

VAASAN SEURAKUNTAYHTYMÄN TIETOSUOJA- JA TIETOTURVAPOLITIikka

Hyväksytty yhteisessä kirkkoneuvostossa 28.11.2024

Sisällys

1. Tietosuoja- ja tietoturvapoliitiikan tarkoitus.....	2
2. Tietosuojan ja tietoturvan määritelmät.....	2
3. Tietosuojan yleiset periaatteet.....	3
4. Tietoturvan yleiset periaatteet.....	4
5. Roolit ja vastuut.....	5

1. Tietosuoja- ja tietoturvapoliitiikan tarkoitus

Vaasan seurakuntayhtymä seurakuntineen on yksi tiedonhallintayksikkö, arkistonmuodostaja ja henkilötietojen rekisterinpitäjä. Tietosuoja- ja tietoturvapoliitiikan tarkoituksena on asettaa yhtenäiset tavoitteet tietosuojan ja tietoturvan toteutumiselle koko seurakuntayhtymässä. Tavoitteena on turvata toiminnan luottamuksellisuus sekä vähentää tietosuojaan ja tietoturvaan liittyviä riskejä.

Huolehtimalla tietosuojasta ja tietoturvasta varmistamme, että rekisteröidyt henkilöt voivat luottaa siihen, että heidän yksityisyyttään kunnioitetaan ja henkilötietojaan suojellaan. Noudatamme tietosuojaa ja tietoturvaa koskevaa lainsäädäntöä ja suosituksia, mm. kirkkolakia, tietosuoja-asetusta, tietosuojalakia, julkisuuslakia sekä kirkkolaissa määritellyin osin tiedonhallintalakia, arkistolakia sekä sosiaali- ja terveydenhuollon asiakastietolakia.

Sovellamme tässä politiikassa määriteltyjä periaatteita seurakuntayhtymän kaikissa toiminnoissa. Lisäksi noudatamme Suomen evankelis-luterilaisen kirkon tietoturvapoliittikkaa ja tietoturvamääräyksiä. Seurakuntayhtymän ja IT-alueen ohjeissa täsmennetään, miten toteutamme tietosuojaa ja tietoturvaa koskevia periaatteita käytännössä.

2. Tietosuojan ja tietoturvan määritelmät

Tietosuojalla tarkoitetaan henkilötietojen suojaamista tietosuojalainsäädännön mukaisesti. Tietosuoja on perusoikeus, joka turvaa rekisteröidyn henkilön oikeudet henkilötietojen käsittelyssä. Henkilötietoja ovat kaikki tiedot, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön.

Tietoturvalla tarkoitetaan niitä toimenpiteitä, joilla turvataan tietojen luottamuksellisuus, eheys ja saatavuus. Tietoturvan avulla varmistetaan, että

- tiedot ovat ainoastaan niiden tahojen saatavilla, joilla on lupa käsitellä tietoja (luottamuksellisuus);
- tietoja muutetaan vain hallitusti, eivätkä ne muutu tai katoa vahingossa (eheys);
- tiedot ovat saatavilla, kun niitä tarvitaan (saatavuus).

Tietoturvatoinenpitemet mahdollistavat henkilötietojen turvallisen käsittelyn. Siten tietoturva on yksi tietosuojan toteuttamisen keino.

3. Tietosuojan yleiset periaatteet

Asianmukaisuus ja käyttötarkoitussidonnaisuus

Käsitlemme henkilötietoja asianmukaisesti ja vain sellaisessa tarkoituksessa, joka on perusteltua seurakunnan toiminnan kannalta. Käsitlemme tietoja ainoastaan tietosuoja-asetuksen mukaisten oikeusperusteiden nojalla.

Arvioimme henkilötietojen käsittelyn vaikutuksia ja riskejä henkilön oikeuksien kannalta. Otamme tietosuojan huomioon kaikessa henkilötietojen käsittelyssä.

Huolehdimme erityisiin henkilötietoryhmiin kuuluvien henkilötietojen suojaamisesta. Käsitlemme näitä tietoja vain lain sallimissa rajoissa ja vain sen verran kuin on välttämätöntä. Erityisiä henkilötietoryhmiä ovat mm. terveyttä, uskontokunnan ja ammattiliiton jäsenyyttä sekä seksuaalista suuntautumista koskevat tiedot.

Luottamuksellisuus

Huolehdimme siitä, että kaikki työntekijät, vapaaehtoistyöntekijät, luottamushenkilöt ja muut käsittelyyn osallistuvat henkilöt ovat tietoisia tietosuojaa koskevista velvollisuuksistaan. Heitä sitoo lakisääteinen tai erikseen kirjallisesti sovittu salassapitovelvollisuus.

Luovutamme henkilötietoja kolmansille osapuolille vain, jos laki siihen velvoittaa tai jos luovutukseen on henkilön suostumus tai muu oikeusperuste.

Varmistamme, että yhteistyökumppanit ja alihankkijat ovat sitoutuneita tietosuojaperiaatteisiimme. Huolehdimme asianmukaisten sopimusten laatimisesta sekä ohjeiden antamisesta yhteistyökumppaneille.

