ajan määrittämiskriteerit
- henkilötietojen tietolähteet
- miten rekisteröity voi käyttää henkilötietoihin liittyviä oikeuksiaan
- rekisteröidyn oikeuksiin ja vapauksiin kohdistuvista riskeistä

Tietosuojaselosteita on ajantasaistettu osana kunnan tiedonhallintamallin laatimista. Tietosuojaselosteita päivitetään tarvittaessa ja tiedonhallintamallin vastuuhenkilöt katselmoivat selosteiden tietosisältöä vuosittain osana

5.3. Rekisteröidyn oikeuksiin liittyvät pyynnöt

Rekisteröidyillä on oikeuksia liittyen omiin henkilötietoihinsa ja niiden käsittelyyn. Rekisteröidyillä henkilöllä

on:

- Oikeus saada pääsy tietoihin
- Oikeus tiedon oikaisemiseen
- Oikeus tietojen poistamiseen
- Oikeus käsittelyn rajoittamiseen
- Oikeus siirtää tiedot järjestelmästä toiseen
- Vastustamisoikeus
- Oikeus riitauttaa automaattinen yksittäispäätös
- Oikeus tehdä valitus valvontaviranomaiselle

5.3.1. Tarkastuspyynnöt

Rekisteröidyllä henkilöllä on oikeus pyytää Suomussalmen kunnalta pääsy häntä itseään koskeviin henkilötietoihin. Rekisteröidyllä on oikeus tarkastaa, mitä häntä koskevia henkilötietoja asiakasrekisteriin on tallennettu tai ettei rekisterissä ole häntä koskevia tietoja. Huoltajalla on pääsääntöisesti oikeus tarkastaa myös lastaan koskevat tiedot.

Tarkastuspyyntö tehdään henkilökohtaisesti käynnin yhteydessä tai omakätisellä allekirjoituksella tai vastaavalla tavalla varmennetulla asiakirjalla tai henkilökohtaisesti rekisterinpitäjän luona. Asiakkaan henkilöllisyys varmennetaan ennen tietojen antamista.

Vuoden 2024 aikana Suomussalmen kunnalle ei tullut omien henkilötietojen tarkastuspyyntöjä.

5.3.2. Oikaisupyynnöt

Rekisteröidyllä henkilöllä on oikeus pyytää Suomussalmen kunnalta häntä itseään koskevien epätarkkojen ja virheellisten henkilötietojen oikaisemista ilman aiheetonta viivytystä.

Asiakkaan tulee pyynnössään yksilöidä ja perustella tarkasti, mitä tietoa vaaditaan korjattavaksi ja mikä on asiakkaan mielestä oikea tieto ja millä tavalla korjaus pyydetään tekemään. Asiakkaan henkilöllisyys varmennetaan ennen tietojen oikaisemista.

Vuoden 2024 aikana Suomussalmen kunnalle ei tullut omien tietojen oikaisupyyntöjä.

5.3.3. Poistopyynnöt

Joissakin poikkeustapauksissa, esimerkiksi jos tietojen käsittely on perustunut henkilön suostumukseen ja henkilö peruuttaa suostumuksensa, henkilöllä on oikeus saada tietonsa poistetuiksi eli tulla unohdetuksi.

Oikeutta tietojen poistamiseen ei ole, jos käsittely perustuu kunnan lakisääteisen velvoitteen noudattamiseen, liittyy yleistä etua koskevan tehtävän suorittamiseen tai kunnalle kuuluvan julkisen vallan käyttämiseen.

Vuodelta 2024 ei raportoitu henkilötietojen poistopyyntöjä.

5.3.4. Rajoittamisoikeus

Henkilöllä voi tietyissä tilanteissa olla oikeus pyytää henkilötietojensa käsittelyn rajoittamista siksi aikaa, kunnes hänen tietonsa on asianmukaisesti tarkistettu ja korjattu tai täydennetty.

