LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

# Näkökulmia Suomen Helluntaikirkon tietosuojakäytäntöön

Juha Koski

2018 Laurea

**Laurea-ammattikorkeakoulu**

# Näkökulmia Suomen Helluntaikirkon tietosuojakäytäntöön

Juha Koski
Liiketalouden koulutusohjelma
Opinnäytetyö
Huhtikuu, 2018

**Laurea-ammattikorkeakoulu** **Tiivistelmä**
Liiketalouden koulutusohjelma
Tradenomi (AMK)

Juha Koski

**Näkökulmia Suomen Helluntaikirkon tietosuojakäytäntöön**

Vuosi 2018 Sivumäärä 65

Opinnäytetyössä tarkastellaan Suomen Helluntaikirkon tietosuojakäytäntöä. Taustalla on keväällä 2018 voimaan tuleva Euroopan Unionin uusi tietosuoja-asetus ja sen johdosta valmisteltava Suomen uusi tietosuojalaki. Näillä on vaikutusta Helluntaikirkon toimintaan. Opinnäytetyön tavoitteena on toimia yhtenä dokumenttina yhdyskunnalle tietosuojan kehittämiseksi. Helluntaikirkko voi halutessaan soveltaa opinnäytetyön tuotoksia uudistaessaan tietosuojakäytäntöään.

Tietoperustassa kuvataan tietosuoja-asetus Helluntaikirkolle soveltuvin osin sekä esitellään muutamia tietoturvaratkaisuja ja näkökulmia. Myöhemmin haastatellaan neljää yhdyskunnan henkilöä tietosuoja-asetuksesta. Tavoitteena on löytää käytännöllisiä paikallisia ja valtakunnallisia ratkaisuja tietoperustan pohjalta Helluntaikirkon tietosuojan parantamiseksi.

Opinnäytetyön tuloksena havaittiin tarve yhteisille koulutuksille ja dokumentaation tuottamiselle. Vaikka seurakunnat ovat erilaisia, samaan aikaan on paljon yhteistäkin, jolloin yhteiset dokumentit auttaisivat kehittämään toimintaan asetuksenmukaiseen suuntaan. Helluntaikirkon toimisto ymmärtää vastuunsa materiaalin tuottamiselle, mutta resurssinsa haasteellisiksi. Koulutuksiakin on jo järjestetty yhdessä helluntailiikkeen oman IK-opiston kanssa. Näiden yhtenä tavoitteena on ollut tukea jäsenseurakuntien omaa prosessia tietosuojan parantamiseksi.

Tuloksena havaittiin myös suljettujen sähköisten tietojärjestelmien käyttäminen henkilörekistereiden käsittelemistä varten yhdeksi ratkaisuksi. Jäsenrekisterissä sellainen onkin jo käytössä. Muiden henkilörekistereiden osalta tätä tarkoitusta varten Helluntaikirkon toimisto on ottanut opinnäytetyön edetessä käyttöön Microsoft Officen 365 -ympäristön, jonka avulla voidaan luoda jokaisen jäsenseurakunnan ja toimiston välille suljettu ympäristö henkilörekistereitä varten. Lisäksi tuetaan jäsenseurakuntien omien ympäristöjen perustamista. Tämä on ollut mahdollista Microsoftin Nonprofit -palvelupaketin kautta, jolloin seurakunta on voinut ottaa Officen 365 -ympäristön käyttöön maksutta.

Tietosuojavastaavan nimeämistä pidetään tärkeänä. Samoin jatkossa muutenkin kriittistä on saada jalkautettua koulutuksissa saatu tai muuten yhdessä pohdittu tietosuojaratkaisu Helluntaikirkon toimiston ja jäsenseurakuntien arkeen. Näihin tarvitaan yhdyskunnan johdon tukea ja tietosuojan pitämistä esillä yhteisillä foorumeilla.

Kehitysehdotuksena ehdotetaan vielä systemaattisempaa johdon sitoutumista tietosuojan kehittämisen prosessiin, dokumentaation tuottamista sekä koulutusten jatkamista. Lisäksi voisi kehittää uuden jäsenrekisteriohjelman ja mobiilisovelluksen, jossa on nykyaikaset käyttöliittymät viranomaisia, seurakuntien johtoa ja jäseniä varten siten, että samalla saadaan työkalut ja ratkaisu rekisteröityjen oikeuksien toteutumista varten ja varmistamiseksi.

Asiasanat: Tietosuoja-asetus, GDPR, Suomen Helluntaikirkko, seurakunta, tietosuojalaki

**Laurea University of Applied Sciences**
Degree Programme in Business economics
Bachelor of Business Administration

**Abstract**

Juha Koski

Views for the Finnish Pentecostal Denomination's General Data Protection Regulation

Year 2018 Pages 65

This thesis subject is the Finnish Pentecostal Denomination's General Data Protection Regulation. The new European Union data protection regulation will apply in the spring 2018 and will affect the Finnish Pentecostal Denomination. The purpose of the thesis was to be one of the denomination's documents for developing its data protection regulation. If willing, the denomination can later decide to use this thesis findings and recommendations.

The theory describes the data protection regulation from the denomination's point of view and it also introduced some IT-security solutions. Later, four persons from the denomination were interviewed to obtain ideas as to how to organize the denomination's data protection regulation development process in practice.

The result of the thesis was that it showed the need for training and documents. Even though the churches are different, at the same time there is a lot of similarities, whereby common documents would help to develop activities in the direction of the regulation. The denomination's office understands its responsibility for developing material, but the challenge is a lack of resources. Training has already been organized in co-operation with the denomination's IK institute. One of the goals of this training has been to support the local churches' own data regulation development process.

It was also found, that the closed IT-systems for handling the persons data is one solution. It is already in use for the membership registration. For the other persons registers the denomination has started to use Microsoft Office 365 environment, which can be used for building closed electronic environment for other registers. Also, local churches own the 365-environment development process and it is supported. This can be done by using Microsoft's Non-profit program, where churches can use Office 365 environment free of charge.

The appointment of the Data Protection Officer is considered important. A common solution is needed. In the future, it is critical to get the data protection solution that has been gained from the training or otherwise discussed together. After that the data protection can be implemented for the denomination. This will require the support of the leadership and use of shared media and forums.

Later it's suggested, that the leaders would commit to the data regulation development process, developing documents and training even more. New computer program and cell phone application with the interface for local registration office for membership registration could also be created. It could also deal with the members rights.

Keywords: Data Protection Regulation, GDPR, Finnish Pentecostal Denomination, Church

Sisällys

# 1 Johdanto

Opinnäytetyön tavoitteena on tehdä ehdotus huomioitavista asioista Suomen Helluntaikirkolle (jatkossa Helluntaikirkko) tietosuojakäytännön uudistamista varten. Taustalla on Euroopan Unionin vuonna 2016 tekemä tietosuoja-asetus (jatkossa tietosuoja-asetus), jota aletaan soveltaa Suomessa kahden vuoden siirtymäajan jälkeen keväällä 2018 (EU 2016/679). Globaalisti aihe tunnetaan nimellä GDPR, General Data Protection Regulation. Yleisellä tasolla voidaan todeta, että Suomessa henkilötietojen käsittely on jo nykyisellään hyvällä tasolla. Sairaaloissa ja muissa organisaatioissa kysytään tarvittaessa lupa henkilötietojen käsittelyyn sekä käytetään suljettuja suojattuja sähköisiä järjestelmiä koulutetun henkilökunnan toimesta. Samaan aikaan uusitun asetuksen myötä tilanne Suomessa on kaikille uusi. Viranomaisten ministeriöistä lähtien tulee itsekin pohtia ja ratkaista omissa organisaatioissaan tietosuojakysymyksiä samaan aikaan kun valmistelevat ohjeita muille. Siitä seuraa se, että yleisellä tasolla ei ole välttämättä vielä varmuutta siitä, kuinka joku yksittäinen tietosuojakysymys tulisi ratkaista. Varmasti esimerkiksi vuoden päästä kokonaisuus on selkeämpi, kun kaikilla on enemmän kokemusta asetuksen soveltamisesta. Tämä saattaa aiheuttaa tiettyä hämmennystä tällä hetkellä. Vastaavasti joku saattaa esiintyä asiantuntijana ja soveltaa jo nyt liikaa, vaikka asetusta aletaan virallisesti soveltaa vasta toukokuussa.

Helluntaikirkolla on useita jäsenseurakuntia ja niissä tuhansia jäseniä, joiden henkilötietoja yhdyskunnassa käsitellään. Tietosuoja-asetus tiukentaa ja tarkentaa tapaa, kuinka henkilötietoja käsitellään. Yksi esimerkki tästä on osoitusvelvollisuus. Aiemmin riitti, että noudatettiin lakia ja jos viranomainen tarkisti henkilötietojen käsittelyä, viranomaisen tehtävä oli osoittaa mahdollinen huolimattomuus tai lain rikkominen. Uuden asetuksen myötä rekisterinpitäjän vastuulla on osoittaa viranomaiselle, kuinka on varmistettu lainsäädännön noudattaminen. (Oikeusministeriö 2017, 14.)

Opinnäytetyö on toiminnallinen. Tavoitteiltaan ja lähtökohdiltaan se eroaa tutkimustyyppisestä opinnäytetyöstä siinä, että työssä esitettyjä väitteitä ei perustella tieteellisesti vaan ratkaistaan niiden toimivuuden perusteella. Valinta tutkimustyyppisen ja toiminnallisen opinnäytetyön välillä tehdään sen perusteella, mikä näkökulma sopii aiheeseen ja mahdollisesti opinnäytetyön tekijälle parhaiten. Toiminnallinen osuus arvioidaan suhteessa ammattialan osaamiseen, jossa yhdistyy taito, tieto sekä kokemuspohjainen ymmärrys, jota kutsutaan myös nimellä hiljainen tieto. Rakentavassa kokemuspohjaisessa ymmärtämisessä on kyse siitä, että osaa ottaa etäisyyttä esillä olevaan asiaan ja pohtia sen eri näkökulmia. Hiljaisen tiedon omaksuminen tapahtuu kokemuksen kautta siten, että on yhteydessä ammatti- tai asiantuntijayhteisöön tai tässä tapauksessa toimeksiantajan yhteisöön, Helluntaikirkkoon. Toiminnallisessa opinnäytetyössä tutkimuksellisuutta kohdistetaan sen toteutustapaan tai ideaan. (Pohjannoro&Taijala 2007, 6, 9, 12-15.) Opinnäytetyön toimeksiantona on ollut tehdä toimenpide-ehdotuksia Helluntaikirkolle tietosuojakäytäntöä varten. Konkreettisena tuotteena olisi voinut

olla valmis Helluntaikirkon tietosuojakäytäntö -dokumentti ja sen käyttöönotto seurakunnissa, mutta se olisi ollut aiheena liian laaja. Aihetta rajattiin siten, että tuotteena on valmistelevan tukimateriaalin ja ohjeistuksen tuottaminen, jota Helluntaikirkko voi halutessaan käyttää varsinaisen tietosuojakäytännön luomiseksi ja jalkauttamiseksi seurakuntiin. Seuraavissa kappaleissa on kuvattu henkilötietojen käsittelyn tietoperustaa. Myöhemmin on haastateltu neljää Helluntaikirkon edustajaa tietosuoja-asetuksesta. Tietoperustan ja haastatteluiden perusteella on luotu kappaleeseen kuusi Helluntaikirkolle ehdotus huomioitavista asioista tietosuojakäytäntöä varten. Ehdotus huomioi Helluntaikirkon toimiston sekä jäsenseurakuntien tarpeet.

# 2 Taustalla vaikuttava lainsäädäntö

## 2.1 Henkilötietolaki

Tähän saakka Suomen käytäntöjä on säädellyt henkilötietolaki, joka on suunnitelmien mukaan tietosuoja-asetuksen johdosta kokonaan kumoutumassa. Järjestelmänä on jatkossa tietosuoja-asetuksen soveltaminen suoraan sitovana säädöksenä. Sen lisäksi kansallisena lainsäädäntönä Suomeen on tulossa tietosuojalaki, joka tarkentaa tietosuoja-asetuksen soveltamista Suomessa. Tuleva tietosuojalaki kumoaa hallituksen esityksen mukaan henkilötietolain kokonaan ja ohjaa aihetta vain puiteluonteisesti ja eräissä yksityiskohdissa. Pääasiallinen säädöstö tulee suoraan tietosuoja-asetuksesta. Lain sisältö voi hallituksen esityksestä vielä eduskunnassa muuttua. Suomen lainsäädäntöä ollaan siis muokkaamassa tietosuoja-asetuksen mukaiseksi tietosuojalailla, joka soveltaa ja tarkentaa tietosuoja-asetusta (Oikeusministeriö 2018).

Muita Helluntaikirkon henkilötietojen käsittelyyn vaikuttavia lakeja ovat henkilötietolaki sekä laki uskontokuntien jäsenrekistereistä. Henkilötietojen käsittelyä ohjaa henkilötietolaki. Lain kolmannen luvun perusteella ihmisten arkaluontoisia tietoja ei lähtökohtaisesti saa käsitellä. Henkilön uskonnollinen vakaumus on arkaluontoinen tieto samoin kuin esimerkiksi rotu tai etninen alkuperä tai sairautta koskeva tieto. Vastaavasti esimerkiksi henkilötunnuksen käsittelyä ei lähtökohtaisesti kielletä, vaan sen käsittelyyn laki antaa luvan tietyin edellytyksin. Arkaluontoisia henkilötietoja saa poikkeuksellisesti käsitellä, jos henkilö on antanut erikseen siihen luvan, jos tieto on tarpeen oikeusvaateen laatimiseksi tai jos asiasta säädetään laissa tai joka johtuu välittömästi rekisterinpitäjälle laissa säädetystä tehtävästä. Uskonnollisilla yhdyskunnilla on rekisteripitovelvoite. Luvun kolme 12 § kohdassa seitsemän määritellään lisäksi, että uskontokuntaa edustavien yhdistystenkin jäsenistöstä voidaan pitää jäsenrekisteriä. Suurin osa Suomen helluntaiseurakunnista on yhdistyspohjaisia, vaikka ainakin osa näistä on liittymässä Helluntaikirkkoon. Esimerkiksi luterilainen kirkko Suomessa on kirkkokunta, mutta helluntailaiset ovat perustaneet paikallisia yhdistyksiä ja toimivat yhdistyslain alla. Vasta vuonna

2003 perustettiin uskonnollisena yhdyskuntana Helluntaikirkko, johon seurakunnat voivat halutessaan liittyä. Opinnäytetyö ei ota kantaa siihen, millä perusteella yhdistyspohjaiset seurakunnat keväällä 2018 voimaan astuvan lainsäädännön myötä pitävät henkilörekistereitään. (Henkilötietolaki 523/1999.) Henkilötietolain toisen luvun 10 § edellyttää rekisterinpitäjältä rekisteriselostetta ja määrittelee, mitä asioita selosteessa tulee olla merkittynä. Esimerkiksi Mäntsälän seurakunta rekisteriselosteessaan kuvaa, kuka rekisteristä vastaa ja miten henkilötietoja käsitellään (2013). Helluntaikirkolla on voimassa oleva rekisteriseloste (Suomen Helluntaikirkko 2017). Nykyään olisi mahdollista tehdä myös tietosuojaseloste, joka on muuten sama kuin rekisteriseloste, mutta siinä kuvataan rekisteröidyn oikeudet. Aiheesta lisää kappaleessa 6.4.

### 2.2 Laki uskontokuntien jäsenrekistereistä

Henkilötietolain luvussa kolme määriteltiin poikkeuslupana peruste uskonnollisten tietojen käsittelyyn, jos asiasta on säädetty laissa tai jos se johtuu rekisterinpitäjälle säädetystä tehtävästä. Laissa uskontokuntien jäsenrekistereistä määritellään, että kirkot ja uskonnolliset yhdyskunnat saavat pitää jäsenistöstään rekisteriä ja tallentaa rekisteriin uskontokunnan hallinnon kannalta tarpeelliset tiedot. Tämä jälkimmäinen laki toimii perusteena Helluntaikirkon henkilörekisterille. Laissa määritellään, mitä tietoja voidaan kerätä. Näitä tietoja ovat esimerkiksi tiedot kastamisesta, uskontokuntaan liittymisestä ja eroamisesta, osoitetiedot, jäsenen ja hänen puolisonsa henkilötunnus sekä alaikäisten lasten nimi ja henkilötunnus sekä tiedot mahdollisista luottamustehtävistä. Lain 3 § määritellään, että henkilötietojen käsittely tulee tehdä siten, miten muussa lainsäädännössä määritellään. Toisin sanoen kaikki tietoturvaan, luottamuksellisuuteen ja muuhun asialliseen tietojen käsittelyyn liittyvät asiat tulee huomioida. Näistä tarkemmin on säädetty henkilötietolain luvussa kaksi. (Laki uskontokuntien jäsenrekistereistä 614/1998).

