

1. 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 tarpeet.

Seurakunnan johto tietosuojatoiminnan omistajana määrittelee tässä politiikassa johtamiseen ja toimintaan liittyvät tietosuojaperiaatteet, tavoitteet ja vastuut (liite 1 Tietosuojavastuut). 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 (mm. luottamushenkilöitä ja vapaaehtoisia), jotka toimeksiantojensa puitteissa käsittelevät seurakunnan omistamaa tai hallinnoimaa tietoa. Tietosuojaoselosteissa määritellään tarkemmin tiedon omistaja. Poliitiikka kattaa seurakunnan omistaman tiedon riippumatta sen esitystavasta, muodosta, suojaustasosta tai elinkaaren vaiheesta.

Tämä politiikka on saatavissa seurakunnan nettisivuilta ja Teamsin tietosuojakansiosta.

2. 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 (ks. kappale Tietosuojan toteuttaminen). Henkilötietojen suojalla tarkoitetaan myös jokaiselle turvattua oikeutta tutustua niihin tietoihin, joita hänestä on kerätty ja tarvittaessa myös saada hänestä kerätyt tiedot muutetuiksi tai poistetuiksi, mikäli tietojen oikaisu on tarpeen.

3. Tietosuojan tavoitteet ja periaatteet

Seurakunta rekisterinpitäjänä arvioi henkilötietojen käsittelyyn liittyvät riskit ja mahdollisesti toteutuvan riskin vaikutukset (riskilähtöisyys) ja valitsee arvioidun riskitason mukaan tarvittavat hallintatoimenpiteet.

Tietosuojariskien hallinta on osa seurakunnan riskienhallintaprosessia, jolloin erityisesti merkittävän tason riskit raportoidaan johdolle. Riskilähtöisyys ohjaa organisaation henkilötietojen käsittelyä ja on erittäin tärkeä osa rekisterinpitäjän osoitusvelvollisuuden toteuttamista.

Seurakunta toteuttaa riskilähtöisen toimintaperiaatteen varmistamiseksi tietosuojan vaikutustenarvioinnin 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 tietosuojan periaatetta. Tietosuoja otetaan huomioon monipuolisesti perustoiminnan yhteydessä (eri toiminnoissa, johtamisessa, hankinnoissa ja kehitystyössä). Tietosuojan oikeanlainen toteutuminen varmistetaan käyttämällä tilannekohtaisesti parhaita mahdollisia ja tarkoituksenmukaisia teknisiä ja organisatorisia riskiarvioon perustuvia ratkaisuja.

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

4. Tietosuojan toteuttaminen

Henkilötietojen käsittely toteutetaan noudattamalla alla lueteltuja periaatteita:

- henkilötietoja käsitellään lainmukaisesti, asianmukaisesti sekä läpinäkyvästi
- henkilötietoja käsitellään suunnitellun käyttötarkoituksen mukaisesti
- henkilötietoja kerätään 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 tietosuojan periaatetta ja sisällyttää tietosuoja-periaatteet ja -vaatimukset jo aikaisessa vaiheessa osaksi henkilötietojen käsittelyä. Näin varmistetaan, että käsittely vastaa tietosuoja-asetuksen vaatimuksia. Seurakunta toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet ja menettelyt tietosuojan varmistamiseksi. Edellä mainittujen toimenpiteiden avulla varmistetaan muun muassa, että:

- oletusarvoisesti kerätään vain henkilötietoja, jotka ovat välttämättömiä käsittelytarkoituksen kannalta
- tietoja ei kerätä eikä säilytetä suurempia määriä eikä kauemmin kuin on välttämätöntä kyseiseen käsittelytarkoitukseen
- henkilötietoja ei oletusarvoisesti saateta rajoittamattoman henkilömäärän saataville
- taataan rekisteröityjen oikeuksien toteutuminen
- taataan henkilötietojen suoja tarvittavin tietoturvakeinoin

Tietosuojan toteuttamisessa seurakunta varmistaa tietosuojalainsäädännön vaatimusten toteutumisen koko käsiteltävien henkilötietojen 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 EU:n tietosuoja-asetuksen vaatimukset ja pystyvät huolehtimaan rekisteröidyn oikeuksien toteutumisesta.

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

5. Rekisteröityjen tietopyyntöprosessi

Seurakunnassa on määritelty menettelytapa ja -ohje siihen, kun rekisteröity käyttää oikeuttaan saada pääsy rekisteröityihin henkilötietoihinsa. Ohje on nimeltään ”Tietoturvapyyntö henkilörekisteristä” (liite 2). Menettelytapaa noudatetaan, kun rekisteröidyt haluavat saada nähtäväkseen omia rekistereissä olevia henkilötietojaan.

6. Henkilöstön tietosuojakoulutus

Seurakuntayhtymä huolehtii henkilöstön riittävästä tietosuojaosaamisesta henkilöstökoulutuksien ja informaation välittämisen kautta. Myös organisaatioon tulevat uudet työntekijät perehdytetään tietosuoja-asioihin järjestelmällisesti uusien työntekijöiden perehdyttämisen yhteydessä. Keskeiset käsitteet on selvitetty liitteessä 4.

7. Toiminta tietoturva- ja tietosuojapoikkeamatilanteissa

Kun seurakunnassa havaitaan tai seurakunnalle ilmoitetaan tapahtuneesta tietoturvaloukkauksesta tai tietosuojapoikkeamasta, niin tuolloin toimitaan ohjeen ”Toiminta tietoturvaloukkaus” (liite 3) mukaisesti. Ohje on tallennettu Teamsin tietoturvakansioon.