Täsmällisyys

Huolehdimme siitä, että henkilötiedot ovat ajan tasalla ja että virheelliset henkilötiedot poistetaan tai korjataan viipymättä.

Osoitusvelvollisuus

Dokumentoimme henkilötietojen käsittelytoiminnot asianmukaisesti ja tarkastelemme dokumentaatiota säännöllisesti.

Säilytyksen rajoittaminen

Säilytämme henkilötietoja vain sen ajan kuin laissa on vaadittu tai käsittelyn tarkoituksen edellyttämän ajan. Kun emme enää tarvitse henkilötietoja, poistamme, anonymisoimme tai arkistoimme ne arkistonmuodostussuunnitelman mukaisesti.

Läpinäkyvyys

Toimimme henkilötietojen käsittelyssä läpinäkyvästi siten, että rekisteröidyt ovat tietoisia, mitä tietoja käsitlemme, miten ja missä tarkoituksessa.

Rekisteröidyn oikeuksista huolehtiminen

Huolehdimme rekisteröidyn oikeuksien toteuttamisesta. Lain mukaan rekisteröidyllä on oikeus pyytää pääsy häntä itseään koskeviin henkilötietoihin sekä oikeus pyytää kyseisten tietojen oikaisemista, poistamista tai siirtämistä toiseen järjestelmään tai käsittelyn rajoittamista. Rekisteröidyllä on myös oikeus vastustaa käsittelyä. Lisäksi rekisteröidyllä on oikeus peruuttaa henkilötietojen käsittelyä koskeva suostumus, jos käsittely perustuu suostumukseen. Rekisteröidyllä on oikeus tehdä valitus valvontaviranomaiselle.

Rekisteröidyn oikeuksien käyttö voi olla rajoitettua silloin, kun käsittelemme tietoja esimerkiksi lakisääteisen tehtävän perusteella.

4. Tietoturvan yleiset periaatteet

Lakisääteinen tietoturva

Tietosuoja-asetuksen mukaan rekisterinpitäjän on tunnistettava henkilötietojen käsittelyyn liittyvät riskit ja toteutettava riskeihin nähden riittävät toimenpiteet tietojen suojaamiseksi. Arkistolaissa määrätään, että asiakirjoja on säilytettävä siten, että ne ovat turvassa tuhoutumiselta, vahingoittumiselta ja asiattomalta käytöltä. Tiedonhallintalaissa puolestaan säädetään velvollisuudesta huolehtia tietoaineistojen ja tietojärjestelmien tietoturvallisuudesta.

Fyysinen tietoturva

Huolehdimme tietojen luottamuksellisuudesta, eheydestä ja saatavuudesta riittävillä fyysisillä toimenpiteillä. Näitä toimenpiteitä ovat esimerkiksi lukitus- ja kulunvalvontajärjestelmät sekä arkistotilojen suojaaminen.

Tekninen tietoturva

Huolehdimme tietojen luottamuksellisuudesta, eheydestä ja saatavuudesta riittävillä teknisillä toimenpiteillä. Toteutamme teknistä tietoturvaa yhteistyössä IT-alueen, Kirkon palvelukeskuksen sekä muiden laitetoimittajien ja tietojärjestelmätoimittajien kanssa. Huolehdimme käyttäjähallinnasta ja noudatamme käyttöoikeuksien minimoimisen periaatetta.

Hallinnollinen tietoturva

Huolehdimme tietojen luottamuksellisuudesta, eheydestä ja saatavuudesta riittävillä hallinnollisilla toimenpiteillä. Näitä toimenpiteitä ovat esimerkiksi ohjeiden laatiminen, henkilöstön kouluttaminen sekä tietoturvan ja tietojenkäsittelyn dokumentointi.

Tietoturvaloukkauksiin reagoiminen

Käsittelemme tietoturvaloukkaukset asianmukaisesti ja kiireellisesti tietosuojalainsäädännön edellyttämällä tavalla. Teemme kaikki toimenpiteet, jotka ovat tarpeen henkilöihin kohdistuvien haitallisten vaikutusten lieventämiseksi tietoturvaloukkaustilanteessa.

5. Roolit ja vastuut

Yhteinen kirkkovaltuusto

Yhteinen kirkkovaltuusto on seurakuntayhtymän ylin päättävä elin, joka hyväksyy seurakuntayhtymän toiminta- ja taloussuunnitelman, tilinpäätöksen ja toimintakertomuksen, joihin sisältyvät tietosuoja- ja tietoturva-asiat.

Yhteinen kirkkoneuvosto

Yhteinen kirkkoneuvosto vastaa siitä, että seurakuntayhtymä täyttää tietosuoja- ja tietoturvaa koskevan lainsäädännön velvoitteet, ja valvoo tietosuojan ja tietoturvan toteutumista. Yhteinen kirkkoneuvosto on hyväksynyt tämän tietosuoja- ja tietoturvapoliitiikan ja sitoutunut siihen.