## 3 Tietosuoja-asetus

### 3.1 Yleiset säännökset

EU:n tietosuoja-asetus on reilun sadan sivun ja 37 500:n sanan tekstikokonaisuus, joka ohjaa henkilötietojen käsittelyä. Kuten edellä on kerrottu, Suomen lakia ollaan muokkaamassa vastaamaan asetusta, joten nyt on jo tiedossa, millainen uusi laki tulee olemaan. Asetus kunnioittaa uskonnonvapautta ja SEUT-sopimuksen kohdan 17 mukaisesti käy vuoropuhelua uskonnollisten ja ei-uskonnollisten järjestöjen kanssa (Euroopan parlamentti 2017). Suomessa Oikeusministeriö tietosuojavaltuutetun kanssa on julkaissut tiiviin ohjeen tietosuoja-asetuksesta (2017). Seuraavassa on asetuksesta erityisesti niistä kohdista, jotka liittyvät Helluntaikirk-

koon. Tekstissä on pyritty valitsemaan organisaatiolle oleelliset kohdat asetuksesta ja kirjaamaan artiklan keskeinen sisältö. Kappaleessa kuusi on ehdotuksia Helluntaikirkon tietosuojakäytäntöön.

Tietosuoja-asetuksella suojellaan luonnollisten henkilöiden perusoikeuksia ja -vapauksia ja erityisesti heidän oikeuttaan henkilötietojen suojaan (1 artikla). Henkilöstä, joiden henkilötietoja käsitellään, käytetään nimitystä rekisteröity. Asetusta sovelletaan henkilötietojen käsittelyyn, jotka muodostavat rekisterin osan tai joiden on tarkoitus muodostaa rekisterin osa (4 artikla.) Henkilötiedoilla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan henkilöön liittyviä tietoja. Tunnistettavissa oleva henkilö on sellainen, joka voidaan suoraan tai epäsuorasti tunnistaa tunnistetiedoista. Näitä ovat nimi, henkilötunnus, sijainti, verkkotunniste tai yhden tai useamman henkilölle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella. Käsittelyllä tarkoitetaan toimia, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin. Näillä tietojoukoilla tarkoitetaan tietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista, hakua, kyselyä, käyttöä tai tietojen luovuttamista siirtämällä. Lisäksi käsittelyllä tarkoitetaan toimia, jossa henkilötietoja levitetään tai asetetaan muutoin saataville, yhteensovitetaan tai yhdistetään, rajoitetaan, poistetaan tai tuhotaan. (4 Artikla.)

Käsittelyn rajoittamisella tarkoitetaan tallennettujen henkilötietojen merkitsemistä siten, että tarkoituksena on rajoittaa niiden myöhempää käsittelyä. Profiloinnilla tarkoitetaan henkilötietojen automaattista käsittelyä, jossa henkilötietoja käyttämällä arvioidaan henkilön tiettyjä henkilökohtaisia ominaisuuksia. Tällöin erityisesti analysoidaan tai ennakoidaan piirteitä, jotka liittyvät henkilön työsuoritukseen, taloudelliseen tilanteeseen, terveyteen, henkilökohtaisiin mieltymyksiin, kiinnostuksen kohteisiin, luotettavuuteen, käyttäytymiseen, sijaintiin tai liikkeisiin. Pseudonymisoimisella tarkoitetaan henkilötietojen käsittelemistä siten, että henkilötietoja ei voida enää yhdistää tiettyyn henkilöön eli rekisteröityyn käyttämättä lisätietoja. Nämä lisätiedot tulee säilyttää erillään ja niihin tulee soveltaa teknisiä ja organisatorisia toimenpiteitä varmistaen, ettei henkilötietojen yhdistämistä tunnistettuun tai tunnistettavissa olevaan henkilöön tapahdu. (4 Artikla.) Profilointia voidaan käyttää esimerkiksi internetissä täytetyn lainahakemuksen käsittelyyn siten, että ohjelma automaattisesti kilpailuttaa useamman pankin ja tarjoaa vastauksen parissa minuutissa. Jotta tämä mahdollistuu, tarvitaan henkilötietojen profilointia. Pseydonymisointi tarkoittaa esimerkiksi tilastotarkoitusta varten tehtyä henkilön nimitietojen poistamista, jotta tilasto voidaan tehdä rekisteröidyn tietosuojaa vaarantamatta.

Rekisterillä tarkoitetaan mitä tahansa jäsenneltyä henkilötietoja sisältävää tietojoukkoa, josta tiedot ovat saatavilla tietyin perustein. Rekisterinpitäjällä tarkoitetaan luonnollista hen-

kilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Henkilötietojen käsittelijällä tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. (4 Artikla.)

### 3.2 Periaatteet

Henkilötietojen suhteen on noudatettava seuraavia vaatimuksia. Niitä on käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi. Ne on kerättävä tiettyä, nimenomaista ja laillista tarkoitusta varten, eikä niitä saa käsitellä myöhemmin näiden tarkoitusten kanssa yhteensopimattomalla tavalla. Myöhempää käsittelyä yleisen edun mukaisia arkistointitarkoituksia tai tilastollisia tarkoituksia varten ei katsota yhteensopimattomaksi alkuperäisten tarkoitusten kanssa. Tästä käytetään nimitystä käyttötarkoitussidonnaisuus. Henkilötietojen on oltava minimoituja. Niiden on toisin sanoen oltava asianmukaisia ja olennaisia ja rajoitettuja siihen, mikä on tarpeen suhteessa niihin tarkoituksiin, joita varten niitä käsitellään. Henkilötietojen tulee olla täsmällisiä ja tarvittaessa päivitettyjä ja rekisterinpitäjän on toteutettava kaikki mahdolliset kohtuulliset toimenpiteet sen varmistamiseksi, että käsittelyn tarkoituksiin nähden epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä. (5 Artikla.)

Henkilötietojen säilytystä tulee rajoittaa. Tämä tarkoittaa, että ne on säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten. Poikkeuksena tähän on yleisen edun mukainen arkistointitarkoitus tai tilastolliset tarkoitukset. Henkilötietoja on käsiteltävä eheästi ja luottamuksellisesti. Tämä tarkoittaa toimia, jolla varmistetaan henkilötietojen asianmukainen turvallisuus, mukaan lukien suojaaminen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta käyttäen asianmukaisia teknisiä tai organisatorisia toimia. (5 Artikla.)

Käsittely on lainmukaista ainoastaan kolmesta seuraavasta lähtökohdasta käsin. Henkilötietoja voidaan käsitellä, jos rekisteröity on antanut suostumuksensa käsittelyyn yhtä tai useampaa erityistä tarkoitusta varten. Niitä voidaan myös käsitellä, jos käsittely on tarpeen sellaisen sopimuksen täytäntöön panemiseksi, jossa rekisteröity on osapuolena, tai sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä. Kolmanneksi, jos käsittely on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi. (6 Artikla.) Helluntaikirkossa suostumus tarvitaan esimerkiksi seurakunnan järjestämän evankeliointikampanjan yhteydessä, mikäli seurakunta haluaa kerätä yhteystietoja osallistujilta jatkoyhteydenpitoa varten. Sopimukseen perustuva käsittely tulee kyseeseen esimerkiksi silloin, kun palkataan henkilö ja kirjoitetaan työsopimus. Tällöin työantaja voi käsitellä palkkaamansa henkilön henkilötietoja sopimuksen perusteella. Vastaavasti Helluntaikirkon jäsenrekisterin pitäminen on lakisääteinen tehtävä, joten jäsentietojen käsittelyyn ei tarvita erillistä lupaa.

Jos tietojenkäsittely perustuu suostumukseen, rekisterinpitäjän tulee pystyä osoittamaan, että rekisteröity on antanut suostumuksen henkilötietojensa käsittelyyn. Jos rekisteröity antaa suostumuksen kirjallisessa ilmoituksessa, joka koskee muitakin asioita, suostumuksen antamista koskeva pyyntö on esitettävä selkeästi erillään helposti ymmärrettävässä ja saatavilla olevassa muodossa yksinkertaisella ja selkeällä kielellä. Jos kirjallinen ilmoitus rikkoo tietosuoja-asetusta, ei se osa ilmoituksesta ole sitova. Rekisteröidyllä on oikeus peruuttaa suostumus milloin tahansa. Suostumuksen peruuttamisen tulee olla yhtä helppoa kuin sen antaminen. (7 Artikla.) Helluntaikirkossa tulee kiinnittää huomiota siihen, että rekisteröity on itse aktiivinen tietojen antamisessa. Lomakkeessa ei tule olla automaattisesti täytettynä lupakohtaa, vaan lupakohdan lomakkeessa tulee olla tyhjä siten, että rekisteröidyn itse tulee laittaa rasti ruutuun antaessaan luvan henkilötietojen käsittelyyn.

Jos palveluja tarjotaan suoraan lapselle sopimuksen perusteella, lapsen henkilötietojen käsittely on lainmukaista lapsen ollessa vähintään 16-vuotias. Jos lapsi on alle 16 vuotta, tällainen käsittely on lainmukaista vain siinä tapauksessa ja siltä osin kuin lapsen huoltaja on antanut siihen suostumuksen tai valtuutuksen. Suomi voi keväällä 2018 varsinaisessa lainsäädännössään säätää tätä tarkoitusta koskevasta alemmasta iästä, joka ei kuitenkaan saa olla alle 13 vuotta. (8 Artikla.) Suomi on ottamassa käyttöön 13 vuoden iän, eli Suomessa jatkossa 13 vuotias voi itse antaa luvan omien henkilötietojensa käsittelyyn (Oikeusministeriö 2018).

Sellaisten henkilötietojen käsittely, joista ilmenee rotu tai etninen alkuperä, poliittisia mielipiteitä, uskonnollinen tai filosofinen vakaumus tai ammattiliiton jäsenyys sekä geneettisten tai biometristen tietojen käsittely henkilön tunnistamista varten tai terveyttä koskevien tietojen tai henkilön seksuaalista käyttäytymistä ja suuntautumista koskevien tietojen käsittely on kiellettyä. Tätä ei sovelleta, jos sovelletaan jotain neljästä seuraavasta. (9 Artikla.)

Ensimmäiseksi, jos rekisteröity on antanut nimenomaisen suostumuksensa kyseisten henkilötietojen käsittelyyn. Toiseksi, jos käsittely suoritetaan poliittisen, filosofisen, uskonnollisen tai ammattiliittotoimintaan liittyvän säätiön, yhdistyksen tai muun voittoa tavoittelemattoman yhteisön laillisen toiminnan yhteydessä ja asianmukaisin suojatoimin, sillä edellytyksellä, että käsittely koskee ainoastaan näiden yhteisöjen jäseniä tai entisiä jäseniä tai henkilöitä, joilla on yhteisöihin säännölliset, yhteisöjen tarkoituksiin liittyvät yhteydet. Henkilötietoja ei saa luovuttaa yhteisön ulkopuolelle ilman rekisteröidyn suostumusta. Kolmanneksi, jos käsittely koskee henkilötietoja, jotka rekisteröity on saattanut julkisiksi. Neljänneksi, jos käsittely on tarpeen yleisen edun mukaisia arkistointitarkoituksia tai tilastollisia tarkoituksia varten 89 artiklan 1 kohdan mukaisesti. (9 Artikla.) Suurin osa Suomen helluntaiseurakunnista on yhdistyspohjaisia, jolloin niihin sovelletaan yhdistyslakia. Tietosuojan kannalta on huomioitava, että yhdistyslain 11 § mukaan jäsenillä on oikeus nähdä yhdistykseen kuuluvien jäsenten nimi

ja kotipaikka (1989/503). Vastaavasti tietosuoja-asetuksen mukaan tieto rekisteröidyn uskonnosta on salassa pidettävä ja sen jakaminen kiellettyä. Toivottavasti uusi tietosuojalaki tarkentaa uskonnollisten yhdistysten toimintaympäristöä.

Jos tarkoitukset, joihin rekisterinpitäjä käsittelee henkilötietoja, eivät edellytä tai eivät enää edellytä rekisterinpitäjän tunnistavan rekisteröidyn, rekisterinpitäjällä ei ole velvollisuutta säilyttää, hankkia tai käsitellä lisätietoja rekisteröidyn tunnistamista varten, jos tämä olisi tarpeen vain tietosuoja-asetuksen noudattamiseksi (11 Artikla).

## 3.3 Rekisteröidyn oikeudet

### 3.3.1 Oikeus saada läpinäkyvää informaatiota henkilötietojen käsittelystä

Rekisterinpitäjän on toteutettava asianmukaiset toimenpiteet toimittaakseen rekisteröidylle tietosuoja-asetuksen mukaiset kaikki käsittelyä koskevat tiedot tiiviisti esitetyssä, läpinäkyvässä, helposti ymmärrettävässä ja saatavilla olevassa muodossa selkeällä ja yksinkertaisella kielellä. Tämä tulee tehdä erityisen huolellisesti silloin, kun tiedot on tarkoitettu lapselle. Tiedot on toimitettava kirjallisesti tai muulla tavoin ja tapauksen mukaan sähköisessä muodossa. Jos rekisteröity pyytää, tiedot voidaan antaa suullisesti, kunhan ensin rekisteröidyn henkilöllisyys on vahvistettu muulla tavoin. (12 Artikla.)

### 3.3.2 Rekisteröidyn oikeus saada pääsy tietoihin

Kun henkilötietoja kerätään rekisteröidyltä, rekisterinpitäjän on samalla toimitettava rekisteröidylle kaikki seuraavat tiedot. Rekisterinpitäjän ja tapauksen mukaan tämän mahdollisen edustajan identiteetti ja yhteystiedot, mahdollisen tietosuojavastaavan yhteystiedot, henkilötietojen käsittelyn tarkoitukset sekä käsittelyn oikeusperuste sekä henkilötietojen vastaanottajat tai vastaanottajaryhmät. (13 Artikla.)

Näiden lisäksi rekisterinpitäjän on silloin, kun henkilötietoja saadaan, toimitettava rekisteröidylle seuraavat viisi lisätietoa, jotka ovat tarpeen asianmukaisen ja läpinäkyvän käsittelyn takaamiseksi. Ensimmäinen näistä on henkilötietojen säilytysaika tai jos se ei ole mahdollista säilytysajan määrittämiskriteerit. Toisena on tieto siitä, että rekisteröidyllä on oikeus pyytää rekisterinpitäjältä pääsy häntä itseään koskeviin henkilötietoihin sekä oikeus pyytää tietojen oikaisemista, poistamista, käsittelyn rajoittamista tai vastustaa käsittelyä sekä oikeutta siirtää tiedot järjestelmästä toiseen. Kolmantena kerrotaan, että rekisteröidyllä on oikeus peruuttaa suostumus milloin tahansa. Tämä ei vaikuta ennen peruuttamista tehdyn käsittelyn lainmukaisuuteen. Neljäntenä kerrotaan oikeudesta tehdä valitus valvontaviranomaiselle ja viidentenä tietojenkäsittelyn peruste. Tämä tarkoittaa tietoa siitä, onko henkilötietojen antaminen lakisääteinen tai sopimukseen perustuva vaatimus tai sopimuksen tekemisen edellyttämä vaatimus sekä onko rekisteröidyn pakko toimittaa henkilötiedot ja tällaisten tietojen

antamatta jättämisen mahdolliset seuraukset. Jos rekisterinpitäjä aikoo käsitellä henkilötietoja edelleen muuhun tarkoitukseen kuin siihen, johon tiedot aluksi kerättiin, rekisterinpitäjän tulee ilmoittaa rekisteröidylle ennen jatkokäsittelyä tästä muusta tarkoituksesta ja annettava asiaankuuluvat lisätiedot. (13 Artikla.)

