Jokioisten seurakunnan tietosuojapolitiikka KV 4.11.2020

Johdanto

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

Jokioisten seurakunnan toiminnan perustana ovat seurakuntien jäsenten ja vapaaehtoisten sekä muiden seurakunnan kanssa tekemisissä olevien henkilöiden tarpeet.

Seurakunnan johto (kirkkoneuvosto) tietosuojatoiminnan omistajana määrittelee tässä politiikassa johtamiseen ja toimintaan liittyvät tietosuojaperiaatteet, vastuut ja tavoitteet. Tietosuojapolitiikka toimii perustana seurakunnan tietosuojaohjeille, joiden tehtävänä on tarkentaa politiikassa annettuja määräyksiä ja ohjeistaa niiden soveltamista käytäntöön.

Tietosuojapolitiikka koskee seurakunnan henkilöstöä ja niitä seurakunnan sidosryhmien edustajia (mm. luottamushenkilöt ja vapaaehtoiset), jotka käsittelevät seurakunnan omistamaa tai hallinnoimaa tietoa. Tietosuojaselosteissa määritellään tarkemmin tiedon omistaja. Politiikka kattaa seurakunnan omistaman tiedon riippumatta sen esitystavasta, muodosta, suojaustasosta tai elinkaaren vaiheesta.

Tietosuojan määritelmä

Oikeus henkilötietojen suojaan on jokaiselle kuuluva perusoikeus. Tämä tarkoittaa, että henkilötietojen käsittelyn on yhtäältä oltava asianmukaista ja toisaalta sen on aina tapahduttava tiettyä tarkoitusta varten ja asianomaisen henkilön suostumuksella tai muun laissa säädetyn oikeuttavan perusteen nojalla (kts. 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, mikäli tietojen oikaisu on tarpeen, tai poistetuiksi.

Tietosuojan tavoitteet ja periaatteet

Seurakunta rekisterinpitäjänä arvioi henkilötietojen käsittelyyn liittyvät riskit ja mahdollisesti toteutuvan riskin vaikutukset (riskilähtöisyys). Rekisterinpitäjä valitsee arvioidun riskitason mukaan tarvittavat hallintatoimenpiteet. Vaikutustenarvioinnin tuloksia käytetään niiden hallintakeinojen määrittelemisessä, joilla pyritään pienentämään henkilötietojen käsittelyn riskitasoa. Samalla varmistetaan tietosuoja-asetuksen vaatimusten toteutuminen.

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.

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.

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 tietosuojaperiaatteet ja -vaatimukset jo aikaisessa vaiheessa osaksi henkilötietojen käsittelyä. Näin varmistetaan, että käsittely vastaa EU:n 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.

Rekisteröityjen tietopyyntöprosessi

Seurakunnassa on määritelty toimintaprosessi ja -ohje liittyen toimintaan rekisteröityjen käyttäessä oikeuttaan saada pääsy henkilötietoihinsa. Ohje on nimeltään ”Rekisteröityjen tietopyyntöprosessi” Tämän prosessin mukaista toimintatapaa noudatetaan, kun rekisteröidyt haluavat saada nähtäväkseen rekistereissä olevia henkilötietojaan.

Henkilöstön tietosuojakoulutus

Seurakunta huolehtii henkilöstön riittävästä tietosuojaosaamisesta henkilöstökoulutuksien ja informaation välittämisen kautta. Myös organisaatioon tulevat uudet työntekijät perehdytetään tietosuoja-asioihin järjestelmällisesti uusien työntekijöiden perehdyttämisen yhteydessä.

Toiminta tietoturva- ja tietosuojapoikkeamatilanteissa sekä ilmoitusvelvollisuus

Seurakunnassa on määritelty toimintaprosessi ja -ohje, miten toimitaan, kun tapahtuu tietoturvaloukkaus. Tämän prosessin mukaista toimintatapaa noudatetaan tietosuojapoikkeamien sattuessa.

Henkilötietojen tietoturvaloukkauksen sattuessa seurakunnalla on rekisterinpitäjänä ilmoitusvelvollisuus valvontaviranomaisen sekä rekisteröidyn suuntaan. Valvontaviranomaiselle tehdään ilmoitus EU:n tietosuoja-asetuksen mukaisesti 72 tunnin kuluessa siitä, kun henkilötietojen tietoturvaloukkaus on tullut ilmi. Rekisteröidylle henkilötietojen tietoturvaloukkaus ilmoitetaan ilman aiheetonta viivytystä.

Tietosuojarikkomukset käsitellään tapauskohtaisesti Jokioisten seurakunnan tietosuojaelimissä.

Kirkkoneuvosto hyväksyy seurakuntaa koskevat sisäisen valvonnan ja riskienhallinnan periaatteet. Periaatteissa on kuvattu eri toimijoiden tehtävät ja vastuut sisäisen valvonnan ja riskienhallinnan jatkuvassa prosessissa.

Liitteet: Tietosuojavastuut (Liite 1)

Keskeiset käsitteet (Liite 2)