TIETOSUOJAPOLITIIKKA

Hyväksytty Rautavaaran seurakunnan kirkkovaltuustossa 18.12.2018. / § 15

Voimassa 1.1.2019 - 31.12.2022.

TIETOSUOJAPOLITIIKAN LÄHTÖKOHTA

Oikeus henkilötietojen suojaan on jokaiselle kuuluva perusoikeus. Tämä tarkoittaa sitä, että henkilötietojen käsittelyn on oltava asianmukaista ja rekisterinpitäjällä on käsittelemiseen lainmukaiset perusteet. Rautavaaran seurakunta noudattaa toiminnassaan EU:n tietosuoja-asetuksen (2016/679) ja kansallisen tietosuojalain (säätäminen kesken, pohjautuu HE 9/2018) perusperiaatteita, joilla turvataan yksilön oikeudet henkilötietojen käsittelyn kaikissa käsittelyvaiheissa koko tiedon elinkaaren ajan.

Tietosuojapolitiikka, joka on seurakunnan ylin tietosuojaa ohjaava dokumentti, määrittää ne periaatteet, toimintatavat, vastuut, valvonnan ja seuraamusjärjestelmän, joita noudatetaan Rautavaaran seurakunnan tietosuojan toteuttamisessa ja kehittämisessä. Asiakirjaa sovelletaan sellaiseen henkilötietojen käsittelyyn, jossa seurakunta toimii rekisterinpitäjänä. Tietosuojapolitiikka koskee koko seurakuntaorganisaatiota (henkilöstö, vapaaehtoistyöntekijät ja luottamushenkilöt) mukaan lukien ne seurakunnan sidosryhmien edustajat, jotka toimeksiantojensa puitteissa käsittelevät Rautavaaran seurakunnan omistamaa tai hallinnoimaa tietoa riippumatta sen esitystavasta, muodosta, suojaustasosta tai elinkaaren vaiheesta.

Seurakunnan palveluiden perustana ovat seurakuntalaisten tarpeet ja tietyt viranomaistoiminnot. Toimintaympäristön laaja-alaisuus ja monimuotoisuus aiheuttavat sen, että henkilötietojen tietosuoja-asetuksen mukaisen käsittelyn merkitys on korostetun suuri. Noudattamalla Suomen evankelis-luterilaisen kirkon tietoturvamääräyksiä ja tämän tietosuojapolitiikan periaatteita varmistetaan, että EU:n yleisen tietosuoja-asetuksen ja sitä täydentävän kansallisen tietosuojalain sekä muiden henkilötietojen käsittelyä seurakunnissa ohjaavien lakien asettamat vaatimukset rekisterinpitäjälle henkilötietojen käsittelyssä täyttyvät.

Tietosuojapolitiikka on julkinen asiakirja, jonka hyväksyy aina kirkkovaltuusto. Asiakirja hyväksytään kirkkovaltuustokaudeksi (4 vuotta), mutta sitä päivitetään tarpeen mukaan. Mahdollisista muutoksista ilmoitetaan aina sekä henkilökunnalle että sidosryhmille ja voimassa oleva versio on julkaistuna seurakunnan internetsivuilla.

TIETOSUOJAN TAVOITTEET JA PERIAATTEET

Tavoitteena on huolehtia tietosuoja-asetuksen mukaisten rekisteröityjen oikeuksien toteutumisesta dokumentoimalla ja ohjeistamalla henkilötietojen käsittelyn käytänteet sekä huolehtimalla käyttäjäkoulutuksesta. Tietosuoja-asetuksen mukaista ohjeistusta ylläpidetään suunnitelmallisesti tietosuojavastaavan toimiessa asiantuntijana ja neuvonantajana.