Vuoden 2024 aikana Suomussalmen kunnalle ei tullut henkilötietojen käsittelyn rajoittamispyyntöjä.

5.3.5. Vastustamisoikeus

Rekisteröidyllä henkilöllä on tietyissä tilanteissa oikeus vastustaa henkilötietojensa käsittelyä eli pyytää, että niitä ei käsiteltäisi ollenkaan.

Henkilötietojen käsittelyn vastustamisvaatimuksia ei tullut kuntaan vuonna 2024.

5.3.6. Riitauttamisoikeus

Rekisteröidyllä on oikeus olla joutumatta sellaisen päätöksen kohteeksi, joka perustuu pelkästään automaattiseen käsittelyyn, kuten profilointiin, ja jolla on häntä koskevia oikeusvaikutuksia tai joka vaikuttaa häneen vastaavalla tavalla merkittävästi.

Kunnalle ei ole tullut yhtäkään yhteydenottoa koskien automaattiseen henkilötietojen käsittelyyn perustuvan päätöksen kohteeksi joutumista.

6. Selosteet käsittelytoimista

Rekisterinpitäjän on ylläpidettävä selosteita käsittelytoimista (tietosuoja-asetuksen 30 artiklan mukaiset selosteet). Selosteet käsittelytoimista ovat yleisiä kuvauksia siitä, miten rekisterinpitäjä käsittelee henkilötietoja. Selosteet käsittelytoimista laaditaan kunnan sisäiseen käyttöön sekä valvontaviranomaista varten. Selosteissa kerrotaan:

- rekisterin tai palvelukokonaisuuden nimi
- rekisterinpitäjä ja yhteystiedot
- tietosuojavastaava ja hänen yhteystietonsa
- henkilötietojen käsittelyn tarkoitukset
- kuvaus rekisteröityjen ryhmistä
- kuvaus henkilötietoryhmistä
- vastaanottajaryhmät
- tietojen säilytysajat
- kuvaus teknisistä ja organisatorisista turvatoimista
- tieto henkilötietojen säännönmukaisista luovutuksista EU/ETA-alueen ulkopuolelle
- viittaus henkilötietojen käsittelijän kanssa solmittuun käsittelyä koskevaan sopimukseen

Seloste käsittelytoimista tuotetaan tiedonhallintamallin tiedoista.

Suomussalmen kunnan selosteet käsittelytoimista ovat ARC-ohjelmassa, johon tiedonhallintamalli on koottu.

7. Tietoturva

Tietoturva liittyy läheisesti tietosuojaan. Rekisterinpitäjän on toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa, että henkilötietojen käsittelyssä noudatetaan tietosuoja-asetusta. Tietoturvatyökalut, kuten käyttöoikeuksien hallinta ja käyttöoikeusrajaukset, järjestelmälokitukset, auditoinnit sekä kyky taata järjestelmien ja palveluiden jatkuva luotettavuus, eheys, käytettävyyden ja vikasietoisuus sekä kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa, ovat teknisiä toimenpiteitä, joilla pyritään varmistamaan tietosuojan toteutuminen.

Suomussalmen kunnassa kunnanjohtajalla on kokonaisvastuu tietoturvallisuuden toteuttamisesta ja tietoturvallisuuden toteutumisen raportoinnista kunnanhallitukselle. Kunnanhallitus seuraa tietoturvan toteutumista ja hyväksyy tietoturvapoliitikan.