Kun tietoja ei ole saatu rekisteröidyltä, rekisterinpitäjän on toimitettava rekisteröidylle seuraavat tiedot. Rekisterinpitäjän ja tämän mahdollisen edustajan identiteetti ja yhteystiedot, mahdollisen tietosuojavastaavan yhteystiedot, henkilötietojen käsittelyn tarkoitukset sekä käsittelyn oikeusperuste, kyseessä olevat henkilötietoryhmät, mahdolliset henkilötietojen vastaanottajat tai vastaanottajaryhmät sekä tarvittaessa tieto siitä, jos rekisterinpitäjä aikoo siirtää henkilötietoja kolmannessa maassa olevalle vastaanottajalle tai kansainväliselle järjestölle. Rekisterinpitäjän tulee toimittaa tiedot viimeistään kuukauden kuluessa henkilötietojen saamisesta ottaen huomioon tietojen käsittelyyn liittyvät erityiset olosuhteet. Jos henkilötietoja käytetään viestintään rekisteröidyn kanssa, tiedot tulee toimittaa viimeistään silloin kun rekisteröityyn ollaan yhteydessä ensimmäisen kerran tai jos henkilötietoja on tarkoitus luovuttaa toiselle vastaanottajalle, viimeistään silloin kun tietoja luovutetaan ensimmäisen kerran. (14 Artikla.)

Jos rekisterinpitäjä aikoo käsitellä henkilötietoja edelleen muuhun tarkoitukseen, rekisterinpitäjän on ilmoitettava rekisteröidylle ennen kyseistä jatkokäsittelyä tästä muusta tarkoituksesta ja annettava asiaankuuluvat lisätiedot. Edellä olevaa ei sovelleta, jos ja siltä osin kuin rekisteröity on jo saanut tiedot tai jos kyseisten tietojen toimittaminen osoittautuu mahdottomaksi tai vaatisi kohtuutonta vaivaa. Tämä saattaa tulla kyseeseen erityisesti käsittelyssä arkistointi- tai tilastollisia tarkoituksia varten ja kun se tehdään siten, että rekisterinpitäjä huolehtii asianmukaisista toimenpiteistä rekisteröidyn oikeuksien ja vapauksien sekä oikeutettujen etujen suojaamiseksi. (14 Artikla.)

Rekisteröidyllä on oikeus saada pääsy tietoihin. Tämä tarkoittaa, että rekisterinpitäjän tulee antaa vahvistus siitä, että rekisteröidyn henkilötietoja käsitellään tai ei käsitellä, ja jos niitä käsitellään, oikeus saada pääsy henkilötietoihin sekä seuraavat tiedot: Käsittelyn tarkoitukset, kyseessä olevat henkilötietoryhmät, vastaanottajat tai vastaanottajaryhmät, erityisesti kolmansissa maissa olevat vastaanottajat tai kansainväliset järjestöt, joille henkilötietoja on luovutettu tai on tarkoitus luovuttaa, mahdollisuuksien mukaan henkilötietojen suunniteltu säilytysaika tai jos se ei ole mahdollista, tämän ajan määrittämiskriteerit. Lisäksi rekisteröidyllä on oikeus saada vahvistus oikeudesta pyytää rekisterinpitäjältä häntä itseään koskevien henkilötietojen oikaisemista tai poistamista taikka henkilötietojen käsittelyn rajoittamista tai vastustaa tällaista käsittelyä sekä oikeus tehdä valitus valvontaviranomaiselle. Jos henkilötietoja ei kerätä rekisteröidyltä, kaikki tietojen alkuperästä käytettävissä olevat tiedot, automaattisen päätöksenteon, muun muassa profiloinnin olemassaolo ja tiedot käsitte-

lyyn liittyvästä logiikasta samoin kuin kyseisen käsittelyn merkittävyys ja mahdolliset seuraukset rekisteröidylle. Jos henkilötietoja siirretään kolmanteen maahan tai kansainväliselle järjestölle, rekisteröidyllä on oikeus saada ilmoitus tarkoitetuista siirtoa koskevista asianmukaisista suojatoimista. Rekisterinpitäjän on toimitettava jäljennös käsiteltävistä henkilötiedoista. Jos rekisteröity esittää pyynnön sähköisesti, tiedot on toimitettava yleisesti käytetyssä sähköisessä muodossa, paitsi jos rekisteröity toisin pyytää. Oikeus saada jäljennös ei saa vaikuttaa haitallisesti muiden oikeuksiin ja vapauksiin. (15 Artikla.)

### 3.3.3 Oikeus tietojen oikaisemiseen ja oikeus tulla unohdetuksi

Rekisteröidyllä on oikeus vaatia, että rekisterinpitäjä oikaisee ilman aiheetonta viivytystä rekisteröityä koskevat epätarkat ja virheelliset henkilötiedot (16 Artikla). Rekisteröidyllä on oikeus saada rekisterinpitäjä poistamaan rekisteröityä koskevat henkilötiedot ilman aiheetonta viivytystä (17 Artikla).

### 3.3.4 Oikeus käsittelyn rajoittamiseen ja rekisterinpitäjän velvollisuus ilmoittaa rajoituksesta

Rekisteröidyllä on oikeus käsittelyn rajoittamiseen, jos rekisteröity kiistää henkilötietojen paikkansapitävyyden, jolloin käsittelyä rajoitetaan tarkistamisen ajaksi tai käsittely on lainvastaista ja rekisteröity vastustaa henkilötietojen poistamista ja vaatii sen sijaan niiden käytön rajoittamista. Käsittelyä rajoitetaan myös, jos rekisterinpitäjä ei enää tarvitse kyseisiä henkilötietoja käsittelyn tarkoituksiin, mutta rekisteröity tarvitsee niitä oikeudellisen vaateen laatimiseksi. Lisäksi käsittelyä rajoitetaan, jos odotetaan sen todentamista syrjäyttävätkö rekisterinpitäjän oikeutetut perusteet rekisteröidyn perusteet. (18 Artikla.)

Jos käsittelyä on rajoitettu, henkilötietoja saa säilyttää, mutta muuten käsitellä ainoastaan rekisteröidyn suostumuksella tai oikeudellisen vaateen laatimiseksi, esittämiseksi tai puolustamiseksi. Lisäksi henkilötietoja voidaan käsitellä toisen henkilön tai oikeushenkilön oikeuksien suojaamiseksi tai tärkeää unionin tai jäsenvaltion yleistä etua koskevista syistä. Jos rekisteröity on saanut käsittelyn rajoitetuksi, rekisterinpitäjän on tehtävä rekisteröidylle ilmoitus, ennen kuin käsittelyä koskeva rajoitus poistetaan. (18 Artikla.) Rekisterinpitäjän on ilmoitettava henkilötietojen oikaisuista, poistoista tai käsittelyn rajoituksista jokaiselle vastaanottajalle, jolle henkilötietoja on luovutettu, paitsi jos tämä osoittautuu mahdottomaksi tai vaatii kohtuutonta vaivaa (19 Artikla). Rekisteröidyllä on automaattisessa käsittelyssä oikeus siirtää tiedot järjestelmästä toiseen, mutta Helluntaikirkolla ei ole käytössä tällaista automaattista käsittelyä (Liite 11).

### 3.3.5 Vastustamisoikeus

Rekisteröidyllä on oikeus henkilökohtaiseen erityiseen tilanteeseensa liittyvällä perusteella vastustaa häntä koskevien henkilötietojen käsittelyä, joka perustuu 6 artiklan 1 kohdan e tai f alakohtaan, kuten profilointiin. Rekisterinpitäjä ei saa enää käsitellä henkilötietoja, paitsi jos

rekisterinpitäjä voi osoittaa, että käsittelyyn on olemassa huomattavan tärkeä ja perusteltu syy, joka syrjäyttää rekisteröidyn edut, oikeudet ja vapaudet tai jos se on tarpeen oikeusvaateen laatimiseksi. Mikäli Helluntaikirkko tekisi suoramarkkinointia, siihen liittyvä vastustamisoikeus on kirjattu liitteeseen (Liite 11).

### 3.3.6 Automatisoidut yksittäispäätökset ja profilointi

Mikäli Helluntaikirkko tekisi automatisoituja yksittäispäätöksiä tai profilointia, asetuksenmukaisesta toimintatavasta on kerrottu tarkemmin liitteessä (Liite 11).

## 3.4 Rekisterinpitäjä ja henkilötietojen käsittelijä

Rekisterinpitäjän on toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet, jotta varmistetaan ja osoitetaan käsittelyn noudattavan tietosuoja-asetusta. Toimenpiteitä on tarkistettava ja päivitettävä tarvittaessa sisältäen myös asianmukaiset tietosuojaa koskevat toimintaperiaatteet. (24 Artikla.) Tietosuoja-asetuksessa on sisäänrakennettu ja oletusarvoinen tietosuoja. Se tarkoittaa, että ottaen huomioon uusimman tekniikan ja toteuttamiskustannukset sekä henkilötietojen käsittelyn luonteen, laajuuden, asiayhteyden ja tarkoitukset sekä riskit henkilöiden oikeuksille, rekisterinpitäjän on toteutettava tehokkaasti asianmukaiset tekniset ja organisatoriset toimenpiteet ja tarvittavat suojatoimet, jotta ne saataisiin sisällytettyä käsittelyn osaksi ja jotta käsittely vastaisi tietosuoja-asetuksen vaatimuksia. Rekisterinpitäjän on toteutettava asianmukaiset tekniset ja organisatoriset toimenpiteet, joilla varmistetaan, että oletusarvoisesti käsitellään vain käsittelyn kunkin erityisen tarkoituksen kannalta tarpeellisia henkilötietoja. Tämä velvollisuus koskee kerättyjen henkilötietojen määriä, käsittelyn laajuutta, säilytysaikaa ja saatavilla oloa. (25 Artikla.)

Rekisterinpitäjä saa käyttää vain sellaisia henkilötietojen käsittelijöitä, jotka toteuttavat riittävät suojatoimet asianmukaisten teknisten ja organisatoristen toimien täytäntöönpanemiseksi niin, että käsittely täyttää tietosuoja-asetuksen vaatimukset ja sillä varmistetaan rekisteröidyn oikeuksien suojelu. Henkilötietojen käsittelijä ei saa käyttää toisen henkilötietojen käsittelijän palveluksia ilman rekisterinpitäjän erityistä tai yleistä kirjallista ennakkolupaa. Kun kyse on kirjallisesta ennakkoluvasta, henkilötietojen käsittelijän tulee tiedottaa rekisterinpitäjää kaikista suunnitelluista muutoksista, jotka koskevat muiden henkilötietojen käsittelijöiden lisäämistä tai vaihtamista ja annettava rekisterinpitäjälle mahdollisuus vastustaa muutoksia. (28 Artikla.)

Henkilötietojen käsittelijän suorittamaa käsittelyä on määritettävä sopimuksella tai oikeudellisella asiakirjalla, jossa vahvistetaan käsittelyn kohde ja kesto, luonne ja tarkoitus, henkilötietojen tyyppi ja rekisteröityjen ryhmät, rekisterinpitäjän velvollisuudet ja oikeudet. Tässä sopimuksessa on säädettävä erityisesti seuraavista asioista. Henkilötietojen käsittelijä käsittelee henkilötietoja vain rekisterinpitäjän antamien dokumentoitujen ohjeiden mukaisesti ja

varmistaa, että henkilöt, joilla on oikeus käsitellä henkilötietoja, ovat sitoutuneet noudattamaan salassapitovelvollisuutta tai heitä koskee asianmukainen lakisääteinen salassapitovelvollisuus sekä toteuttaa käsittelyn turvallisesti artiklan 32 mukaan. Lisäksi tulee noudattaa toisen henkilötietojen käsittelijän käytön edellytyksiä. Edelleen tulee auttaa rekisterinpitäjää mahdollisuuksien mukaan vastaamaan pyyntöihin, jotka koskevat rekisteröidyn oikeuksien käyttämistä sekä auttaa rekisterinpitäjää varmistamaan, että henkilötietojen turvallisuuteen (32–36 artikla) säädettyjä velvollisuuksia noudatetaan ottaen huomioon käsittelyn luonne ja henkilötietojen käsittelijän saatavilla olevat tiedot. (28 Artikla.)

Henkilötietojen käsittelijän tulee myös rekisterinpitäjän valinnan mukaan poistaa tai palauttaa käsittelyyn liittyvien palveluiden tarjoamisen päätyttyä kaikki henkilötiedot rekisterinpitäjälle ja poistaa olemassa olevat jäljennökset, paitsi jos lainsäädännössä vaaditaan säilyttämään henkilötiedot. Vielä tulee saattaa rekisterinpitäjän saataville kaikki tiedot, jotka ovat tarpeen artiklan 28 velvollisuuksien noudattamisen osoittamista varten sekä sallia ja osallistua rekisterinpitäjän tai hänen valtuuttamansa auditoijan suorittamat auditoinnit ja tarkastukset. Henkilötietojen käsittelijän tulee ilmoittaa rekisterinpitäjälle, jos hän katsoo, että ohjeistus rikkoo tietosuoja-asetusta tai muita tietosuojasäännöksiä. (28 Artikla.)

Henkilötietojen käsittelijän tulee noudattaa rekisterinpitäjän ohjeita (29 Artikla). Rekisterinpitäjän tulee ylläpitää selostetta vastuullaan olevasta käsittelytoiminnasta (30 Artikla). Jos tapahtuu henkilötietojen tietoturvaloukkaus, rekisterinpitäjän tulee ilmoittaa siitä ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa sen ilmitulosta valvontaviranomaiselle, paitsi jos henkilötietojen tietoturvaloukkauksesta ei todennäköisesti aiheudu henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä. Jos ilmoitusta ei anneta 72 tunnin kuluessa, valvontaviranomaiselle on toimitettava perusteltu selitys. Henkilötietojen käsittelijän on ilmoitettava henkilötietojen tietoturvaloukkauksesta rekisterinpitäjälle ilman aiheetonta viivytystä saatuaan sen tietoonsa. Ilmoituksessa tulee vähintään kuvata tietoturvaloukkaus, mukaan lukien mahdollisuuksien mukaan asianomaisten rekisteröityjen ryhmät ja arvioidut lukumäärät sekä henkilötietotyyppien ryhmät ja arvioidut lukumäärät, ilmoitettava tietosuojavastaavan nimi ja yhteystiedot lisätietoja varten, kuvattava henkilötietojen tietoturvaloukkauksen todennäköiset seuraukset sekä kuvattava toimenpiteet, joita rekisterinpitäjä on ehdottanut tai jotka se on toteuttanut henkilötietojen tietoturvaloukkauksen johdosta, tarvittaessa myös toimenpiteet mahdollisten haittavaikutusten lieventämiseksi. (33 Artikla.)

Aihetta on kuvattu tarkemmin vielä liitteessä (Liite 12).

### 3.4.1 Tietosuojavastaava

Rekisterinpitäjän ja henkilötietojen käsittelijän tulee nimittää tietosuojavastaava aina kun heidän ydintehtävänsä muodostuvat luonteensa, laajuutensa ja/tai tarkoitustensa näkökulmasta laajamittaisesta rekisteröityjen säännöllisestä ja järjestelmällisestä seurannasta (37

Artikla). Rekisterinpitäjän ja henkilötietojen käsittelijän on varmistettava, että tietosuojavastaava otetaan asianmukaisesti ja ajoissa mukaan henkilötietojen suojaa koskevien kysymysten käsittelyyn. Heidän on tuettava tietosuojavastaavaa antamalla tälle tarvittavat resurssit, pääsyn henkilötietoihin ja käsittelytoimiin sekä hänen asiantuntemuksensa ylläpitämiseksi. Heidän on lisäksi varmistettava, ettei tietosuojavastaava ota vastaan ohjeita tehtäviensä hoitamisen yhteydessä. Rekisterinpitäjä tai henkilötietojen käsittelijä ei saa erottaa tai rangaista tietosuojavastaavaa tehtäviensä hoitamisesta. Tietosuojavastaava raportoi suoraan organisaation ylimmälle johdolle. Rekisteröidyt voivat ottaa yhteyttä tietosuojavastaavaan kaikissa asioissa, jotka liittyvät heidän henkilötietojensa käsittelyyn ja tietosuoja-asetuksessa määriteltyjen oikeuksiensa käyttöön. Tietosuojavastaavaa sitoo hänen tehtäviensä suorittamista koskeva salassapitovelvollisuus unionin oikeuden tai jäsenvaltion lainsäädännön mukaisesti. Tietosuojavastaava voi suorittaa muita tehtäviä, mutta rekisterinpitäjän tai henkilötietojen käsittelijän on varmistettava, että tällaiset tehtävät eivät aiheuta eturistiriitoja. (38 Artikla.)