Seurakunnan toiminnassa toteutetaan sisäänrakennetun ja oletusarvoisen tietosuojan periaatetta ja ne sisällytetään jo aikaisessa vaiheessa osaksi henkilötietojen käsittelyä. Tietosuoja otetaan huomioon monipuolisesti muun muassa johtamisessa, hankinnoissa, kehitystyössä sekä toimintaprosesseissa. Tietosuojan oikeanlainen toteutuminen varmistetaan myös käyttämällä tilannekohtaisesti parhaita mahdollisia teknisiä ja organisatorisia riskiarvioon perustuvia ratkaisuja.

Rekisterinpitäjänä seurakunta arvioi henkilötietojen käsittelyyn liittyvät riskit ja valitsee arvioidun riskitason mukaan tarvittavat hallintatoimenpiteet. Riskilähtöisen toimintaperiaatteen varmistamiseksi tehdään tietosuojan vaikutustenarviointeja, joiden tuloksia käytetään sopivien riskitason pienentämiseen tähtäävien keinojen määrittämiseen.

HENKILÖTIETOJEN KÄSITTELYN PERIAATTEET

Perusperiaatteet Rautavaaran seurakunnan omistaman tai hallinnoiman henkilötiedon käsittelyssä:

- 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
- henkilötietojen käsittelystä annetaan henkilöstölle kirjalliset ohjeet

Rautavaaran seurakunta huolehtii henkilöstönsä (palkattuun henkilöstöön rinnastuvat tässä myös seurakunnan luottamushenkilöorganisaatioissa sekä henkilötietojen käsittelyä edellyttävissä vapaaehtoistehtävissä toimivat vastuunkantajat) riittävästä tietosuojaosaamisesta henkilöstökoulutuksien ja muun informaation välittämisen kautta. Myös organisaatioon tulevat uudet toimijat perehdytetään tietosuoja-asioihin järjestelmällisesti. Erityisesti tämä korostuu niissä tehtävissä, joissa käsitellään henkilötietoja ja toteutetaan rekisteröityjen oikeuksien toteuttamisprosesseja.

Rautavaaran seurakunta voi rekisterinpitäjänä ulkoistaa valitsemansa osan henkilötietojen käsittelystä toimeksisaajalle, henkilötietojen käsittelijälle. Sopimuskumppaneiksi valitaan vain sellaisia henkilötietojen käsittelijöitä, jotka noudattavat hyvää henkilötietojen käsittelytapaa asianmukaisten teknisten ja organisatoristen toimenpiteiden avulla, täyttävät tietosuoja-asetuksen vaatimukset ja pystyvät huolehtimaan rekisteröidyn oikeuksien toteutumisesta. Henkilötietojen käsittelyä sisältävien hankintojen kohdalla tietosuojaan liittyvät näkökohdat huomioidaan jo hankinnan suunnitteluvaiheessa ja ne saatetaan osaksi tarjouspyyntöä sekä myöhemmin laadittavaa kirjallista sopimusta. Tietosuoja-asetuksen mukaan sopimuksessa tulee määritellä tarkasti henkilötietojen käsittelyn kohde, tarkoitus ja kesto sekä käsiteltävät henkilötiedot. Rekisterinpitäjä vastaa henkilötietojen käsittelijälle annettavasta ohjeistuksesta.

Rautavaaran seurakunnalla on määritetty toimintaprosessi ja -ohje rekisteröityjen oikeuksien toteuttamiseksi. Tämän prosessin mukaista toimintatapaa noudatetaan silloin, kun rekisteröidyt ilmaisevat halunsa käyttää EU:n yleisessä tietosuoja-aseuksessa kuvattuja oikeuksiaan. Seurakunta huolehtii siitä, että tieto ohjeistuksesta sekä sen sisällöstä on kaikkien työntekijöiden helposti saavutettavissa. Rekisteröidylle informoidaan hänen oikeuksistaan sekä tavasta, jolla oikeutta seurakunnassa toteutetaan ennen tietojen kirjaamista tietosuoja-asetuksen ja – lain vaatimukset huomioon ottaen.

