

Tietosuojapolitiikka

Ikaalisten seurakunnan tietosuojapolitiikka

Johdanto

Tietosuojapolitiikka määrittää ne periaatteet, toimintatavat ja vastuut, joita noudatetaan Ikaalisten seurakunnan tietosuojan toteuttamisessa ja kehittämisessä. Tämä tietosuojapolitiikka koskee henkilötietojen käsittelyä, jossa seurakunta toimii rekisterinpitäjänä. Kirkkoneuvoston hyväksymä tietosuojapolitiikka on tietosuojan ylin asiakirja seurakunnassa.

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. Poliitiikka kattaa seurakunnan omistaman tiedon riippumatta sen esitystavasta, muodosta, suojaustasosta tai elinkaaren vaiheesta.

Tämä politiikka on saatavissa Ikaalisten seurakunnan nettisivuilta.

Tietosuojan määritelmä

Oikeus henkilötietojen suojaan on jokaiselle kuuluva perusoikeus. Tämä tarkoittaa, että henkilötietojen käsittelyn tulee olla asianmukaista ja sen on tapahduttava tiettyä tarkoitusta varten joko asianomaisen henkilön suostumuksella tai muun laissa säädetyn oikeuttavan perusteen nojalla (kts. kappale Tietosuojan toteuttaminen). Henkilötietojen suojalla tarkoitetaan myös jokaiselle turvattua oikeutta tutustua tietoihin, joita hänestä on kerätty ja muutostarpeissa saada nämä tiedot oikaistuksi 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 tietosuojasetuksen vaatimusten toteutuminen.

Tietosuojariskien hallinta on osa seurakunnan riskienhallintaprosessia, jossa erityisesti merkittävän tason riskit tulee tunnistaa ja johdon tulee olla niistä tietoinen. Riskilähtöisyys ohjaa organisaation henkilötietojen käsittelyä ja on 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) huomioimalla tietosuojaperiaatteet ja -vaatimukset jo varhaisessa suunnitteluvaiheessa. Tietosuojan toteutuminen varmistetaan käyttämällä tilannekohtaisesti parhaita mahdollisia ja tarkoituksenmukaisia teknisiä ja organisatorisia riskiarvioon perustuvia ratkaisuja.

Seurakunnan tulee huolehtia tietosuojasetuksen mukaisten rekisteröityjen oikeuksien toteutumisesta dokumentoimalla ja ohjeistamalla henkilötietojen käsittelyn käytänteet sekä huolehtimalla käyttäjäkoulutuksesta.

Tietosuojaan 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 tarvittavat tekniset ja organisatoriset toimenpiteet ja menettelyt tietosuojaan 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

Tietosuojaan toteuttamisessa seurakunta varmistaa tietosuojalainsäädännön vaatimusten toteutumisen koko käsiteltävien henkilötietojen elinkaaren ajan.

Seurakunta voi rekisterinpitäjänä ulkoistaa valitsemansa osan henkilötietojen käsittelystä henkilötietojen käsitteijälle. Seurakunta valitsee sopimuskumppanikseen vain sellaisia henkilötietojen käsitteijöitä, jotka noudattavat hyvää henkilötietojen käsittelytapaa sekä täyttävät EU:n tietosuoja-asetuksen vaatimukset ja pystyvät huolehtimaan rekisteröidyn oikeuksien toteutumisesta. Seurakunnan ja erikseen valitun henkilötietojen käsitteijäroolissa toimijan välille laaditaan kirjallinen sopimus. EU:n tietosuoja-asetuksen mukaan sopimuksessa tulee määritellä mahdollisimman tarkasti henkilötietojen käsittelyn kohde, tarkoitus ja kesto sekä sopia käsiteltävät henkilötiedot ja sopimus voi sisältää vaatimuksia.

Rekisteröityjen tietopyyntöprosessi

Seurakunnassa on määritelty toimintaprosessi ja -ohje liittyen toimintaan rekisteröityjen käyttäessä oikeuttaan saada pääsy henkilötietoihinsa. Ohje on nimeltään ”Rekisteröityjen tietopyyntöprosessi”, ja se on netissä seurakunnan tietosuojasivulla. Tätä toimintatapaa noudatetaan rekisteröidyn pyytäessä 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.

Tietosuojaan liittyvät keskeiset periaatteet ja käsitteet löytyvät kirkon tietosuojavastaavien julkaisemasta Kirkon tietosuojakäsikirjasta. Kirkon tietosuojakäsikirja toimii tietopohjana sekä luottamushenkilöille että seurakuntien ylimmille viranhaltijoille ja johtavissa tehtävissä toimiville. Kirkon tietosuojakäsikirjaan tulee johtavissa tehtävissä toimivien tutustua riittävällä tasolla, kirja on nähtävillä mm. seurakunnan internet sivulla sekä kirkon Sakasti-intranetissa.

Toiminta tietoturva- ja tietosuojapoikkeamatilanteissa sekä ilmoitusvelvollisuus

Seurakunnassa on määritelty toimintaprosessi ja -ohje, miten toimitaan, kun tapahtuu tietoturvaloukkaus. Ohje löytyy intranetistä tietosuojasivuilta. Tämän prosessin mukaista toimintatapaa noudatetaan tietoturvapoikkeamien 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 korkeariskinen tietoturvaloukkaus ilmoitetaan ilman aiheetonta viivytystä. Tietosuojarikkomukset käsitellään tapauskohtaisesti Ikaalisten 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.