

Jämsän seurakunnan tietosuojapolitiikka

Johdanto

Tietosuojapolitiikka määrittää ne periaatteet, toimintatavat, vastuut, valvonnan ja seuraamisjärjestelmän, joita noudatetaan seurakunnan tietosuojan toteuttamisessa ja kehittämisessä. Tämä tietosuojapolitiikka koskee henkilötietojen käsittelyä, jossa seurakunta toimii rekisterinpitäjänä.

Seurakunnan toiminnan perustana ovat seurakunnan jäsenten ja vapaaehtoisten sekä muiden seurakunnan kanssa tekemisissä olevien henkilöiden hengelliset ja hengelliseen toimintaan liittyvät tarpeet.

Seurakunnan johto tietosuojatoiminnan omistajana määrittelee tässä politiikassa johtamiseen ja toimintaan liittyvät tietosuojaperiaatteet, vastuut ja tavoitteet. Poliitiikka toimii perustana seurakunnan tietosuojaan koskeville ohjeille, joiden tehtävänä on tarkentaa politiikassa annettuja määräyksiä ja ohjeistaa niiden soveltamista käytäntöön.

Tietosuojapolitiikka koskee koko seurakunnan henkilöstöä mukaan lukien seurakunnan sidosryhmien edustajia, jotka toimeksiantojensa puitteissa käsittelevät seurakunnan omistamaa tai hallinnoimaa tietoa (mm. luottamushenkilöitä ja vapaaehtoisia). Tietosuojaselosteissa määritellään tarkemmin tiedon omistaja. Poliitiikka kattaa seurakunnan omistaman tiedon riippumatta sen esitystavasta, muodosta, suojaustasosta tai elinkaaren vaiheesta.

Tämä tietosuojapolitiikka on luettavissa seurakunnan kotisivuilta.

Tietosuojan määritelmä

Oikeus henkilötietojen suojaan on jokaiselle kuuluva perusoikeus. Tämä tarkoittaa, että henkilötietojen käsittelyn on yhtäältä oltava asianmukaista ja toisaalta se on aina tapahduttava tiettyä tarkoitusta varten ja asianomaisen henkilön suostumuksella tai muun laissa säädetyn oikeuttavan perusteen nojalla.

Henkilötietojen suojalla tarkoitetaan myös jokaiselle turvattua oikeutta tutustua niihin tietoihin, joita hänestä on kerätty ja tarvittaessa myös saada tiedot muutetuiksi tai poistetuiksi, mikäli tietojen oikaisu on tarpeen.

Tietosuojan tavoitteet ja periaatteet

Tietosuojan arvioinnin lähtökohtana on riskien arviointi. Seurakunta rekisterinpitäjänä arvioi henkilötietojen käsittelyyn liittyvät riskit ja valitsee arvioidun riskitason mukaan tarvittavat hallintatoimenpiteet. Tietosuojariskien hallinta on osa seurakunnan riskienhallintaprosessia, jolloin erityisesti merkittävän tason riskit raportoidaan johdolle saakka.

Riskilähtöisyys ohjaa organisaation henkilötietojen käsittelyä ja on erittäin tärkeä osa rekisterinpitäjän osoitusvelvollisuuden toteuttamista. Seurakunta toteuttaa riskilähtöisen toimintaperiaatteen

varmistamiseksi tietosuojaan vaikutustenarviointeja sellaisten henkilötietojen käsittelytoimille, joiden suunnitteluvaiheessa on todennäköistä, että käsittelytoimiin liittyy yksilöiden oikeuksien ja vapauksien kannalta merkittäviä riskejä.

Vaikutustenarvioinnin tuloksia käytetään niiden hallintakeinojen määrittelemisessä, joilla pyritään pienentämään henkilötietojen käsittelyn riskitasoa. Samalla varmistetaan tietosuoja-asetuksen vaatimusten toteutuminen.