TOIMINTA TIETOSUOJAPOIKKEAMATILANTEISSA SEKÄ ILMOITUSVELVOLLISUUS

Rautavaaran seurakunta noudattaa Suomen evankelis-luterilaisen kirkon tietoturvapolitiikkaa, jossa on määritetty toimintaprosessi ja ohje tietoturvaloukkausten varalta. Tämän prosessin mukaista toimintatapaa noudatetaan myös tietosuojapoikkeamia havaittaessa.

TIETOSUOJAVASTUUT ORGANISAATIOSSA

Tietosuojan toteutumisen valvontaan ja ylläpitämiseen osallistuu jokainen seurakunnan henkilöstöön ja järjestelmien ja palveluiden käyttäjiin kuuluva osana omaa yleistä toimintavastuutaan. Suurin osa tietosuojan toteuttamiseksi tehdystä työstä sisältyy Rautavaaran seurakunnassa työskentelevien normaaleihin tehtäviin. Tietosuojan ohjaustehtävissä ja kehittämisessä tarvitaan sen lisäksi erityisasiantuntemusta ja nimettyjä vastuuhenkilöitä.

Johdon vastuu

Rekisterinpitäjän ylin johto on aina viimekädessä vastuussa kaikessa alaisuudessaan tapahtuvasta henkilötietojen käsittelystä, myös silloin kun käsittely on annettu tehtäväksi kolmannelle osapuolelle. Johdon tehtävänä on määrittää, miten henkilötietoja käsitellään ja ohjeistaa kaikkia käsittelyn osapuolia, sekä valvoa käsittelyn asianmukaisuutta.
Tietosuojan vastuujärjestelyiden tulee seurata seurakunnan toiminnan mahdollisia muutoksia. Olennaista on, että tehtävien hoito on järjestetty, myös varahenkilöiden osalta.

Tietosuojavastaavan rooli

EU:n yleisen tietosuoja-asetuksen mukaisesti Rautavaara seurakunnalle nimetään tietosuojavastaava. Nimittämisestä päättää joko määräaikaiseksi tai toistaiseksi voimassa olevaksi seurakunnan kirkkoneuvosto. Nimitys voi olla myös osa-aikainen tai jaettu. Mikäli tietosuojavastaavan tehtävät on järjestetty IT-aluekohtaisena palveluna, sisällytetään tietosuojavastaavan tehtävät kyseessä olevien seurakuntien IT-alueen yhteistyösopimukseen.

Tietosuojavastaavan tehtävänkuva ja esimiessuhteet määritellään tarvittaessa erikseen kuitenkin siten, ettei tietosuojavastaavan riippumattomuus tietosuojatehtäviä hoitaessaan vaarannu. Tietosuojatehtävien osalta tietosuojavastaavan esimiehenä toimii Rautavaaran seurakunnan talouspäällikkö.

Tietosuojavastaava raportoi toiminnastaan ja seurakunnan tietosuojan tilasta ylimmälle johdolle. Kirjallinen tietotilinpäätös laaditaan ja esitetään kirkkoneuvoston toimikauden 1. neljänneksellä ja viedään sen jälkeen kirkkovaltuustolle tiedoksi.

Tietosuojaryhmän tai tietosuojahenkilön rooli

Suomen evankelis-luterilaisen kirkon ohjeistuksen mukaisesti tietosuojavastaavan lisäksi seurakuntiin on nimettävä tietosuojaryhmä tai tietosuojahenkilö. Rautavaaran seurakunnassa valitaan tietosuojahenkilö.

Seurakunnan vastuunjako tietosuojan asiakirjojen laadinnassa on esitetty tämän asiakirjan liitteessä 1.