Tietosuojavastaavan tehtäväkuva on seuraava. Hänen tulee antaa rekisterinpitäjälle tai henkilötietojen käsittelijälle sekä henkilötietoja käsitteleville työntekijöille tietoja ja neuvoja, jotka koskevat tietosuoja-asetuksen ja muiden unionin tai jäsenvaltioiden tietosuojasäännösten mukaisia velvollisuuksia. Hänen tulee seurata, että noudatetaan tietosuoja-asetusta ja muita tietosuojalainsäännöksiä sekä rekisterinpitäjän tai henkilötietojen käsittelijän henkilötietojen suojan toimintamenettelyjä sisältäen vastuunjaon, tiedon lisäämisen sekä käsittelyyn osallistuvan henkilöstön koulutuksen ja tähän liittyvät tarkastukset. Lisäksi tietosuojavastaavan tulee antaa pyydettäessä neuvoja tietosuojaa koskevasta vaikutustenarvioinnista ja valvoa sen toteutusta, tehdä yhteistyötä valvontaviranomaisen kanssa sekä toimia valvontaviranomaisen yhteyspisteenä käsittelyyn liittyvissä kysymyksissä, mukaan lukien 36 artiklan mukainen ennakkokuuleminen ja tarvittaessa kuuleminen muista mahdollisista kysymyksistä. (39 Artikla.)

Yhdistykset ja muut elimet, jotka edustavat rekisterinpitäjien tai henkilötietojen käsittelijöiden eri ryhmiä, voivat tietosuoja-asetuksen säännösten soveltamisen täsmentämiseksi laatia käytännesääntöjä, muuttaa tai laajentaa niitä, kunhan valvontaviranomainen on ensin antanut lausunnon, että ehdotettu luonnos on tietosuoja-asetuksen mukainen, rekisteröinyt ja julkaissut sen (40 Artikla).

### 3.5 Henkilötietojen siirrot kolmansiin maihin tai kansainvälisille järjestöille sekä valvontaviranomaiset

Mikäli Helluntaikirkko siirtää tai aikoisi siirtää henkilötietoja kolmansiin maihin, toimintaa ohjaava tietosuoja-asetuksen mukainen toiminta on kuvattu liitteessä. Samassa liitteessä on kuvattu Suomessa toimivien riippumattomien valvontaviranomaisten toiminta. (Liite 13.)

### 3.6 Oikeussuojakeinot, vastuu ja seuraamukset sekä erityistilanteet

Rekisteröidyllä on oikeus tehdä valitus valvontaviranomaiselle, jos hän katsoo, että häntä koskevien henkilötietojen käsittelyssä rikotaan tietosuoja-asetusta. Tämän ei tule kuitenkaan rajoittaa muita hallinnollisia muutoksenhakukeinoja tai oikeussuojakeinoja. Valvontaviranomaisen tulee ilmoittaa valituksen tekijälle valituksen etenemisestä ja ratkaisusta sekä oikeussuojakeinojen mahdollisuudesta. (77 Artikla.) Tietosuoja-asetuksen säännösten rikkomisesta voi seurata hallinnollinen sakko, joka on enintään 20 000 000 euroa, tai jos kyseessä on yritys, neljä prosenttia sen edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta sen mukaan, kumpi näistä määristä on suurempi (83 Artikla.)

Liitteessä on kerrottu vielä joitain erityistilanteita koskevia säädöksiä, kuten henkilötietojen käsittelystä journalistiseen tarkoitukseen (Liite 10).

### 3.7 Loppusäännökset

Tietosuoja-asetusta sovelletaan 25.5.2018 alkaen, se on kaikilta osiltaan velvoittava ja sitä sovelletaan sellaisenaan kaikissa jäsenvaltioissa (99 Artikla).

## 4 Tietoturva ja turvallisuuskäytännöt

Henkilötietoja käsitellään sähköisissä järjestelmissä, minkä johdosta niiden tietoturvan tulee olla ajan tasalla. IT-palveluntarjoajat ovat tuottaneet erilaisia ratkaisuja noudattaakseen tietosuoja-asetusta. Samalla he painottavat sitä, että viimekädessä vasta viranomainen asetusta soveltaessaan kesällä 2018 ottaa kantaa siihen, onko ratkaisu oikeasti viranomaisia tyydyttävä. Tämän vuoksi voi joskus olla hankala valita järjestelmätoimittaja, koska tarvitaan asiantuntemusta tietämään, millaiset toiminnot oikeasti tekevät järjestelmästä asetuksen mukaisen. Yksi kriittinen asia on se, että tietosuoja-asetuksen mukaan merkittävän tietoturvaloukkauksen tapahtuessa tulee kyetä 72 tunnin kuluessa raportoimaan siitä viranomaisille. Tähän tarvitaan ratkaisu, joka on yleensä kehittynyt palomuuri tai erillinen ohjelma, joka kykenee seuraamaan dataliikennettä ja tarvittaessa raportoimaan oman organisaation edustajaa automaattisesti (Töyrylä&Ylärakkola 2016, 11-12).

Mahdollisesti yksi eniten resursseja vaativista tehtävistä on henkilötietovarantojen kokoaminen. Henkilötietoja on vuosien varrella saatettu kerätä useaan paikkaan, eikä kukaan mahdollisesti muista, mitä tietoja on kerätty ja minne. Ne tulisi silti kerätä ja koota sekä määritellä, kuinka niitä jatkossa käsitellään esimerkiksi suljetussa sähköisessä järjestelmässä. Mikäli henkilötietovarannot ovat liian hajallaan ja kokoaminen ei ole mahdollista, ratkaisuna voi käyttää esimerkiksi Veritaksen Data Insight -työkalua, joka mahdollistaa tietojen suojaamisen ja käyttämisen hallitusti (2017).

Microsoftilta on löydettävissä tietosuojalauseke, joka kertoo mitä tietoja kerätään ja miten niitä käytetään (2018a). Sen lisäksi yhtiö kertoo, missä esimerkiksi Office 365:n palvelimet fyysisesti sijaitsevat (Microsoft 2018b). Suomalaisten tiedot säilytetään Euroopassa, jotta varmistetaan toimiminen tietosuoja-asetuksen mukaisesti. Yhtiö toimii globaalisti ja ymmärtää, että muiden maanosien ja maiden yritysten toimiessa Euroopassa tulee huomioida tietosuoja-asetus. Käytännössä tämä merkitsee sitä, että Eurooppa edellä tietosuoja-asetuksesta tulee globaali asia. Microsoft lähestyy Office 365 -ympäristössä tietosuoja-asetusta neljän toiminnon kautta. Näitä ovat itse tieto, pääsyn kontrolloiminen, suojaus sekä raportointi (Liite 1). Microsoft tarjoaa toimijalle ensimmäiseksi työkaluja erilaisten hakujen tekemiseen riippuen siitä, mikä on tarve. Seuraavaksi hallinnoidaan sitä, kuka pääsee tietoon käsiksi. Tähän kuuluu salasanojen hallinta, mutta tarvittaessa tunnistautumiseen voidaan lisätä biometrisiä tunnisteita, paikkaan (IP-ositteeseen) tai aikaan liittyviä rajoituksia tai esimerkiksi sääntöjä sähköpostien tai muun tiedon suodatukseen. Kolmantena tietoa voidaan salata tai muuten suojata eri tavoin sekä tarvittaessa varmuuskopioiden avulla palauttaa. Neljäntenä yhtiö tarjoaa erilaisia työkaluja lokitietojen ja muiden tietojen raportoimista varten. (Liite 1.) Lähestymistapana on vahva tunnistautuminen, jolloin voidaan luottaa siihen, että tiedetään, kuka kirjautuu (Liite 2). Sen jälkeen järjestelmiin jäävät lokitiedot mitä siellä on tehty, jolloin ne voidaan yhdistää henkilöön. Käyttöä voidaan myös rajoittaa tarpeen mukaan ja yhtiöllä on erilaisia järjestelmiä vastaamaan yhtiöiden erilaisia tarpeita (Liite 3).

F-Securen tietoturvaratkaisun nimi on Radar. Ajatuksena on hallita kriittisten alueiden haavoittuvuuksia. Järjestelmä paljastaa IT:n haavoittuvuudet ja tietoturvauhat skannaamalla. (F-Secure 2018b.) Järjestelmä raportoi haavoittuvuuksista ja tarjoaa työkalun, jolla voi huolehtia tietoturvasta. (F-Secure 2018c, 3.) Cisco:lla on myös ratkaisu tietosuoja-asetusta varten. Sen avulla voi hallita käyttöoikeuksia, tunnistaa uhkia ja muutenkin suojata järjestelmiä (2018). Kaikkien näiden avulla voidaan toteuttaa käytännössä tietojen suojaaminen ja esimerkiksi se, että 72 tunnin kuluessa voidaan tarvittaessa viranomaisille raportoida tietoturvaloukkauksista.

Henkilötietojen käsittelyn turvallisuutta voi lähestyä myös jakamalla turvallisuus tekniseen turvallisuuteen ja käsittelijävastuuseen. Teknistä turvallisuutta ovat käytännöt, järjestelmän virussuojaus, pääsyoikeusroolit, tietojen hävittämisen prosessi sekä tunnistautumistavat. Käytännöt tarkoittavat yksilöivien käyttäjätunnusten käyttämistä, harkittuja salasanavaatimuksia, palomuurisuojausta sekä kriittisten tilojen kameravalvontaa. Tietojen hävittäminen tarkoittaa sen prosessointia, kuinka vanhat tiedot hävitetään, sen suunnittelemista mihin henkilötietoihin hävitysprosessi liittyy, millä perusteella säilytysaika määrittyy, kuinka usein tiedot hävitetään ja miten tieto hävitetään. Käsittelyvastuuna ovat palvelukäytännöt, järjestelmälokit ja varmuuskopiointi. Palvelukäytännössä kuvataan tarkemmin alihankkijoiden toiminnan auditointi, auditointien mahdollistaminen ja niihin osallistuminen, avoin tiedotus käytännöistä ja niiden päivittymisestä, henkilöstön sitouttaminen salassapitovelvollisuuteen, häiriöistä ja

loukkauksista tiedottaminen sekä kuvataan henkilötietoja käsittelevän henkilöstön lakisääteinen salassapitovelvollisuus. (Tietosuojamalli 2018b.)

Helluntailiikkeen lähetysjärjestön Fida Internationalin tietohallintopäällikkö Aki Tervo on kouluttanut omaa organisaatiotaan tietoturvasta ja tietosuojasta opettamalla henkilöstöä arvioimaan riskejä (Liite 6). Voidaan pohtia, onko esimerkiksi uhka tietokoneen salasanojen menettämiseen vähäinen, kohtalainen vai vakava. Sen jälkeen pohditaan, onko uhkaan varauduttu. Varautuminen on voinut olla heikkoa, tyydyttävää tai kohtalaista. Tilanne on kuitenkin hallinnassa, jos uhka on arvion perusteella vähäinen ja siihen on varauduttu hyvin. Vastaavasti tulisi ryhtyä välittömiin toimiin, jos uhka on vakava ja siihen on varauduttu heikosti. Ideana on, että uhasta ja siihen varautumisesta annetaan numero ja ne kerrotaan keskenään. Jos uhka on vakava ja saa luvun kolme sekä varautuminen on heikkoa, jolloin sekin saa numeron kolme, kertolaskun tulos on yhdeksän. Mitä korkeampi luku, sitä kriittisempää on aloittaa välittömät toimet tilanteen parantamiseksi. (Tervo 2018.)

Tervo on tehnyt myös tietoturvakortin järjestelmien arvioimista varten (Liite 7). Kortin mukaan järjestelmälle annetaan pisteitä sen mukaan, kuinka erilaiset asiat ovat kunnossa. Pisteitä saa esimerkiksi, jos salasanan koordinointi on hallittua tai jos varmuuskopioinnin palautusta testataan säännöllisesti. Lisäksi järjestelmät kuvataan kolmella tasolla haavoittuviksi, sellaisiksi joissa on parannettavaa tai turvallisiksi. Jotta on mahdollista päästä tasolle parannettavaa, tulee ensin täyttää kaikki tason haavoittuva kriteerit. (Tervo 2018). Tällainen työkalu on tietoturvaan perehtymättömällekin havainnollista, jotta ymmärtää mihin tulee kiinnittää huomiota.

# 5 Haastattelut

## 5.1 Haastateltavien valinta

Opinnäytetyötä varten haastateltiin yhteensä neljää henkilöä Helluntaikirkon toimistosta sekä jäsenseurakunnista. Haastateltavat valittiin siten, että huomioitiin Helluntaikirkon johdon ja yhdyskunnan hallituksen näkökulma. Sen lisäksi valittiin edustaja isommasta ja pienemmästä seurakunnasta. Samalla valittiin haastateltavaksi pastori tai muu palkattu henkilö sekä vapaaehtoisena seurakunnan hallinnossa toimiva henkilö. Näillä valinnoilla tavoiteltiin mahdollisimman monipuolista näkökulmaa, kokemusta ja johdannossa esiteltyä hiljaisen tiedon osaamista Helluntaikirkon tietosuojakysymyksistä. Tavoitteena oli löytää käytännön ratkaisuja Helluntaikirkolle tietosuojakäytännön luomista varten. Haastattelukysymykset ovat liitteenä (Liite 4). Haastattelu aloitettiin esittämällä tietosuojavaltuutetun arvio siitä, että organisaation tietosuojan heikoin lenkki on sen johto ja pyytämällä kommentoimaan arviota (Aarnio 2017).

## 5.2 Helluntaikirkon toiminnanjohtaja Esko Matikainen

Helluntaikirkon toiminnanjohtaja Esko Matikaisen mukaan tietosuojan heikoimmassa lenkissä Helluntaikirkossa on eri osa-alueita. Henkilötietojen käsittely toimistossa tehdään jo nyt hyvin. Henkilötietoihin pääsee käsiksi vain toiminnanjohtaja ja toimiston työntekijä. Paperit ovat lukitussa kaapissa ja avainten käyttöä valvotaan. Pilvipalveluiden osalta saattaa haasteena olla tietyn pilvipalvelun käyttäminen, kuten esimerkiksi Google drive:n käyttäminen. Salasanojen käyttö on hyvällä mallilla. Haasteena voi olla sähköpostilla asiakirjojen lähettäminen; jatkossa on tarpeen selvittää, tarvitaanko suojattua sähköpostia tai muuta ratkaisua varmistamaan hyvä tietosuoja. Henkilötietoja käsittelevien henkilöiden henkilötietojen käsittely saattaa vaihdella; toiset ovat huolellisempia kuin toiset. (Matikainen 2018).

Matikaisen mukaan Helluntaikirkon tietosuojakäytännössä tulisi olla ainakin mahdollisuus suojatun ympäristön käyttämiseen siten, että toimittaisiin toimistossa ja seurakunnissa samassa ympäristössä. Sähköpostiliikenne toimiston ja hallinnon välillä tulisi voida salata tarvittaessa. Henkilötietojärjestelmä on nykyisen lain mukainen ja nyt se tulee vielä tarkistaa, jotta varmistetaan sen vastaavan myös uutta tietosuoja-asetusta. Omilla tietokoneilla ei tule säilyttää henkilörekistereitä, vaan käsitellä niitä ainoastaan suljetussa ympäristössä. Kassakaappi tulisi hankkia toimistoon. Salasanojen hallintaan voi käyttää esimerkiksi F-Securen Key-sovellusta (2018). Tietosuojakäytännössä tulisi olla kirjalliset ohjeet ja käytänteet. (Matikainen 2018).

Jotta oletusarvoinen tietosuoja voisi toteutua, toimistossa asiakirjojen käsittely ja viestien välittäminen tulisi tehdä vielä paremmin. Vaikka nyt jo ollaan tarkkoja henkilötietojen käsittelyssä, tietosuojan huomioiminen kaikissa asioissa sen kaikissa vaiheissa vaatii vielä työtä. Jäsenseurakunnille tulisi jakaa informaatiota, jotta seurakunnat voisivat helposti hahmottaa asetuksen ja tarjota heille samalla ratkaisua. Hallituksen ja työryhmien työskentelyssä käytänteet henkilötietojen käsittelyssä vaihtelevat. Jokainen arvioi itse onko hallituksen tai työryhmän asia salassa pidettävä. Paperitulosteita käytetään vaihtelevasti eikä aina välttämättä pohdita, tarvitaanko tulostetta oikeasti eikä sen jälkeen ole tietoa, mitä papereille tapahtuu. (Matikainen 2018).