Seurakunnan toiminnassa toteutetaan sisäänrakennetun ja oletusarvoisen tietosuojaan periaatetta. Tietosuoja otetaan huomioon monipuolisesti perustoiminnan yhteydessä (eri toiminnoissa, johtamisessa, hankinnoissa ja kehitystyössä). Tietosuojaan oikeanlainen toteutuminen varmistetaan käyttämällä tilannekohtaisesti parhaita mahdollisia ja tarkoituksenmukaisia teknisiä ja hallinnollisia ratkaisuja.

Seurakunnan tavoitteena on huolehtia tietosuoja-asetuksen mukaisten rekisteröityjen oikeuksien toteutumisesta dokumentoimalla ja ohjeistamalla henkilötietojen käsittelyn käytänteet sekä huolehtimalla henkilötietojen käyttäjien koulutuksesta ja ohjeistamisesta.

Tietosuojaan toteuttaminen

Henkilötietojen käsittely toteutetaan noudattamalla seuraavia periaatteita:

- henkilötietoja käsitellään lainmukaisesti, asianmukaisesti sekä läpinäkyvästi
- henkilötietoja käsitellään suunnitellun käyttötarkoituksen mukaisesti
- henkilötietoja kerätään vain tietyn käyttötarkoituksen mukainen määrä, ei enempää
- henkilötietojen käsittely toteutetaan täsmällisesti
- henkilötietoja säilytetään käyttötarkoituksen kannalta tarkoituksenmukainen aika
- henkilötietojen käsittelyssä toteutetaan henkilötietojen eheyden ja luottamuksellisuuden periaatetta.

Seurakunta toteuttaa sisäänrakennetun ja oletusarvoisen tietosuojaan periaatetta ja sisällyttää tietosuojaperiaatteet ja -vaatimukset jo aikaisessa vaiheessa osaksi henkilötietojen käsittelyä.

Näin varmistetaan, että käsittely vastaa tietosuoja-asetuksen vaatimuksia. Seurakunta toteuttaa tarvittavat tekniset toimenpiteet ja menettelyt tietosuojaan varmistamiseksi.

Näillä toimenpiteillä huolehditaan tietosuojasta niin, että:

- kerätään vain henkilötietoja, jotka ovat välttämättömiä käsittelytarkoituksen kannalta
- tietoja ei kerätä eikä säilytetä suurempia määriä eikä kauemmin kuin on välttämätöntä kyseiseen käsittelytarkoitukseen
- henkilötietoja ei saateta henkilöiden saataville, joille niiden käsittely ei kuulu
- taataan rekisteröityjen oikeuksien toteutuminen
- taataan henkilötietojen suoja tarvittavin tietoturvakeinoin
- taataan, että tietosuojalainsäädännön vaatimukset toteutuvat käsiteltävien henkilötietojen koko elinkaaren ajan.

Seurakunta voi rekisterinpitäjänä ulkoistaa valitsemansa osan henkilötietojen käsittelystä henkilötietojen käsittelijälle. Seurakunta valitsee sopimuskumppanikseen vain sellaisia henkilötietojen käsittelijöitä, jotka noudattavat hyvää henkilötietojen käsittelytapaa sekä täyttävät tietosuoja-asetuksen vaatimukset ja pystyvät huolehtimaan rekisteröidyn oikeuksien toteutumisesta.

Seurakunnan ja erikseen valitun henkilötietojen käsittelijän välille laaditaan sopimus, joka on kirjallinen. Tietosuoja-asetuksen mukaan sopimuksessa tulee määritellä henkilötietojen käsittelyn kohde, tarkoitus ja kesto sekä sopia käsiteltävät henkilötiedot. Sopimuksen sisältö vaatimuksineen tulee määritellä mahdollisimman tarkasti.