LIITE 1 VASTUUT TIETOSUOJAN ASIAKIRJOISTA

Seurakunnassa tietosuojaan liittyvät asiakirjat laaditaan oheisen vastuutaulukon perusteella:

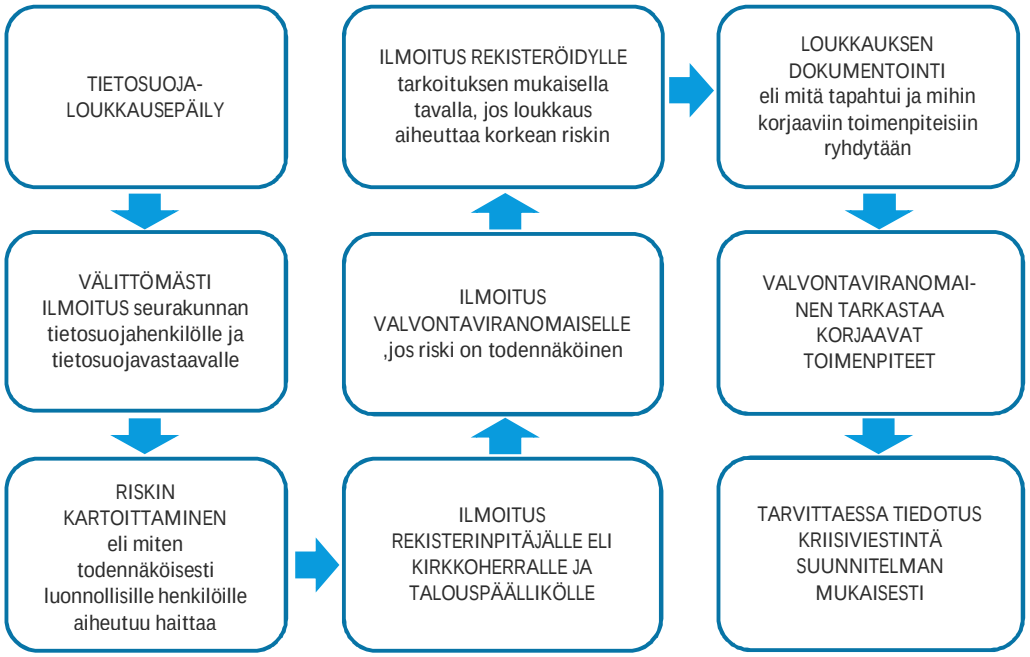
Dokumentaatio	Hyväksyjä	Laadinta- ja tiedotusvastuu	Informointi
tietosuojapolitiikka	kirkkovaltuusto	rekisterinpitäjän johto	koko organisaatio ja sidosryhmät
toimintaohje tietosuojaloukkausepäilyssä	kirkkovaltuusto osana tietosuojapolitiikkaa	rekisterinpitäjän johto	koko organisaatio ja sidosryhmät
tietosuojarikkomukset ja seuraamukset	kirkkovaltuusto osana tietosuojapolitiikkaa	rekisterinpitäjän johto	koko organisaatio ja sidosryhmät
tietosuojavastaavan tehtävänkuva	kirkkoneuvosto	valmistelu sen viranhaltijan tai luottamuselimen toimesta, jolle on johtosäännössä tai sopimuksessa määritelty tietosuojavastaavan toiminnan seurakunnallinen tai alueellinen koordinointi.	koko organisaatio
seloste käsittelytoimista (koko seurakunta)	rekisterinpitäjän johto	rekisterinpitäjän johto	informointi tietosuoja-asetuksen mukaisesti
tietosuojaselosteet	rekisterinpitäjän johto	rekisterinpitäjän johto tai kunkin toiminnan seurakunnallinen vastuuhenkilö	informointi tietosuoja-asetuksen mukaisesti
tietosuojaohjeet organisaation ja sidosryhmien käyttöön	rekisterinpitäjän johto	rekisterinpitäjän johto	koko organisaatio ja sidosryhmät
asiakkaan informointikäytänteet	rekisterinpitäjän johto	rekisterinpitäjän johto	koko organisaatio
seuranta- ja valvontasuunnitelmat	rekisterinpitäjän johto	tietosuojavastaava	hallintojohtaja/ rekisterinpitäjän johto
riskilähtöinen vaikutustenarviointi	rekisterinpitäjän johto	rekisterinpitäjän johto yhdessä tietosuojavastaavan kanssa.	hallintojohtaja/ rekisterinpitäjän johto
tietosuojavastaavan toimenpiderekisteri		tietosuojavastaava	tietosuojayhteyshenkilö/ kirkkoneuvosto
koulutus ja perehdytyssuunnitelmat	rekisterinpitäjän johto	rekisterinpitäjän johto yhdessä tietosuojavastaavan kanssa	koko organisaatio