Riskiperusteinen lähestymistapa toteutuu Helluntaikirkossa silloin, kun asioihin suhtaudutaan sopivalla tavalla ”epäluuloisesti”. Tällä Matikainen tarkoittaa tarkkuutta kaikenlaisessa henkilötietojen käsittelyssä ja sen ottamista huomioon, että joku voi tulla esimerkiksi toimistoon kysymään tai hakemaan henkilötietoja, jotka eivät henkilölle kuulu. Seurakunnille tulee antaa tietoa riskien arvioimisesta, jotta ne voivat omaksua riskiperustaisen lähestymistavan tietosuojaan. Osoitusvelvollisuus toteutuu silloin parhaiten, kun valitsee yhteistyökumppaneita, jotka pystyvät toimittamaan tarvittavat dokumentit osoitusvelvollisuutta varten. Tähänkin tarvitaan kirjallisia ohjeita, eli että mitä asioita osoitusvelvollisuuden toteutumiseksi dokumenteilla tulee kyetä osoittamaan. (Matikainen 2018).

Rekisteröityjen oikeuksien toteuttamista varten järjestelmätoimittajan kanssa tulee neuvotella ja varmistua, että oikeudet pystytään toteuttamaan. Tähän voi ratkaisuna olla esimerkiksi mobiilisovellus, jonka kautta suojatusti näkee omia tietoja. Lisäksi tulee pitää huolta, että vain tarpeellinen tieto kerätään. Väestörekisterikeskuksen tietoja käyttämällä voidaan varmistua oikeista henkilötiedoista ja siltä osin varmistua rekisteröidyn oikeuden toteutumisesta. Matikainen pitää tärkeänä tietosuojavastaavan nimeämistä Helluntaikirkolle. Palvelun voisi hankkia esimerkiksi ostopalveluna kumppanilta. (Matikainen 2018).

Henkilötietojen asianmukainen käsittely on jäsenseurakunnan johdon eli vanhimmiston vastuulla. Helluntaikirkon tulee luoda järjestelmä tai ympäristö, jossa käyttöoikeuksin jakaminen on hallittua. Ympäristön luominen on Helluntaikirkon toimiston vastuulla. Sen jälkeen valitaan henkilöt, jotka voivat jakaa oikeuksia. Näitä voivat olla esimerkiksi seurakunnan nimenkirjoittaja, joka kirjautuu pankkitunnuksien avulla järjestelmään ja siellä jakaa tunnuksia. Järjestelmän tulee pakottaa huolellisuuteen. Jotta hyvä henkilötietojen tietosuoja voisi toteutua, järjestelmän tulee olla sellainen, joka täyttää kriteerit. Sen jälkeen yhdyskunnan kokous keskustelee ja sen tulee päättää asioista ja käytänteistä ja sitouttaa oma organisaatio niihin. Helluntaikirkon toimisto toteuttaa yhdyskunnan kokouksen päätöstä. Henkilötietojen käsittelijöitä tulee kouluttaa ja dokumentointia tarvitaan lisää. Vanhimmiston tai vastaavan hallituksen puheenjohtajalla on virallinen vastuu seurakunnasta ja tietosuoja-asetuksen noudattamisesta. Helluntaikirkon toimiston tehtävänä on muistuttaa vastuusta ja antaa sen lisäksi työkaluja. Haasteena on resurssien saaminen, koska toimistossa tarvitaan palkkarahaa tietosuoja-asetuksesta seuraavien vastuiden hoitamiseksi. Samaan aikaan puhutaan valtakunnallisesta kirkosta, jolloin tietosuoja-asiat tulee hoitaa hyvin. (Matikainen 2018).

### 5.3 Helluntaikirkon hallituksen puheenjohtaja ja Helsingin Saalem-seurakunnan johtaja Mika Yrjölä

Suomen suurimman helluntaiseurakunnan Helsingin Saalemin johtava pastori sekä Helluntaikirkon hallituksen puheenjohtaja Mika Yrjölä pitää tietosuojakäytännön luomista tärkeänä. Yrjölän mukaan Aarnion arvio Helluntaikirkon jäsenseurakunnissa osuu oikeaan vaihtelevasti. Monissa paikoissa johto voi olla heikoin lenkki, mutta ei aina. On ollut tietämättömyyttä ja sen johdosta toimeenpanossa puutteita. Helsingin Saalem-seurakunnassa tietosuojaan on herätty ja tehty toimenpiteitä. Samoin Helluntaikirkon toimistossa tietosuojaan liittyvä prosessi on hyvässä vauhdissa. Yksi esimerkki tästä on tämä opinnäytetyö. Sen lisäksi koulutusta seurakunnille on järjestetty ja tullaan järjestämään. IT-laitteiden turvallisuus on jo tähänkin asti ollut hyvä. (Yrjölä 2018).

Yrjölän mukaan Helluntaikirkon tietosuojakäytännössä tulisi olla ainakin kaikki se, mitä laki vaatii. Rekisteriselosteiden tulee olla kunnossa sekä tarkentaa kenellä on pääsy tietoihin ja muutenkin tulee olla olemassa selkeät käytännöt ja ohjeet. Vaikka IT-laitteiden turvallisuus

on hyvä, tarvitaan laitteiden käyttöön perehdyttämistä. Talousohjelmissa ja esimerkiksi luottokorttien käytössä tulee olla selkeät kirjalliset ohjeet ja käytänteet. Helluntaikirkko järjestää aiheesta koulutusta, valmistaa kirjallista materiaalia sekä luo rekisteriselosteen pohjamallin jäsenseurakuntia varten. Tietosuojakäytännössä Yrjölälle on tärkeää se, mitä tietoja kerätään ja miksi sekä miten niitä käytetään. (Yrjölä 2018.)

Oletusarvoinen tietosuoja toteutuu Yrjölän mukaan konkretisoimalla tarpeeksi, kuten sanomalla: ”Jos käsittelet yhtä listaa tai yhtä nimeä, tietosuoja koskee sinua”. Riskiperusteinen lähestymistapa saavutetaan luomalla käyttöoppaita tai esimerkiksi lyhyitä videoklippejä siitä, kuinka tietosuojan toteutumisen riskejä voisi käytännössä arvioida. Haasteena on kiinnostuksen herättäminen, jotta toiminnassa hyvä henkilötietojen tietosuoja voisi olla oletusarvoisesti ja läpileikkaavasti mukana ja jotta toiminnassa arvioitaisiin tietosuojan riskejä. Ratkaisuna Yrjölä pitää viestin tiivistämistä oleellisena. Esitystapa on tärkeä, jotta kiinnostutaan. Lasten tietosuojan toteutuminen tulee huomioida. Leiritoiminnassa tulee olla suostumus esimerkiksi siitä, millaista lääkettä voidaan antaa tai voidaanko ottaa valokuvia. Samaan aikaan tiedostetaan se, että nuoret itse ottavat kuvia ja jakavat niitä. Toisaalta nuoret tietävät pelisäännöt toisinaan jopa paremmin kuin aikuiset. Helluntaikirkon toimiston tulee auttaa laatimaan dokumentaatiota, jotta osoitusvelvollisuus voisi toteutua. Sen lisäksi jokaisella jäsenseurakunnalla on myös vastuu dokumentaation tuottamisesta osoitusvelvollisuuden toteuttamiseksi. (Yrjölä 2018.)

Kaikilla seurakunnilla tulee olla tiedossa rekisteröityjen oikeudet sekä varautua niihin. Jos seurakunnan toimistossa rekisteröidyn pyynnöstä on esimerkiksi mahdollisuus muuttaa rekisteröidyn tietoja tai kieltää tietojen käsittely, Yrjölä pohtii, tuleeko muutos käytännössä huomioitua kaikissa kyseisissä henkilörekistereissä. Seurakunnilla tulee olla selvillä, miten asetus heitä velvoittaa. Yhtenä ratkaisuvaihtoehtona Yrjölän mukaan voisi olla sopiva paikallinen vakuutus asian hoitamisesta. Jotta varmistetaan seurakuntien henkilötietoja käsittelevien henkilöiden asetuksenmukainen työskentely, pitäisi ainakin aluksi olla olemassa tapa, jolla saadaan tieto seurakunnasta, kuka hoitaa asiaa. Helluntaikirkon hallituksen roolina on sopia asiasta. Helluntaikirkossa tulisi olla Yrjölän mukaan tietosuojavastaava. Sen lisäksi tietosuoja tulisi nostaa yhteisille päättäjien päiville. Lisäksi seurakuntia tulisi informoida suullisesti ja kirjallisesti sekä tiedottaa liikkeen yhteisessä Ristin Voitto -lehdessä. (Yrjölä 2018.)

### 5.4 Seurakunnan pastori Helena Korhonen

Lappeenrannan Helluntaiseurakunnan pastorin Helena Korhosen mukaan yleisesti Aarnion edellä esitetty väite pitää hyvinkin paikkaansa. Sekä hän että seurakunta ovat orientoituneet ja johtotiimissä on tietosuojaan perehtynyt ylilääkäri. Haasteena voi olla johtoryhmän tietosuojaosaaminen kokonaisuudessaan siten, että tiimin jokaisella jäsenellä olisi kattava käsitys tietosuojasta. Helluntaikirkon tietosuojakäytännössä tulisi ainakin olla kuvaus jäsenrekisterin

ylläpidosta ja sen tulee olla lainmukainen. On luotava käytännöt ja valittava luotettavat henkilöt käsittelemään henkilörekistereitä sekä valita asetuksen mukainen ulkopuolinen palvelun tuottaja. Henkilöiden oikeudessa saada tietoja läpinäkyvästi on ollut aiemmin ontuvuutta, mutta jatkossa sen pitää olla läpinäkyvää. Korhosen mukaan tulee ymmärtää rekisterejä olevan useita ja että jokaisen käyttötarkoitus tulee olla suunniteltu ja huolellisesti ohjeistettu asetuksen käyttötarkoitussidonnaisuusperiaatteen toteutumiseksi. Korhonen pitää tärkeänä kaikkea päivittäisessä toiminnassa olevia asioita. Diakoniatyössä tulee esille esimerkiksi henkilön sosiaalinen asema, jolloin toimijoiden tulee saada ohjeistus, kuinka heidän henkilötietojaan käsitellään. Samoin lasten ja nuorten työssä ohjaajat käsittelevät monia asioita ja tämä on iso haaste, koska on paljon eri toimijoita, joista osa on itsekin nuoria. Silti tulisi olla yhteiset käytänteet. Haasteena ovat sosiaalisen median rekisterit ja lisäksi tulisi olla päätökset siitä, mitä yhteisiä asioita on ja kuka niistä vastaa. Tärkeää on, ettei tietoja luovuteta ulkopuolelle. (Korhonen 2018.)

Oletusarvoisen tietosuojan osalta on selkeästi parantamisen varaa. Tietosuoja toimii hyvin palkatuiden henkilöiden ja johdon kohdalla, mutta yksittäiset vapaaehtoiset eivät ehkä miellä tätä. Jos ulkopuolelta soitetaan, joku saattaisi antaa henkilötietoja. Tähän liittyvät koulutukset ovat menossa seurakunnassa. Riskiperusteisen lähestymistavan vuoksi tietosuojan riskiarviot tulee uusia tietyin väliajoin. Kun tietokone jää pois työntekijän aktiivikäytöstä, se saatetaan siirtää palvelemaan jonkun ryhmän toimintaa, esimerkiksi kerhon musiikintoistovälineenä. Korhonen kysyy, kuka tyhjentää koneen? Salasanat tulee uusia tietyin väliajoin. Avoimet koneet ovat tietosuojan kannalta hankalia, varsinkin jos niillä pääsee internettiin. IT-asiat ovat riskialttiimpia tietosuojan kannalta. Riskien hallinta on haastavaa ja siinä vaaditaan asennekasvatusta. Suurin riski on, että henkilöt toimivat väärin. Osoitusvelvollisuuden parantamiseksi tällä hetkellä seurakunnassa ollaan luomassa systemaattisesti käytänteet eri osa-alueisiin. Näistä Korhonen mainitsee lokitiedot asioista, mitkä on opastettu. Lisäksi vaitiolosopimukset on allekirjoitettu, jossa henkilötietojen käsittelijä vakuuttaa saaneensa tiedon ja ohjeistuksen tietosuoja-asioista sekä sitoutuvansa niihin. Seurakunnan toiminnassa kertyy tietoa, joka ei vanhene. Tulee olla käytänteet ja kirjallinen ohjeistus ja dokumentaatio, kuinka arkistoja säilytetään ja kuinka niihin pääsee käsiksi. Alaikäisten kohdalla aiemmin on riittänyt, että vanhemmalta on saatu suullisesti asianmukaiset luvat. Tämä ei riitä enää, vaan tulee luoda käytäntö kirjallisesta luvan pyytämisestä, jotta se voidaan tarvittaessa osoittaa todeksi. (Korhonen 2018.)

Rekisteröityjen oikeuksien toteutumiseksi tietojen tulee olla suojattuna siten, etteivät ne joudu ulkopuolisen käsiin. Kun rekisteröity kysyy tietoja, seurakunnan tulee olla tietoinen henkilön tiedoista ja rekisteriselosteessa tulee näkyä rekisteröidyn oikeus omiin tietoihinsa. Lappeenrannan Helluntaiseurakunnassa on jo nimetty tietosuojavastaava ja Korhosen mukaan sellainen tulisi olla valtakunnallisestikin. Jotta seurakuntien henkilötietoja käsittelevät henkilöt tekisivät työnsä tietosuoja-asetuksen mukaisesti, Korhosen mukaan tietosuojavastaavan

tulisi olla mukana nimeämisessä ja senkin vuoksi vastaavan nimeäminen on tärkeää. Henkilötietojen käsittelijät nimeää pastori tai tietosuojavastaava. Lisäksi manuaaliset henkilötiedot tulee olla lukitussa tilassa ja avaimet vain henkilöillä, jotka tehtävään on nimetty. Jotta Helluntaikirkossa valtakunnallisesti aidosti toteutuisi hyvä henkilötietojen tietosuoja, tarvitaan koulutusta. IK-opiston koulutus on hyvä (2018). Joka seurakunnasta kahden tai kolmen henkilön tulisi käydä koulutus, jotta henkilötietojen tietosuojaan liittyvä kokonaisuus opittaisiin. Tietosuojasta tulisi tulla sellainen ajattelutapa, että opitaan näkemään, mikä kuuluu tietosuojaan. Tietosuoja ei ole mörkö, vaan hyvä asia ja ihmisten turvaksi. Kun nähdään näin, asennoidutaan paremmin. Nyt pitää havahtua siihen, että sähköposti on väärä väline henkilötietojen lähettämiseen. Tähän on totuttu, mutta se ei enää sovellu kaikkeen.

### 5.5 Seurakunnan edustaja Esa Juuti

Joensuun Helluntaiseurakunnan johdon edustajanan Esa Juutin mukaan tietosuojan heikoin lenkki voi olla yksittäiset toimijat, jotka eivät huolehdi tietosuojasta joidenkin pienempien henkilörekistereiden osalta. Toisaalta samaan aikaan suljetussa järjestelmässä oleva sähköinen iso jäsenrekisteri on suojattu ja henkilötietoja käsittelevät ainoastaan tehtävään nimetyt henkilöt. Koska isoimpana henkilörekisterinä oleva jäsenrekisteri on suojattu, tietovuotoja tai tietoturvaloukkauksia ei pääse helposti tapahtumaan. Muiden pienempien henkilörekistereiden osalta voi olla haasteellisempaa, koska kaikki toimijat eivät välttämättä ole mieltäneet salassapidon tärkeyttä. IT-järjestelmien suojauksen osalta Juuti kertoi huomanneensa jokin aika sitten haavoittuvuuden, mutta tämä korjattiin välittömästi. Kun henkilötietoja käsitellään sähköisessä ympäristössä, suojaamisen tulee olla kunnossa. Läpinäkyvyys on tärkeää, jotta tiedetään, kuka käsittelee tietoja. Helluntaikirkon tuki jäsenseurakunnille on tärkeää, jotta saadaan hyviä käytäntöjä ja dokumenttipohjia hyvän tietosuojan toteuttamista varten. Helluntaiseurakunnissa on henkilörekistereissä Helluntaikirkon jäsenten lisäksi myös muita ihmisiä, kuten mahdollisen seurakuntayhdistyksen jäseniä. Näistä henkilörekistereistä tulee myös huolehtia. Ruohonjuuritason toiminnassa tulee ensin keskittyä isoimpiin henkilörekistereihin ja sen jälkeen kehittää pienempien asioiden tietosuojaratkaisua. (Juuti 2018.)