8. Tietosuojaa koskevat vaikutustenarvioinnit

Tietosuojaa koskevan vaikutustenarvioinnin tarkoituksena on tunnistaa, arvioida ja hallita henkilötietojen käsittelyyn liittyviä riskejä. Tietosuoja-asetuksen mukaan arvioinnin on sisällettävä vähintään järjestelmällinen kuvaus suunnitelluista käsittelytoimista ja käsittelyn tarkoituksista, arvio käsittelytoimien tarpeellisuudesta ja oikeasuhteisuudesta tarkoituksiin nähden, arvio rekisteröityjen oikeuksia ja vapauksia koskevista riskeistä sekä suunnitellut toimenpiteet riskeihin puuttumiseksi. Vaikutustenarvioinnin tuloksena syntyy näkemys tarvittavista hallintakeinoista, joita tarvitaan pienentämään riskitasoa ja varmistamaan asetuksen vaatimusten toteuttaminen. Tietosuojaa koskevat vaikutustenarvioinnit on luontevaa kytkeä osaksi muuta tiedonhallinnan muutosvaikutusten arviointia.

Suomussalmen kunnalla on käytössä tietosuojan vaikutustenarvioinnin (DPIA) prosessi, joka tehdään tietosuojan hallintaohjelmaan. Vuonna 2024 toteutettiin prosessi, jossa esihenkilöt ja toimistohenkilöstöä koulutettiin tietosuojan vaikutusten arvioinnin tekemiseen. Yhteensä vaikutustenarviointia tehtiin 22 ohjelmasta tai henkilötietojen käsittelytoimesta.

9. Käsiteltävät henkilötiedot ja niiden elinkaaren hallinta

Henkilötietojen elinkaaren hallinnalla pyritään varmistamaan, että henkilötietoja käsitellään vain niin kauan, kuin on niiden käyttötarkoituksen kannalta tarpeellista. Lisäksi pyritään huolehtimaan siitä, että henkilötiedot poistetaan ja asiakirjat hävitetään sen jälkeen, kun määritelty säilytysaika on päättynyt.

Henkilötietojen säilytysaikoja on määritelty osana yleisiä tietojen säilytysaikoja muun muassa kunnan tiedonohjaussuunnitelmassa ja tiedonhallintamallissa. Tiedonhallintamallin kautta tiedot tulevat myös tietosuojaa koskevaan dokumentaatioon, kuten tietosuojaoselosteille ja selosteeseen käsittelytoimista.

10. Sopimukset ja hankinnat

Arvioitaessa tietosuoja-asetuksen asettamia velvoitteita sopimusehtojen kannalta, lähtökohdaksi on otettava asetuksen asettama velvollisuus sopia henkilötietojen käsittelystä sopimuksella, kun joku muu (kuten kunnan palveluntuottaja) käsittelee tietoja rekisterinpitäjän

(kunnan) puolesta. Se kohdistuu sekä rekisterinpitäjään että henkilötietojen käsittelijään. Tietosuoja-asetuksessa säädetään sopimisveloitteen lisäksi tietosuojaa koskevan sopimuksen minimisisältö eli ne kohdat, joista ainakin tulee sopia. Rekisterinpitäjän ja käsittelijän välisiin sopimuksiin ja hankintoihin on laadittu erillinen tietosuoja- ja salassapitoliiite, jossa on määritelty henkilötietojen käsittelyn edellytykset. Osana tiedonhallintamallia kerätään tietoja siitä, mitkä tahot toimivat henkilötietojen käsittelijöinä, ja onko näiden tahojen kanssa sovittu henkilötietojen käsittelystä. Ennen tietosuoja-asetuksen voimaantuloa tehtyihin sopimuksiin muutokset tehdään viimeistään uuden sopimuskauden alkaessa.

11. Lainsäädäntö, koulutus ja ohjeistus

Rekisterinpitäjän on toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja osoittaa, että henkilötietojen käsittelyssä noudatetaan tietosuojasetusta. Organisatorisiin toimenpiteisiin sisältyvät muun muassa koulutukset ja ohjeistukset, joita kunnan henkilötietoja käsitteleville työntekijöille annetaan.