Rekisteröityjen tietopyyntöprosessi

Jos rekisteröity käyttää oikeuttaan ja haluaa saada tarkastettavaksi, korjatakseen tietoja tai poistaakseen omia tietojaan, tulee hänen täyttää kirkkoherravirastosta ja seurakunnan kotisivuilta löytyvä henkilötietoja koskeva tietopyyntölomake.

Rekisteröidyn tulee tehdä pyynnöt tietojen tarkistuksesta kirjallisena ja toimittaa pyyntö henkilökohtaisesti Jämsän seurakunnan kirkkoherravirastoon viraston aukioloaikoina. Pyyntöön toimittajalla tulee olla henkilötodistus mukanaan.

Vastaus tietopyyntöön toimitetaan rekisteröidylle ilman aiheetonta viivytystä ja viimeistään kuukauden kuluessa tietopyynnön vastaanotosta. Tarkastusoikeuden käytöstä peritään korvaus, jos edellisestä tarkastuksesta on kulunut vähemmän kuin vuosi.

Henkilöstön tietosuojakoulutus

Seurakunta huolehtii henkilöstön riittävästä tietosuojaosaamisesta henkilöstökoulutuksien ja informaation välittämisen kautta. Uudet työntekijät perehdytetään tietosuoja-asioihin perehdyttämisen yhteydessä. Myös seurakunnassa toimiville vapaaehtoisille painotetaan henkilötietojen suojaamisen tärkeyttä.

Toiminta tietoturva- ja tietosuojapoikkeamatilanteissa sekä ilmoitusvelvollisuus

Henkilötietojen tietoturvaloukkauksella tarkoitetaan tapahtumaa, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu tai niihin pääsee käsiksi ulkopuolinen taho, jolla ei ole oikeutta käsitellä tietoja. Tietoturvaloukkaus voi tapahtua vahingossa tai tahallisesti. Esimerkiksi jos työntekijä lähettää henkilötietoja sisältävän sähköpostin väärälle henkilölle tai jos työtietokone varastetaan tai joku murtautuu henkilötietoja sisältävään järjestelmään.

Kuka tahansa voi havaita tietoturvaloukkauksen. Jos seurakunnan työntekijä havaitsee henkilötietojen tietoturvaloukkauksen on hänen ilmoitettava siitä välittömästi omalle esimiehelleen ja seurakunnan tietoturvasta vastaavalle henkilölle. He arvioivat onko kyseessä todellinen henkilötietoihin kohdistunut tietoturvaloukkaus vai ei. Jos on, he ilmoittavat välittömästi seurakunnan johdolle ja tietosuojavastaavalle.

Ilmoitus tulee tehdä ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa siitä, kun loukkaus on tullut ilmi. Tai jos näin ei voida toimia niin tietosuojavaltuutetun toimistolle on toimitettava perusteltu selitys.

Seurakunnan on ilmoitettava tietoturvaloukkauksesta myös rekisteröidylle, jos loukkaus todennäköisesti aiheuttaa korkean riskin henkilön oikeuksille ja vapauksille. Ilmoitus on tehtävä ilman aiheetonta viivytystä. Jos tietoturvaloukkaus kohdistuu suureen henkilömäärään, loukkauksesta voidaan kertoa median välityksellä julkisena tiedonantona tai muulla vastaavalla tavalla.

Tietosuojavastuut Jämsän seurakunnassa

Tietosuojan vastuujärjestelyjä päivitetään seurakunnan toiminnan tai hallinnon muuttuessa. Jotkut vastuut saattavat kuulua samalle henkilölle tai hänen varahenkilölleen.

Tietosuojatoimintaa johtaa seurakunnan ylin johto, johon kuuluvat kirkkoherra, talousjohtaja, tietosuojan yhteyshenkilö sekä luottamuselimenä kirkkoneuvosto. Vaikka seurakunnalle on valittu tietosuojavastaava, hän ei ole vastuussa seurakunnan henkilötietojen käsittelyn lainmukaisuudesta, vaan seurakunnan johtohenkilöt ovat siitä vastuussa.