Oletusarvoisen tietosuojan toteuttamiseen ei vielä pystytä. Helluntaikirkon toimisto voisi antaa vinkkejä tilanteista, milloin tietosuoja voi vaarantua, jotta ne tulisi huomioitua. Riskiperusteisesta lähestymistavasta Juuti mainitsee seurakunnan oman toimiston. Toimisto on tuulinen avokonttori, jossa ihmisiä tulee ja menee. On aika vähän tilaa toimia. Ratkaisuna seurakunta on järjestellyt tiloja ja siirtänyt esimerkiksi sielunhoidollisten keskustelujen paikan toisaalle. Seurakunnan toimistossa käy muitakin vieraita, minkä johdosta on muutettu paperisten arkistojen säilytyspaikkaa erillislukittuun tilaan. Tilan lukko vaihdetaan, jotta varmistutaan, kenellä on avain ja jotta avainhallinta on jatkossa koordinoitua. Sähköistä järjestelmää ollaan uusimassa Officen 365 -ympäristöön. Prosessin aikana uusitaan salasanat ja jaetaan so-

pivat käyttöoikeudet, jotta voidaan toimia suljetussa ympäristössä. Osoitusvelvollisuuden toteuttamiseksi tulee ainakin koota sirpaloituja henkilörekistereitä ja hävittää vanhoja pois. Tulee luoda systeemi, jossa on hallittu ympäristö. Henkilörekisterit tulee koota ja lisätä ohjeita, kuinka niitä käytetään. Rekisteröityjen oikeudet jäsenrekisterin osalta on helpompi toteuttaa, koska tiedot ovat jo nyt suljetussa järjestelmässä. Leiritietojen ja muiden pienrekistereiden osalta tilanne paranee, kun saadaan koottua tiedot sähköiseen ympäristöön. Henkilörekisterin aukaiseminen ja arkistojen ylläpitäminen tulee jopa luonnostaan hallitummaksi. Haasteena on saada henkilötietojen käsittelijät luopumaan papereista ja saada heidät käsittelemään tietoja ainoastaan sähköisessä ympäristössä. Jäsenrekisteriohjelmaan tulee tieto seurakuntaan liittymisestä. Lisäksi jo nyt noudatetaan lapsi- ja nuorisotyön ohjeistusta, joten näiden avulla voidaan toteuttaa rekisteröityjen oikeuksiakin. Luultavasti tämä vaatii vähän tarkennusta, mutta hyvä pohjakäytäntö on jo nyt olemassa. (Juuti 2018.)

Helluntaikirkossa valtakunnallisesti sekä Joensuun Helluntaiseurakunnassa tulisi olla tietosuojavastaava. Henkilötietoja käsittelevät tällä hetkellä erikseen nimetyt henkilöt, jotka pääsevät tekemään henkilötietomuutoksia järjestelmään. Jatkossa käsittelyä voisi terävöittää pyytämällä nimen vaitiolositoumukseen. Tulisi luoda muidenkin henkilörekistereiden osalta suljettu ympäristö missä niitä käsitellään ja kouluttaa henkilöt käyttämään ympäristöä. Jotta seurakunnassa voisi aidosti toteutua hyvä henkilötietojen tietosuoja, tulisi ainakin koulutuksen kautta saada aikaan asennemuutos tai asenteen terävöittäminen siten, että hyvän tietosuojan toteutumista pidettäisiin tärkeänä. Sen lisäksi sähköisen ympäristön tulee olla suojattu ja henkilökunnan tulee oppia havaitsemaan vaaroja. Tällä hetkellä ollaan tekemässä kartoitusta, mitä sosiaalisen median sivuja seurakunnan toiminnassa käytetään. Muutenkin tulee siirtyä käyttämään keskitettyjä sähköisiä ympäristöjä, joita voi päivittää, koska paperit ovat hankalampia tietosuojan kannalta. Samaan aikaan sähköisessä ympäristössäkin on toki riskinsä, mutta ne ovat paremmin hallittavissa. Tietosuojassa kaiken kaikkiaan on vielä paljon opittavaa. Kaikki tuki Helluntaikirkon toimiston puolelta on tervetullutta. Olematta IT-spesialisti tai järjestöjyrä, tarvitaan apua, jotta voisi nähdä tietosuojan punaisen langan jota seurata. Tämän toteutumiseksi pienet vinkit eivät olisi pahitteeksi. Muuten voi käydä niin, että esimerkiksi nuorisotyön puolella tietosuoja koetaan mahdottomana peikkona, kaikkea pidetään kiellettynä ja toimiminen on hankalaa. Paremminkin tulisi löytää tasapaino, koska elämä ei oleellisesti muutu yhdessä yössä ja maalaisjärjenkin käyttö on sallittua. (Juuti 2018.)

### 5.6 Haastatteluiden yhteenveto

Yhteenvetona voi todeta haastateltavien pitävän hyvän henkilötietojen tietosuojan toteutumista tärkeänä. Kevään aikana tuotettuja materiaaleja ja koulutuksia pidettiin hyvänä ja niitä toivottiin lisää. Valmistautuminen tietosuoja-asetuksen soveltamiseen Helluntaikirkossa on aloitettu ja valmistautuminen etenee kevään aikana. Aihe on silti uusi ja seurakunnat kaipaavat sen vuoksi apua Helluntaikirkon toimistolta ja hallinnolta. Yhdyskunnan toimisto auttaisi

mielellään, mutta kokee resurssinsa rajalliseksi. Haastatteluista yhteenvetona saa kuvan, että joskus voi käydä niinkin, että seurakunta vastuuttaa Helluntaikirkon toimistoa ja johtoa pyytämällä apua ja materiaalia. Samaan aikaan johto muistuttaa, että se toiminnassaan ja hallituksena toteuttaa ainoastaan seurakuntien vuosikokousten päätöksiä. Jotta Helluntaikirkko ja sen jäsenseurakunnat saadaan mukaan parantamaan tietosuojaa, tarvitaan asian pitämistä esillä laajasti. Yrjölän mukaan: ”Jos käsittelet yhtä listaa tai yhtä nimeä, tietosuoja koskee sinua”. Vastaavasti Korhonen kuvasi, kuinka tietosuoja on hyvä asia ja ihmisten turvaksi. Haastateltavat puhuivat monipuolisesti eri osa-alueista ja sen johdosta yhteenvetona voikin todeta, että haastatteluiden perustella tarvitaan nimenomaan kokonaisvaltaista lähestymistä tietosuojaan. Tarvitaan ylimmästä johdosta alkaen jokaiseen vapaaehtoistyöntekijään asti kaikki mukaan, koska jokaisella on rooli omasta toimenkuvastaan käsin olla parantamassa henkilötietojen tietosuojaa.

# 6 Johtopäätökset Suomen Helluntaikirkon tietosuojakäytäntöön

## 6.1 Lähtötilanne

Tietoperustan ja siihen peilaavien haastatteluiden perusteella hyvän tietosuojan toteutuminen on Helluntaikirkolle tärkeää. Helluntaikirkolla on olemassa tietosuojaan liittyviä käytäntöjä ja näitä käytäntöjä se voi halutessaan uudistaa ja kehittää. Tässä opinnäytetyössä ehdotetaan, että Helluntaikirkko loisi yhdyskunnalle Tietosuojakäytäntö-nimisen kirjallisen dokumentaation ja ohjeistuksen, jossa kerrotaan, kuinka Helluntaikirkossa hyvästä henkilötietojen tietosuojasta on tarkoitus huolehtia. Tietosuojakäytäntöä voi kuvata myös eräänlaiseksi perusasiakirjaksi, jossa kuvattaisiin Helluntaikirkon tietosuojaratkaisut ja käytännöt kirjallisesti. Tietosuojakäytännössä tulisi kuvata, mitä tietoja Helluntaikirkon kanssa vuorovaikutuksessa olevilta kerätään ja kuinka niitä käytetään. Näitä tulisi kuvata toimiston ja johdon, työntekijöiden sekä rekisteröidyn eli seurakuntalaisen näkökulmasta. Seuraavissa kappaleissa kerrotaan periaatteita ja näkökulmia Helluntaikirkon työntekijöille, jäsenseurakuntien vastuunkantajille ja muille henkilöille, jotka käsittelevät henkilötietoja Helluntaikirkossa.

Kuten aiemmin on kerrottu, Euroopan unionin uudistettu yleinen tietosuoja-asetus astui voimaan keväällä 2016 ja sitä aletaan soveltaa keväällä 2018, jolloin viimeistään henkilötietojen käsittelyn tulee Helluntaikirkossakin olla asetuksen mukaista. Helluntaikirkolla tarkoitetaan näissä johtopäätöksissä Helluntaikirkon toimistoa sekä sen kaikkia jäsenseurakuntia yhdessä. Seurakuntien jäsenrekisterit ovat henkilörekistereitä ja asetus tiukentaa henkilötietojen käsittelyä. Tarvitaan parempia IT-laitteistoja sekä kirjallinen dokumentaatio siitä, kuinka varmistetaan asetuksen noudattaminen. Vaikka aiemmin on riittänyt esimerkiksi tietokoneelta käytettävän seurakunnan jäsenrekisteriohjelman yhdistäminen palvelimeen, joka on suojattu

palomuurilla ja virustorjunnalla, pitää uuden asetuksen myötä palvelimen lisäksi havaita tietoturvaloukkaukset, tunnistaa tunkeutuminen, tietää onko tietoja kadonnut ja jos on, mitä tietoja on kadonnut. Laitteiston asetuksenmukainen toiminta on rekisterinpitäjän eli seurakunnan vastuulla, ei laitetoimittajan, kuten helposti voisi ajatella.

Tietosuoja-asetuksen uusi asia on osoitusvelvollisuus, joka tarkoittaa henkilötietojen käsittelyyn liittyvien prosessien ja tietosuojaperiaatteiden käytännön toteutuksen dokumentointia. Seurakunnan tulee arvioida henkilötietojen käsittelyn riskejä. Asetuksessa riskeillä tarkoitetaan seurakunnan jäsenelle mahdollisesti aiheutuvia fyysisiä, aineellisia tai aineettomia vahinkoja esimerkiksi silloin, kun tietojen käsittely saattaa johtaa syrjintään, identiteettivarkauteen tai petokseen, taloudelliseen menetykseen, sosiaaliseen vahinkoon tai pseudonymisoinnin kumoutumiseen. Viimeksi mainittu tarkoittaa esimerkiksi somekirjoittelussa käytetyn nimimerkin yhdistämistä henkilötietoihin. Riski voi olla korkeampi silloin, kun käsitellään erityisiä henkilötietoryhmiin kuuluvia tietoja, kuten lasten tietoja.

Tarvittaessa tulee tehdä vaikutusten arviointi, jossa tarkastellaan suunniteltuja toimenpiteitä, joilla lievitetään jäsentietojen käsittelyyn kohdistuvaa riskiä ja varmistetaan henkilötietojen suoja sekä asetuksen toteutuminen kaikessa toiminnassa. Tietojen suojaamisesta on huolehdittava kaikissa käsittelyn vaiheissa alkaen tietojen keräämisestä ja päättyen tietojen tuhoamiseen. Käsittelyn turvallisuus edellyttää esimerkiksi kykyä taata järjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus sekä kykyä palauttaa tietojen saatavuus ja pääsy tietoihin nopeasti fyysisen tai teknisen vian sattuessa. Tietojen suojaaminen edellyttää myös henkilötietojen käsittelyn seuraamista ja valvontaa. Helluntaikirkon kanssa vuorovaikutuksessa olevalla henkilöllä on oikeus läpinäkyvään informaation käsittelyyn, oikeus nähdä omat tietonsa, oikeus tietojen oikaisemiseen, oikeus tulla unohdetuksi sekä muutamia muita asianmukaiseen henkilötietojen käsittelyyn liittyviä oikeuksia.

### 6.2 Prosessi seurakunnassa

Helluntaikirkon lakityöryhmän jäsen varatuomari Markku Luoma on suunnitellut ehdotuksen prosessista, kuinka tietosuojaa voisi parantaa jäsenseurakunnissa tietosuoja-asetuksen mukaiseksi (liite 9). Luoma ehdottaa, että seurakunnan johto asettaa työryhmän valmistelemaan asiaa. Sen jälkeen työryhmä kartoittaa nykyiset henkilörekisterit sekä kokoaa, suunnittelee ja päivittää tarvittavat dokumentaatiot ja järjestää koulutukset ja muut toimenpiteet. Työryhmä voi myös esittää henkilöä tietosuojavastaavaksi sekä henkilöä vastuunkantajaksi, kuka on rekisterinpitäjän edustajana vastuussa henkilörekistereistä. Seurakunnan johto käsittelee esityksen ja hyväksyy tai vahvistaa tehdyt dokumentit sekä nimittää tarvittaessa vastuunkantajan, tietosuojavastaavan sekä henkilötietojen käsittelijät. Lopuksi tietosuojavastaava ja vastuunkantaja alkavat toteuttamaan suunniteltuja ja päätettyjä toimenpiteitä. (Luoma 2018.)

### 6.3 Yleiset ohjeet ja periaatteet

Seuraavassa on ehdotus yleisistä ohjeista ja periaatteista, joita Helluntaikirkko voi halutessaan ottaa käyttöön. Helluntaikirkko kerää henkilötietoja yhdyskuntajärjestyksessään määritellyn toimintansa järjestämiseksi. Henkilötietoja ei luovuteta ulkopuolisille ilman rekisteröidyn lupaa. Rekisteröity tarkoittaa seurakunnan jäsentä, lastenleirin osallistujaa, seurakuntien henkilökuntaa tai ketä tahansa muuta Helluntaikirkon kanssa vuorovaikutuksessa olevaa henkilöä, jonka henkilötietoja käsitellään. Toiminnassa huomioidaan erityisesti erityiset henkilöryhmät, kuten lapset. Samoin huolehditaan siitä, että lähtökohtaisesti kiellettyjen henkilötietojen käsittelyssä noudatetaan erityistä huolellisuutta. Uskonnon merkitseminen rekisteröidyn henkilötietoihin on lähtökohtaisesti kiellettyä, mutta voidaan tehdä lakisääteisen tehtävän suorittamiseksi, eli uskonnollisen yhdyskunnan jäsenrekisteristä huolehtimiseksi.

Helluntaikirkko sitoutuu toteuttamaan kaikessa toiminnassaan henkilötietojen yksityisyyden suojaa ja ohjaa käsittelemään henkilötietoja tietosuoja-asetuksen mukaisesti. Henkilötietojen käsittelyssä tulee noudattaa erityistä huolellisuutta, olivatpa tiedot sähköisessä muodossa tai paperilla. Henkilötietoja säilytetään suojatussa tietojärjestelmässä tai paperiversiot lukitussa tilassa tai kassakaapissa. Helluntaikirkko seuraa viranomaisten ohjeistusta tietosuojasta, josta lisää kappaleessa 6.15. Lisäksi Helluntaikirkko voi halutessaan pyytää henkilötietojen käsittelijöitä allekirjoittamaan salassapito- ja vaitiolositoumuspaperin (Liite 8). Tällä tavalla saadaan täytettyä artiklan 28 kirjallinen osuus sekä osoitusvelvollisuudenkin toteuttamista varten kerättyä dokumentaatiota. Samaa dokumenttia voi hyödyntää, kun sitoutetaan palkattua henkilöstöä sekä vapaaehtoisia asetuksenmukaiseen toimintaan.