11.1. Henkilötietojen käsittelyä koskeva lainsäädäntö

Kunnan työntekijät joutuvat käsittelemään henkilötietoja työssään monenlaisiin käyttötarkoituksiin. Suurin osa henkilötietojen käsittelystä kunnassa perustuu lakiin sekä yleistä etua koskevaan etuun tai julkiseen valtaan. Laissa ei tarvitse suoraan sanoa, että henkilötietoja saa käsitellä, vaan kunnalla on tehtävään perustuva oikeus henkilötietojen käsittelyyn eli laissa määrätyn tehtävän hoitaminen edellyttää henkilötietojen käsittelyä.

11.2. Henkilötietojen käsittelyä koskeva ohjeistus

Palvelualat ohjeistavat henkilökuntaa tietojärjestelmiensä edellyttämien henkilötietojen käsittelyjen osalta. Kunnassa on oma tietoturva- ja tietosujoaohje.

Hallintopalveluissa on laadittu ohjeistus henkilötietojen käsittelystä kunnan hallinnossa sekä julkaisemisesta toimielinten ja viranhaltijoiden päätöksissä ja päätösten julkaisemisessa avoimessa tietoverkossa. Asian käsittelyssä julkaistaan vain asian käsittelyn kannalta välttämättömät henkilötiedot ja henkilötiedot poistetaan muutoksenhakuajan jälkeen.

12. Henkilötietojen tietosuojaloukkaukset

Henkilötietojen tietosuojaloukkauksella tarkoitetaan tapahtumaa, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu tai niihin pääsee käsiksi ulkopuolinen taho, jolla ei ole oikeutta käsitellä tietoja.

Tietosuojaloukkaus voi tapahtua vahingossa tai tahallisesti. Henkilötietojen tietosuojaloukkauksia ovat esimerkiksi tietojen lähettäminen väärälle henkilölle, kadonnut henkilötietoja sisältävä paperi, omaan työhön kuulumattomien henkilötietojen katselu, kadonnut muistitikku, varastettu tietokone tai murtautuminen henkilötietoja sisältävään järjestelmään.

Tietosuojaloukkausten varalta kunnalla on menettelyohjeistus.

Tietosuojaloukkausilmoituksia oli sivistyspalveluissa kolme, elinvoimapaalveluissa kolme ja teknisissä palveluissa kaksi sekä hallintopalveluissa yksi kappale. Raportoiduista tietosuojaloukkausilmoituksista tehtiin tietoturvaloukkauksen arviointi ja mikään ilmoituksista ei aiheuttanut jatkotoimenpiteitä.

13. Valvontaviranomaisten selvitys- ja tietopyynnöt

Tietosuojavaltuutettu on Suomen kansallinen valvontaviranomainen, joka valvoo tietosuojalainsäädännön noudattamista. Tietosuojavaltuutetun toimisto saattaa lähettää rekisterinpitäjille selvityspyynnöitä. Suomussalmen kuntaan ei tullut selvityspyynnöitä vuonna 2024.

14. Tietosuojatyön kehittämistarpeet

Yksi tietotilinpäätöksen keskeisistä tehtävistä on nostaa esille ongelmakohtia ja kehittymisen paikkoja tietosuojatyössä.

Tietosuojatyöhön liittyviä kehittämiskohteita ovat:

1. Ylläpidetään vuosittain riittävän tietosuoja- ja turvakoulutuksen tarjoamista kunnan henkilökunnalle sekä uuden työntekijän perehdytyksessä.
2. Tietosuojan vaikutusten arvioinnin juurruttaminen ja yksikköjen vastuu omien tietosuojaselosteidensa ajantasaisuudesta
3. Varmistetaan, että kaikki kunnan palvelusopimuskumppanit sitoutuvat noudattamaan palvelutoiminnassaan EU-tietosuoja-asetuksen tietoturva- ja tietosuoja vaatimuksia. Tietoturvasta ja -suojasta laadittu sopimusliite on vakiona käytössä hankintoihin ja sopimuksiin liitettäväksi
4. Tietosuoja- ja tietoturvapoliittikka pidetään ajantasaisena ja päivitetään jälleen vuonna 2025.