Lisäksi yhteinen kirkkoneuvosto

- vastaa seurakuntayhtymälle annettujen tietoturvallisuutta koskevien määräysten ja ohjeiden noudattamisesta;
- huolehtii siitä, että seurakuntayhtymälle on nimetty tietosuojan ja tietoturvan yhteyshenkilöt;
- hyväksyy seurakuntayhtymän tietosuoja- ja tietoturvapoliitiikan, joka on yhteensopiva IT-alueen tietoturvapoliitiikan ja kirkon tietosuoja- ja tietoturvaa koskevien linjausten kanssa.

Tietosuojavastaava

Yhteinen kirkkoneuvosto nimittää tietosuojavastaavan hoitamaan tietosuoja-asetuksen mukaisia tehtäviä. Tietosuoja-asetuksen mukaan tietosuojavastaava

- seuraa tietosuojasääntöjen noudattamista organisaatiossa;
- antaa tietoa ja neuvoja tietosuojalainsäädännön mukaisista velvollisuuksista johdolle ja työntekijöille;
- tekee yhteistyötä valvontaviranomaisen kanssa ja on valvontaviranomaisen yhteyshenkilö.

Tietosuojaytöryhmä

Yhteinen kirkkoneuvosto nimeää tietosuojaytöryhmän, jossa on jäseniä erityisesti niiltä työaloilta, joissa henkilötietojen käsittelyn riskit ovat suurimmat. Tietosuojaytöryhmä

- valmistelee ja kehittää dokumentaatiota, ohjeistusta ja sisäisiä menettelytapoja tietosuojan toteuttamiseksi ja osoittamiseksi;
- raportoi toiminnastaan ja tietosuojan tilasta yhteiselle kirkkoneuvostolle.

Tietosuojan ja tietoturvan yhteyshenkilö

Yhteinen kirkkoneuvosto nimeää tietosuojan ja tietoturvan yhteyshenkilön. Yhteyshenkilö

- toimii tietosuojaytöryhmän koollekutsujana;
- toimii yhteyshenkilönä seurakuntayhtymän ja tietosuojavastaavan välillä;
- huolehtii saamiensa tietosuojan ja tietoturvaan liittyvien ohjeiden, suositusten ja määräysten tiedottamisesta kaikille työntekijöille;

- osallistuu esihenkilöiden tukena uusien työntekijöiden perehdyttämiseen tietosuoja ja tietoturva koskeissa kysymyksissä;
- ottaa vastaan ilmoituksia seurakuntayhtymässä havaituista tietoturvapoikkeamista ja tietoturvaloukkauksista ja raportoi niistä IT-alueen tietoturvavastaavalle sekä seurakuntayhtymän johtoryhmälle.

Johto ja esihenkilöt

Seurakuntayhtymän johto ja esihenkilöt

- vastaavat siitä, että tietosuoja huomioidaan arjen toiminnassa, päätöksenteossa ja sopimuksissa;
- varmistavat, että kaikki heidän alaisensa ovat tietoisia tietosuoja- ja tietoturvapolitiikan ja -ohjeiden sisällöstä ja noudattavat niitä;
- ilmoittavat tietosuojan ja tietoturvan yhteyshenkilölle, jos on suunnitteilla muutoksia tai uudistuksia, joihin liittyy henkilötietojen käsittelyä.

Työntekijät, vapaaehtoiset ja luottamushenkilöt

Jokainen työntekijä, vapaaehtoistyöntekijä ja luottamushenkilö

- noudattaa omassa toiminnassaan tietosuojaan ja tietoturvaan liittyviä ohjeita ja asianmukaisia toimintatapoja;
- on vaitiolovelvollinen tietosuojalain 35 § sekä allekirjoittamansa salassapitositoumuksen mukaisesti;
- on velvollinen välittömästi ilmoittamaan tietosuojan ja tietoturvan yhteyshenkilölle havaitsemastaan tietoturvaloukkauksesta tai -poikkeamasta.

IT-alueen tietoturvaryhmä

Rannikon IT-keskuksen tietoturvaryhmä ylläpitää IT-alueen seurakuntatalouksien tietoturvapolitiikkaa ja tietoturvallisuuteen liittyviä määräyksiä, ohjeita ja suosituksia siten, että ne ovat linjassa kirkon yhteisten määräysten kanssa. Tietoturvaryhmä

- valvoo tietoturvamääräysten noudattamista;
- käsittelee ajankohtaisia tietoturvallisuutta koskevia kysymyksiä;
- suunnittelee ja järjestää tietoturvallisuuteen liittyvää koulutusta.

IT-alueen tietoturvavastaava

Rannikon IT-keskuksen tietoturvavastaava kehittää IT-alueen seurakuntien tietoturvallisuutta.

Tietoturvavastaava

- vastaa tietoturvallisuuteen liittyvien ohjeiden, suositusten ja määräysten tiedottamisesta;
- ottaa vastaan havaintoja tietoturvallisuuteen liittyvistä tapahtumista ja poikkeamista ja raportoi ne säännöllisesti tietoturvaryhmälle ja kirkon tietoturvapäällikölle;
- hyväksyy tietoturvauhan tai poikkeamatilanteen yhteydessä sellaisen seurakuntatalouden tietoturvamääräyksen, joka on voimassa enintään kaksi kuukautta.