Tavoitteena voisi olla, että tulevaisuudessa kaikki henkilötiedot käsitellään vain sähköisesti suljetuissa järjestelmissä. Jokaisessa tietokoneessa, jolla käsitellään henkilötietoja, tulee olla henkilökohtainen tunnus ja salasana, jota ei ole lupa luovuttaa kenellekään. Tietojärjestelmiin kirjaudutaan vain tietokoneen henkilökohtaisen tunnuksen jälkeen ohjelman henkilökohtaisen tunnusten ja salasanan avulla, jota ei ole lupa luovuttaa kenellekään. Tietokoneiden tietoturvan, sisältäen ainakin palomuurin ja virustorjunnan, tulee olla kunnossa ja ajan tasalla. Ohjelmistojen pilvipalvelimissa tulee lisäksi olla toiminnot tietosuoja-asetuksen mukaista tietoturvaa varten.

Mikäli henkilötietoja käsitellään paperilla, tulee huolehtia siitä, että muilla ei ole pääsyä papereihin. Jos paperi on toimiston pöydällä tai hyllyssä kansiossa, toimiston oven tulee olla lukittuna aina kun henkilötietojen käsittelijä ei ole paikalla. Toimistoon tulee olla avain vain henkilötiedon käsittelijällä. Jos toimistoa käyttävät muutkin, paperia tulee säilyttää lukitussa kaapissa tai kassakaapissa, johon vain henkilötiedon käsittelijällä on avain, ja vara-avaimen hallinnan tulee olla koordinoitua. Helluntaikirkossa palkatut työntekijät tai vapaaehtoiset toisinaan tehdessään etätöitä käsittelevät henkilötietoja. Mikäli henkilötietoja on tarpeen käsi-

tellä paperilla, tulee huolehtia, että myös etäpisteessä on asianmukainen kassakaappi tai lukittava kaappi, johon muilla perheenjäsenillä tai vierailla ei ole pääsyä. Haasteena paperilla olevissa henkilörekistereissä on varmuuskopiointi ja tietojen palauttaminen esimerkiksi tulipalon, vesi- tai muiden vahinkojen tai varkauksien jäljiltä. Näihin tulisi kuitenkin varautua ja henkilörekisteri kyetä tarvittaessa palauttamaan. Lisäksi mahdollisista laajamittaisesta tietoturvaloukkauksesta tulisi kyetä raportoimaan viranomaisia 72 tunnin kuluessa. Tämä voi olla hankala toteuttaa, jos varkaat murtautuvat taloon ja vievät henkilörekisterin lukollisesta kaapista ja jos henkilötietojen käsittelijä on esimerkiksi matkalla. Tämän johdosta usein ratkaisuna on pilvipohjaiset järjestelemät, jolloin varmuuskopiointi ja tietojen palauttaminen on helpompaa.

Henkilötietojen valokuvaaminen tietokoneen ruudulta tai muu vastaava toiminta on kiellettyä. Tietoja käsitellään vain järjestelmän sisällä ja mahdollisesta siirrosta tulee sopia tietosuojavastaavan kanssa etukäteen, jotta varmistetaan tietosuojan toteutuminen. Jos on tarpeen käsitellä, esimerkiksi Excelissä olevaa seurakunnan lastenleirin osallistujaluetteloa, suositellaan seuraavaa. Seurakunnan olisi hyvä luoda Teams- tai Sharepoint-ympäristö (tai vastaava), johon seurakunnan henkilötietojen käsittelijöillä on omat henkilökohtaiset tunnukset, jota ei luovuteta kenellekään. Tähän seurakunnan omaan suljettuun Sharepoint-ympäristöön voidaan tallentaa esimerkiksi lastenleirin tietoja. Ympäristöön voidaan antaa käyttöoikeuksia tarvittaville henkilöille esimerkiksi vain yhteen hakemistokansioon tai yhteen tiedostoon. Tällöin tietoja ei tarvitse siirtää mihinkään, esimerkiksi sähköpostilla, vaan henkilörekisterin käyttäjä(t) voi(vat) käsitellä tietoa yhdessä paikassa. Vaikka käyttäjät olisivat fyysisesti eri paikassa, henkilörekisterin käyttäjät tunnuksillaan kirjautuneena ottavat yhteyttä yhteen ja samaan Sharepoint-ympäristöön.

Muistitikkujen ja muiden siirrettävien tallentimien käyttöä tulee välttää, koska muistitikku ja sen huolimaton käyttö on yksi isoimmista tietoturvariskeistä. Järjestelmien varmuuskopioinnin hoitaa palvelutarjoaja, joten esimerkiksi seurakunnan jäsenrekisterin tai sen osien varmuuskopioiminen muistitikulle (tai tietokoneelle) on kiellettyä. Jos jotain erityistä tarkoitusta varten joku muu henkilörekisteri tallennetaan muistitikulle tai muulle siirrettävälle tallentimelle, minimivaatimuksena on salasanan asettaminen muistitikkuun ja erikseen siinä olevaan tiedostoon. Muistitikkua tulee säilyttää lukitussa tilassa, mielellään kassakaapissa.

Sähköpostilla henkilörekisterin tietojen lähettämistä tulee välttää. Suositellaan Teams- tai Sharepoint-ympäristöä lähettämisen sijaan siten, että sähköpostilla lähetetään ainoastaan linkki suljettuun Sharepointiin. Tarvittaessa voidaan myös käyttää suojattua sähköpostia tai vähintään suojata salasanalla sähköpostin liite. Word- ja Excel -tiedostot suojataan Tiedosto-valikon Tiedot-alavalikon Suojaa tiedosto -kohdasta. Salasana tulee toimittaa vastaanottajalle erikseen, esimerkiksi soittamalla tai tekstiviestillä.

Yleisenä periaatteena on, että tulevaisuudessa henkilötietojen käsittelijän tunnistautumisesta pyritään tekemään mahdollisimman vahva. Tulevaisuudessa erilaiset tekniset ratkaisut kehittyvät siihen suuntaan, että tunnuksien ja salasanojen lisäksi voidaan teknisillä ratkaisuilla määritellä muitakin tunnistautumisen kriteerejä, kuten tieto siitä, mistä fyysisesti kirjaudutaan järjestelmään. Tämän johdosta tiedetään vielä varmemmin, kuka henkilötietoja käsittelee. Järjestelmät rakennetaan siten, että käsittelijän tietojen käsittelystä jää aina jälki järjestelmään, joka puolestaan edistää vastuullista henkilötietojen käsittelyä ja helpottaa selvitystyötä mahdollisissa tietoturvaloukkauksissa.

Henkilötiedoilla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan henkilöön liittyviä tietoja. Tunnistettavissa oleva on henkilö, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella. Käsittelyllä tarkoitetaan toimia, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti, kuten tietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakua, kyselyä, käyttöä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista. Rekisterillä tarkoitetaan mitä tahansa jäsenneltyä henkilötietoja sisältävää tietojoukkoa, josta tiedot ovat saatavilla tietyin perustein.

### 6.4 Rekisterit ja rekisterinpitäjä

Helluntaikirkon rekisteriselosteessa kerrotaan henkilötietojen keräämisestä ja käyttämisestä. Rekisteriseloste on lähetetty seurakuntiin ja se on saatavana myös Helluntaikirkon toimistosta, mistä se voidaan tarvittaessa toimittaa sitä kysyvälle. Rekisteriseloste on aiemmin otsikoitu nimellä jäsenrekisterin rekisteriseloste. Helluntaikirkossa on kuitenkin muitakin henkilörekistereitä kuin jäsenrekisteri. Tämän johdosta rekisteriselostetta ehdotetaan päivitettäväksi siten, että jäsenrekisterin sijaan puhuttaisiin henkilörekistereistä, jolloin se kattaa jäsenrekisterin lisäksi muutkin henkilörekisterit. Liitteessä on ehdotus päivitetystä rekisteriselosteesta (Liite 5).

Huhtikuussa 2018 Tietosuojavaltuutetun toimisto julkaisi rekisteriselosteen oheen tietosuojaselosteen, jonka alku on sama kuin rekisteriselosteessa. Tietosuojaselosteessa on lisäksi kolme lisäkohtaa siitä, kuinka rekisteröidyn oikeudet toteutuvat organisaatiossa. Selosteessa kuvataan, kuinka organisaatio toteuttaa tarkastusoikeuden, oikeuden vaatia tiedon korjaamista sekä muut henkilötietojen käsittelyyn liittyvät oikeudet. (Tietosuojavaltuutetun toimisto 2018b.) Helluntaikirkon kannattaisi päivittää liitteen viisi rekisteriseloste tietosuojaselosteeksi.

Helluntaikirkossa käsitellään henkilötietoja yhdyskuntajärjestyksessä kuvatun toiminnan järjestämiseksi. Helluntaikirkon organisaatio rakentuu siten, että sillä on toimisto Helsingissä ja jäsenseurakuntia eri puolilla Suomea. Seurakunnat ovat itsenäisiä ja toimiston roolina on tuottaa tukipalveluja. Toimisto ja seurakunnat toimivat rekisterinpitäjinä ja henkilötietojen käsittelijöinä omissa asioissaan Helluntaikirkon yhdyskuntajärjestyksen mukaisen toiminnan järjestämiseksi.

Helluntaikirkon toimiston ja jäsenseurakuntien yhteinen yksi Helluntaikirkon rekisteriseloste riittää kattamaan normaalin seurakuntaelämän. Rekisteriselosteen käsite ’toimintansa järjestämiseksi’ sisältää jumalanpalvelustoiminnot, leirit, jäsen- (asiakas) tiedotuksen, jäsenrekisterit, hallituksien- ja työryhmien kokoonpanotiedot, puhelinluettelon ja muut normaalit seurakunnan ja toimiston toiminnot. Oleellista on, että jo puhelinluettelo muodostaa henkilörekisterin, mutta yksittäisiä rekistereistä ei tarvitse listata, vaan oleellista on käyttötarkoitus. Henkilötietoja kerätään tiettyä tarkoitusta varten, eli Helluntaikirkon seurakuntien ja toimiston toimintaa varten. Mikäli käyttötarkoitus muuttuisi siten, että tietoja kerättäisiin esimerkiksi suoramarkkinointia varten, sillä olisi heti vaikutusta rekisteriselosteeseen. (Tietosuojavaltuutetun toimisto 2018b).

Helluntaikirkon toimiston omaa toimintaa on esimerkiksi vihkilupien koordinointi Helluntaikirkossa. Jäsenseurakuntien omaa toimintaa on esimerkiksi jumalanpalvelustoiminnan järjestäminen. Omien toimintojen lisäksi jäsenrekisteriä käsitellään osittain yhdessä seuraavalla tavalla. Henkilöjäsen hakeutuu ensin jäseneksi jäsenseurakuntaan. Jäsenseurakunta lisää, tarvittaessa muokkaa tai erottaessa lopulta poistaa rekisteröidyn tiedot. Rekisteröity saa jäsenpalvelut jäsenseurakunnasta. Helluntaikirkon toimiston roolina on hallinnoida valtakunnallista jäsenrekisteriä ja toimia yhteyshenkilönä valtakunnallisesti Väestörekisterikeskuksen kanssa jäsenrekisteriasioissa.

Mikäli toimisto tai jäsenseurakunta luo uuden henkilötietorekisterin sellaista toimintoa varten, jota ei ole mainittu yhdyskuntajärjestyksessä, siitä olisi hyvä ilmoittaa Helluntaikirkon mahdollisesti myöhemmin nimitettävälle tietosuojavastaavalle, tehdä asianmukainen rekisteriseloste ja varmistaa tietosuojan toteutuminen.

## 6.5 Helluntaikirkon henkilötietovarannot

### 6.5.1 Toimiston henkilörekisterit

Helluntaikirkon toimiston isoimman henkilörekisterin muodostaa yhdyskunnan valtakunnallinen jäsenrekisteri. Työntekijöiden henkilörekisterinä on palkkarekisteri sekä erilaiset muut henkilörekisterit työtehtävien tekemistä varten. Näitä ovat ryhmien kokoonpanot, kuten hallituksen jäsenlista, työryhmien kokoonpanolistat, lista vihkioikeuden haltijoista, lista pastorin tai lähetystyöntekijän valtakirjaa hakeneista ja saaneista sekä arkistointitiedot edellisistä.

Näitä rekistereitä tulee käsitellä kappaleissa 6.1 - 6.4 kuvattujen ohjeiden ja periaatteiden mukaan.

### 6.5.2 Jäsenseurakuntien henkilörekisterit

Seurakuntien jäsenrekisterit muodostavat henkilörekisterin. Sen lisäksi jäsenseurakuntien pastoreista ja muista työntekijöistä on palkkarekisteri sekä muita henkilörekistereitä työtehtävien tekemistä ja seurakunnan toimintaa varten. Seuraavassa on, esimerkin omaisesti, listattu muutamia rekistereitä. Kuten aiemmin on kerrottu, rekisterillä tarkoitetaan siis mitä tahansa jäsenneltyä henkilötietoja sisältävää tietojoukkoa, josta tiedot ovat saatavilla tietyin perustein. Henkilörekistereitä muodostavat vanhimmiston henkilötiedot, vapaaehtoistyöntekijöiden henkilötietolista sekä työmuodoissa mukana olevien henkilötietolista. Näitä ovat solu- tai pienryhmätoiminnassa, perhetyössä -, nuorisotyössä -, varhaisnuorisotyössä -, lapsityössä sekä muissa työmuodoissa mukana olevien henkilötietolista. Lisäksi henkilörekisterin muodostaa leirien ja evankeliointi- sekä muiden tapahtumien järjestelyä tai jälkeenpäin tehtävää yhteydenottoa varten tehty henkilötietolista sekä seurakuntien ulkomailla olevien (lähetys)työntekijöiden henkilötietolista. Lisäksi henkilörekisterin muodostaa erilaisia toimintoja varten koottu henkilötietolista. Näitä ovat henkilötiedot seurakunnan vahtimestareista ja järjestysmiehistä, tiedot seurakunnan avaimen haltijoista, tiedot siistijöistä, tiedot keittiöhenkilökunnasta, tiedot seurakunnan muusikoista ja laulajista sekä tiedot seurakunnan kirpputorin vapaaehtoisista. Kaikenlaista markkinointitarkoitusta, evankeliointia tai jäsenhankintaa varten kootut henkilötiedot muodostavat myös henkilörekisterin. Myös seurakunnan, leirikeskuksen tai muun kiinteistön mahdollinen videovalvonta muodostaa oman henkilörekisterin, koska videokuvasta henkilö on tunnistettavissa.

Näitä rekistereitä tulee käsitellä edellisissä kappaleissa 6.1 - 6.5 kuvattujen ohjeiden ja periaatteiden mukaan.

## 6.6 Tietosuojaperiaatteiden toteuttaminen

### 6.6.1 Sisäänrakennettu ja oletusarvoinen tietosuoja

Henkilötietojen käsittelyn tulee olla sisäänrakennetun ja oletusarvoisen tietosuojan mukaista. Tämä tarkoittaa pääpiirteittäin vanhan henkilötietolain mukaista henkilötietojen käsittelyn suunnittelu- ja huolellisuusvelvoitetta. Käsittelyn tulee olla lainmukaista, kohtuullista ja läpinäkyvää. Henkilötietoja tulee käsitellä vain tiettyä käyttötarkoitusta varten ja vain siinä laajuudessa, mikä on tarpeen kyseisen tehtävän suorittamista varten. Henkilötietojen tulee olla täsmällisiä ja mahdolliset oikeinkirjoitusvirheet, vanhat osoitetiedot tai muut virheet henkilötiedoissa tulee korjata. Tietoja tulee säilyttää vain sen aikaa, kun on tarpeellista ja huolehtia sen jälkeen viipymättä tietojen asianmukaisesta hävittämisestä. Tietoja on käsiteltävä tavalla, jolla varmistetaan henkilötietojen suojaaminen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta.

Helluntaikirkon tietosuojaperiaatteet toteutuvat siten, että kaikessa toiminnassa ja sen kaikissa vaiheissa tulee huomioida tietosuojan toteutuminen. Ei niin, että tietosuoja on yksi huomioitava asia seurakunnan toiminnassa samaan tapaan kuin kiinteistö, lapsityö, tai jäsenhuolto. Tietosuoja toteutuu, kun rakennetaan ratkaisut, jossa kaiken toiminnan kaikissa vaiheissa varmistetaan tietosuojan toteutuminen. Seurakunnan kiinteistössä huolehditaan tietosuojasta esimerkiksi järjestämällä mahdollisen kameravalvonnan hallinta asianmukaisesti tai varmistamalla, että seurakunnan ilmoitustaululla oleviin henkilötietoihin on asianmukainen peruste, mahdollisesti kirjallinen lupa. Lapsityössä huomioidaan ensinnäkin se, että lasten tietoja erityisenä ryhmänä tulee lähtökohtaisesti käsitellä vielä huolellisemmin tietosuoja-asetuksen mukaisesti. Samoin huolehditaan, että tarvittaessa alaikäisten lasten vanhemmilta kysytään lupa henkilötietojen käsittelyyn.