Hyvän tietosuojan toteutuminen sisältyy jokaisen työntekijän tavallisiin päivittäisiin työtehtäviin.

TIETOSUOJAVASTUUT

Kirkkoneuvosto:

- Hyväksyy seurakunnan tietosuojapolitiikan.
- Vastaa seurakunnalle annettujen tietosuojaa koskevien määräysten ja ohjeiden noudattamisesta.
- Huolehtii siitä, että seurakunnalle on nimetty tietosuojavastaava ja tietosuojan yhteyshenkilö.
- Huolehtii riittävästä resursseista hoitaa tietosuojaa.

Ylin johto:

- Vastaa henkilötietojen käsittelyn lainmukaisuudesta.
- Huolehtii kirkkoneuvoston päätösten valmistelusta.
- Huolehtii riittävistä työntekijäresursseista.
- Vastaa mahdollisista tietoturvaloukkausten viestinnästä tietosuojan yhteyshenkilön ja tietosuojavastaavan kanssa.
- Huolehtii esimiesten ja muun henkilöstön riittävästä koulutuksesta.

Tietosuojavastaava:

- Valvoo, että henkilötietojen käsittelyssä noudatetaan tietosuojasäännöksiä.
- Neuvo seurakunnan työntekijöitä toimimaan henkilötietojen käsittelyssä tietosuojasäännösten mukaisesti.
- Tiedottaa tietosuojan ohjeita, suosituksia ja määräyksiä seurakunnan työntekijöille.
- Vastanottaa mahdolliset tietosuojaan liittyvät poikkeamat ja raportoi ne eteenpäin tietosuojavaltuutetun toimistoon.
- Raportoi seurakunnan ylimmälle johdolle.
- Rekisteröidyt voivat ottaa yhteyttä tietosuojavastaavaan asioissa, jotka liittyvät heidän henkilötietojensa käsittelyyn ja tietosuoja-asetukseen perustuvien oikeuksiensa käyttöön.

Tietosuojayhteyshenkilö:

- Huolehtii saamiensa tietosuojaan liittyvien ohjeiden, suositusten ja määräysten tiedottamisesta seurakunnan työntekijöille.
- Ottaa vastaan tietosuojaan liittyviä poikkeamia ja välittää ne eteenpäin esimiehelle ja tietosuojavastaavalle.
- Päivittää tietosuojaselosteet yhdessä työalojen vastaavien työntekijöiden kanssa määräajoin.
- Antaa neuvoja ja opastaa työntekijöitä tietosuojaan liittyvissä asioissa.
- Toimii yhteyshenkilönä tietosuojavastaavan ja seurakunnan ylimmän johdon välillä.

Esimies:

- Huolehtii työntekijöidensä osalta siitä, että tietojärjestelmien käyttöoikeudet vastaavat työntehtävien tarpeita.
- Puuttuu kaikkiin havaitsemiinsa tietosuoja koskeviin ongelmiin ja epäkohtiin.
- Välittää tietoa tietosuojaan liittyvistä määräyksistä ja ohjeista työntekijöilleen.
- Järjestää uusien työntekijöiden tietosuojaperehdytyksen ja on myös velvollinen huolehtimaan siitä, että kaikki ymmärtävät asian tärkeyden.
- Huolehtii siitä, että annettuja ohjeita myös noudatetaan.

Työntekijä:

- Perehtyy häntä koskeviin tietosuojan liittyviin ohjeisiin ja noudattaa niitä.
- Ottaa kaikessa toiminnassaan huomioon tietosuoja-asetuksen ja tietosuojalain mukaisen huolellisuusvelvoitteen ja julkisuuslain mukaisen hyvän tiedonhallintatavan.
- Raportoi heti esimiehelleen ja tietosuojayhteyshenkilölle jos huomaa, että on tapahtunut tietoturvaloukkaus.

LIITTEET:

- **Liite 2: Tietosuojan keskeiset käsitteet**