LIITE 2 TOIMINTAMALLIT

Henkilötietojen tietosuojaloukkauksen osalta Rautavaaran seurakunnalla on rekisterinpitäjänä ilmoitusvelvollisuus sekä valvontaviranomaiselle että rekisteröidylle, jos loukkauksesta voi aiheutua riski luonnollisten henkilöiden oikeuksille ja vapauksille. Valvontaviranomaiselle tehdään ilmoitus tietosuoja-asetuksen mukaisesti 72 tunnin kuluessa siitä, kun henkilötietojen tietoturvaloukkaus on tullut ilmi. Rekisteröidylle henkilötietojen tietoturvaloukkaus ilmoitetaan ilman aiheetonta viivytystä, mikäli riskiarvion perusteella se katsotaan aiheelliseksi.

Kaikki tietosuojaloukkaukset ja niiden käsittely kirjataan tietosuojavastaavan toimenpiderekisteriin, loukkauksista ilmoitetaan rekisterinpitäjän johdolle riippumatta loukkauksen vakavuudesta ja siitä onko ilmoitus valvontaviranomaiselle katsottu tarpeelliseksi.

Tietosuojaloukkauksen tapahduttua toimitaan seuraavasti:



Tietosuojarikkomukset käsitellään tapauskohtaisesti ja mahdollisiin seuraamuksiin sovelletaan seuraavaa tietosuojarikkomusten seuraamustaulukkoa:

TEON TAHALLISUUDEN ASTE

RIKKOMUKSEN VAKAVUUS

	Tietämättömyys Osaamattomuus Huolimattomuus Vahinko Tahattomuus	Piittaamattomuus Törkeä huolimattomuus Välinpitämättömyys Tahallisuus Toistuvuus	Rikoksentekotarkoitus (Vahingonteko, luvaton käyttö, vakoilu, salassapitorikos, aseman/väärinkäyttö) Hyötymistarkoitus
Vakava rikkomus/rikos Asiakastiedon tai liikesalaisuuden luvaton käsittely ja luovuttaminen. Rikoslain alaisen materiaalin oikeudeton käsittely. Tekijänoikeuslain alaisen materiaalin laiton levittäminen.	Työnantaja käynnistää palvelussuhteen päättämismenettelyn Tutkintapyyntö poliisille harkintaan Kirjallinen varoitus	Työnantaja käynnistää palvelussuhteen päättämismenettelyn Tutkintapyyntö poliisille Kirjallinen varoitus	Työnantaja käynnistää palvelussuhteen päättämismenettelyn Tutkintapyyntö poliisille
Rikkomus (vakava väärinkäyttö tai turvallisuuden vaarantaminen) Ohjelmien tai pelien luvaton kopiointi. Ylläpitäjän työkalujen luvaton hallussapito. Tunnuksen luovuttaminen. Tiedon luottamuksellisuuden vaarantaminen.	Kirjallinen varoitus Huomautus	Työnantaja käynnistää palvelussuhteen päättämismenettelyn Käyttöoikeuden peruminen Kirjallinen varoitus	Työnantaja käynnistää palvelussuhteen päättämismenettelyn Tutkintapyyntö poliisille Kirjallinen varoitus
Lievä rikkomus (väärinkäytös) Henkilökohtaisen tietoturvan laiminlyönti. Epäasiallinen käytös. Haitan aiheuttaminen. Resurssien tuhlaus. Luvaton kaupallinen tai poliittinen toiminta. Kulunvalvontasääntöjen rikkominen.	Huomautus Opastus Puheeksi ottaminen	Kirjallinen varoitus Opastus Huomautus Puheeksi ottaminen	Tutkintapyyntö poliisille harkintaan Kirjallinen varoitus