### 6.6.2 Osoitusvelvollisuus

Osoitusvelvollisuus tarkoittaa henkilötietojen käsittelyyn liittyvien prosessien ja tietosuojaperiaatteiden käytännön toteutuksen dokumentointia. Helluntaikirkon tietosuojakäytännössä tulisi olla kirjattuna, kuinka Helluntaikirkossa varmistetaan tietosuoja-asetuksen toteutuminen. Tämä sisältää ohjeet toimistolle ja jäsenseurakunnille sekä asianmukaiset dokumentoidut tietotekniset ratkaisut. Lisäksi vuosittain olisi hyvä tehdä tietotilinpäätös, jonka avulla voidaan seurata tehtyjä tietosuojaratkaisuja ja niiden toteutumista. Tietotilinpäätöstä voi verrata talouden vuosittaiseen tilinpäätökseen, jossa raportoidaan organisaation talous. Tietotilinpäätöksen avulla raportoidaan tietosuoja-asiat. Tässä voi käyttää mallina esimerkiksi Tietosuojavaltuutetun toimiston ohjetta (2012).

## 6.7 Riskit jäsentietojen käsittelyssä

Helluntaikirkon tulee tietosuoja-asetuksen mukaisesti arvioida henkilötietojen käsittelyyn liittyvät riskit. Näillä riskeillä tarkoitetaan seurakunnan jäsenelle mahdollisesti aiheutuvia fyysisiä, aineellisia tai aineettomia vahinkoja esimerkiksi silloin, kun tietojen käsittely saattaa johtaa syrjintään, identiteettivarkauteen tai petokseen, taloudelliseen menetykseen, sosiaaliseen vahinkoon tai pseudonymisoinnin kumoutumiseen. Viimeksi mainittu tarkoittaa esimerkiksi somekirjoittelussa käytetyn nimimerkin yhdistämistä henkilötietoihin. Riski voi olla korkeampi silloin, kun käsitellään erityisiä henkilötietoryhmiin kuuluvia tietoja, kuten lasten tietoja. Helluntaikirkko on kartoittanut riskejä, mutta niitä ei julkaista tässä opinnäytetyössä. Helluntaikirkon tietosuojakäytäntöä pyritään kehittämään siten, että se poistaa tai pienentää riskejä mahdollisimman paljon. Haastattelujen perusteella riskinä on ainakin huolimattomuus ja/tai välinpitämättömyys tietojen käsittelyssä sekä tietosuoja-asetuksen tuntemisen puute, jonka johdosta ei tiedetä kuinka tulisi toimia. Riskinä voi olla huolimaton salasanojen hallinta, jäsenseurakuntien tietokoneiden tietoturva, vastuunkantajien rajoittuneet tietotekniset taidot muiden henkilörekistereiden kuin jäsenrekisterin käytön osalta, huolimattomuus henki-

lötietoja sisältävien papereiden käsittelyssä seurakuntien toimistossa sekä sen huomiotta jättäminen, että tieto henkilön uskonnosta tai lasten tiedot ovat erityisen arkaluontoisia ja vaativat erityistä huolellisuutta.

### 6.8 Tietosuojaa koskeva vaikutustenarviointi

Mikäli Helluntaikirkkoon otetaan käyttöön uutta teknologiaa ja käsitellään laajamittaisesti erityisiin henkilötietoryhmiin kuuluvia tietoja, tulisi tehdä vaikutuksenarviointi. Helluntaikirkon rekisterinpitäjän tai mahdollisesti nimetyn tietosuojavastaavan tulisi konsultoida asianomaisia viranomaisia, kuten esimerkiksi tietosuojavaltuutetun toimistoa ennen toimenpidettä, jotta minimoidaan riskit ja varmistetaan muutenkin tietosuoja-asetuksen toteutuminen.

### 6.9 Henkilötietojen käsittelyn oikeusperusteet

Helluntaikirkossa henkilötietojen käsittelyä tehdään lakisääteisen velvoitteen noudattamiseksi. Toisin sanoen uskonnollisten yhdyskuntien tulee pitää jäsenistään henkilörekisteriä toimintansa järjestämiseksi. Tämä sisältää Helluntaikirkon rekisteriselosteessa mainitut tiedot. Tarvittaessa henkilöltä kysytään suostumus henkilötietojensa käsittelyyn yhtä tai useampaa erityistä tarkoitusta varten. Henkilön ollessa osapuolena sopimuksessa erillistä suostumusta ei tarvita.

### 6.10 Henkilötietojen käsittelyn ulkoistaminen

Helluntaikirkko ei ulkoista henkilötietojen käsittelyä. Henkilötietojen käsittelijä ei saa käyttää toisen henkilötietojen käsittelijän palveluksia ilman rekisterinpitäjän kirjallista lupaa.

### 6.11 Rekisteröidyn oikeudet

Seurakunnan jäsenillä ja muilla Helluntaikirkon järjestelmiin rekisteröidyillä henkilöillä on oikeus saada tietoa rekistereihin tallennetuista tiedoista läpinäkyvästi ja saada muutenkin yksityiskohtaiset tiedot rekisteröidyn oikeuksien käyttöä varten. Seuraavassa on listattu oikeuksia. Tämän lisäksi suositellaan vierailemaan Tietosuojavaltuutetun toimiston nettisivuilla, josta löytyy lisää tietoa rekisteröidyn oikeuksista (2014).

#### 6.11.1 Oikeus saada läpinäkyvää informaatiota henkilötietojen käsittelystä.

Helluntaikirkko varmistaa läpinäkyvän informaation käsittelyn toimittamalla henkilötietojen käsittelyä koskevat tiedot rekisteröidylle tiiviisti esitetyssä, läpinäkyvässä, helposti ymmärrettävässä ja saatavilla olevassa muodossa. Jäsenrekisterin tiedot on kirjattu seurakuntiin lähetetyssä rekisteriselosteessa. Lupaan perustuvien henkilötietojen käsittelyä koskevat tiedot toimitetaan lupaa kysyttäessä. Mikäli rekisteröity esittää pyynnön toimenpiteelle, viimeistään kuukauden kuluessa toimitetaan tieto siitä, mihin toimiin on ryhdytty.

### 6.11.2 Rekisteröidyn oikeus saada pääsy tietoihin

Rekisteröidyllä on oikeus saada jäljennös häntä koskevista henkilötiedoista kuukauden kuluessa sen jälkeen, kun Helluntaikirkko on varmistanut pyynnön esittäjän henkilöllisyyden.

### 6.11.3 Oikeus tietojen oikaisemiseen ja oikeus tulla unohdetuksi

Mikäli henkilötiedoissa on kirjoitusvirhe, väärä osoite tai joku muu virhe ja rekisteröity esittää pyynnön tietojen oikaisemiseen, Helluntaikirkko oikaisee tiedon ja ilmoittaa rekisteröidylle oikaisusta. Pyydettäessä Helluntaikirkko poistaa rekisteröidyn henkilötiedot, henkilötietoihin liittyvät linkit, jäljennökset ja kopiot seuraavin poikkeuksin. Jäsenrekisterin pitäminen on Helluntaikirkolle lakisääteinen velvoite, jonka johdosta jäsentietoja ei voida poistaa, mikäli jäsenyys yhdyskunnassa jatkuu. Tilastointi- ja arkistointitarkoitusta varten kerättyjä tietoja ei poisteta.

### 6.11.4 Oikeus käsittelyn rajoittamiseen ja rekisterinpitäjän velvollisuus ilmoittaa rajoituksesta

Mikäli Helluntaikirkko on poistamassa rekisteröidyn henkilötietoja, rekisteröidyllä on oikeus poistamisen sijaan pyytää käsittelyn rajoittamista asian selvittelyn ajaksi. Samoin Helluntaikirkko rajoittaa pyydettäessä rekisteröidyn henkilötietojen käsittelyä selvittelyn ajaksi, mikäli Helluntaikirkko on rekisteröidyn näkemyksen mukaan korjaamassa henkilötietoja virheellisesti. Mikäli käsittelyä rajoitetaan, rajoituksen aikana Helluntaikirkko säilyttää tietoja muuttamatta niitä ja ilmoittaa käsittelyn rajoittamisesta rekisteröidylle.

### 6.11.5 Oikeus siirtää tiedot järjestelmästä toiseen

Rekisteröidyn oikeutta siirtää suostumukseen tai sopimukseen perustuvia henkilötietoja järjestelmästä toiseen ei sovelleta, koska Helluntaikirkko ei käsittele tietoja automaattisesti.

### 6.11.6 Vastustamisoikeus

Helluntaikirkko ei käytä julkista valtaa eikä sen jäsenrekisteriä käytetä profilointi- tai suoramarkkinointitarkoituksiin, joten vastustamisoikeutta ei siltä osin sovelleta. Tietoja ei käytetä muuhun tarkoitukseen, kuin niihin, mitä varten ne on kerätty. Mikäli Helluntaikirkko luvan saatuaan profilointi- tai suoramarkkinointitarkoitusta varten käsittelee rekisteröidyn henkilötietoja, rekisteröidyllä on henkilökohtaiseen erityiseen tilanteeseensa liittyvällä perusteella oikeus vastustaa tätä, jolloin Helluntaikirkko ei käsittele rekisteröidyn tietoja. Tarkoitusperää ei laajenneta ilman rekisteröidyn lupaa.

### 6.11.7 Automatisoidut yksittäispäätökset ja profilointi

Helluntaikirkko ei käsittele eikä profiloi rekisteröidyn tietoja pelkästään automaattisesti. Helluntaikirkko tiedostaa, että automattisessa käsittelyssä rekisteröidyllä on oikeus vastustaa käsittelyä, mikäli se vaikuttaa häneen merkittävästi. Tämä koskee erityisesti erityisiä henkilöryhmiä, kuten lapsia.

## 6.12 Helluntaikirkon toimiminen muissa EU:n jäsenvaltioissa

Helluntaikirkon henkilörekistereitä käsitellään vain Suomessa.

## 6.13 Tietoturva ja tietoturvaloukkauksiin valmistautuminen

Tietoturvalla tarkoitetaan usein tietokone- ja muita IT-ratkaisuja tietosuojan toteuttamiseksi. Tietoturva koskettaa lisäksi toimitiloja, järjestelmiä, tietoja ja tietoliikenteen suojausta, tietojen salausta ja pääsyn rajoittamista. Tavoitteena on turvata tietojenkäsittelyn eheys, luottamuksellisuus ja saatavuus.

Yleisten ohjeiden kappaleessa kerrottiin, kuinka Helluntaikirkko voisi käyttää tietoturvan parantamiseksi asianmukaisia suljettuja järjestelmiä, joihin kirjaudutaan henkilökohtaisilla tunnuksilla. Jos tapahtuu henkilötietojen tietoturvaloukkaus, rekisterinpitäjän on ilmoitettava siitä ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa valvontaviranomaiselle, paitsi jos henkilötietojen tietoturvaloukkauksesta ei todennäköisesti aiheudu henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä. Tämä voidaan toteuttaa siten, että järjestelmään lisätään erillinen ohjelma tai sen palomuuri- tai muuta ratkaisua parannetaan siten, että järjestelmä lähettää automaattisesti tiedon rekisterinpitäjälle mahdollisista tietoturvaloukkauksista tai yrityksistä päästä järjestelmään. Sen lisäksi rekisterin yhteyshenkilöä tulee ohjeistaa tarvittaessa raportoimaan tietosuojaviranomaisia ja rekisteröityjä mahdollisen tietoturvaloukkauksen vaikutuksista. Ehdotetaan myös erillisen suunnitelman ja dokumentaation tekemistä etukäteen valmiiksi mahdollisten tietoturvaloukkausten varalle, johon kirjataan henkilökuntaa varten ohjeet, mistä mahdollisen tietoturvaloukkauksen tiedot löytyvät ja ohje miten tietopyyntöihin vastataan rekisteröidylle ja 72 tunnin kuluessa viranomaisille. Tulee myös valmistella elpymisprosessi, jonka mukaan ensin estetään lisävahingot, seuraavaksi määritellään ongelma tarkemmin ja ratkaistaan se sekä lopuksi varmistetaan, ettei vastaavaa tapahdu enää jatkossa.

Helluntaikirkko voisi lähestyä tietoturvaa ja sen parantamista Fidan tapaan arvioimalla siihen liittyviä riskejä (Liite 6). Voidaan pohtia, onko esimerkiksi uhka tietokoneen salasanojen menettämiseen vähäinen, kohtalainen vai vakava. Sen jälkeen pohditaan, onko uhkaan varauduttu. Varautuminen on voinut olla heikkoa, tyydyttävää tai kohtalaista. Tilanne on hallinnassa, jos uhka on arvion perusteella vähäinen ja siihen on varauduttu hyvin. Vastaavasti tulisi ryhtyä välittömiin toimiin, jos uhka on vakava ja siihen on varauduttu heikosti.

Helluntaikirkko voi halutessaan ohjeistaa, ettei tule klikata tuntemattomia sähköpostilinkkejä eikä tuntemattomien verkkosivujen mainoslinkkejä. Tulee myös varoa tuntemattomia verkkosivustoja eikä luottaa teknisenä tukena esiintyvien henkilöiden yhteydenottoihin, ellei tiedä varmuudella kenestä on kyse. Koskaan ei tule luovuttaa henkilökohtaisia kirjautumistietoja toiselle käyttäjälle tai ulkopuoliselle henkilölle. Ei tule avata sähköpostilinkkejä, joissa väitetään vastaanottajan voittaneen jotain. Ei tule uskoa sähköpostiviesteihin tai tekstiviesteihin, joissa pyydetään tekemään päivityksiä klikkaamalla linkkiä. Seurakunnan tai henkilökohtaiseen pankkisovellukseen ei tule kirjautua sähköpostilinkin välityksellä.

### 6.14 Tietosuojavastaavan nimittäminen

Helluntaikirkon tulisi nimittää tietosuojavastaava. Hänen tehtäviinsä kuuluu antaa rekisterinpitäjälle tai henkilötietojen käsittelijöille tietoja ja neuvoja, jotka koskevat tietosuoja-asetusta ja Suomen tietosuojasäännösten mukaisia velvollisuuksia. Hänen tulee seurata, että noudatetaan tietosuoja-asetusta, muita Suomen tietosuojalainsäännöksiä ja rekisterinpitäjän tai henkilötietojen käsittelijän toimintamenettelyjä, jotka liittyvät henkilötietojen suojaan, mukaan lukien vastuunjako, tiedon lisääminen ja käsittelyyn osallistuvan henkilöstön koulutus ja tähän liittyvät tarkastukset. Lisäksi hänen tulee antaa pyydettäessä neuvoja tietosuojaa koskevasta vaikutustenarvioinnista ja valvoa sen toteutusta tietosuoja-asetuksen 35 artiklan mukaisesti ja tehdä yhteistyötä valvontaviranomaisen kanssa sekä toimia valvontaviranomaisen yhteyspisteenä käsittelyyn liittyvissä kysymyksissä, mukaan lukien tietosuoja-asetuksen 36 artiklan mukainen ennakkokuuleminen ja tarvittaessa kuuleminen muista mahdollisista kysymyksistä.

Käytännöllisenä haasteena on Helluntaikirkon toimiston neuvoa antava rooli suhteessa jäsenseurakuntien itsenäiseen asemaan. Jos nimitetään valtakunnallinen tietosuojavastaava Helluntaikirkkoon, jossa jäsenseurakunnat ovat itsenäisiä, järjestelyistä sovittaessa olisi samalla sopimalla määriteltävä tietosuojavastaavan oikeudet päästä perehtymään seurakunnan tietosuojajärjestelyihin tai tarkastamaan niitä. Samaan aikaan suurin osa jäsenseurakunnista on pienehköjä muutaman sadan hengen yhteisöjä, jolloin paikallisen tietosuojavastaavan nimittäminen jokaiseen pieneenkin jäsenseurakuntaan ei välttämättä ole tarkoituksenmukaista. Kysymyksen voisi ottaa yhdyskunnan vuosikokouksen asialistalle ratkaistavaksi. Suuremmat jäsenseurakunnat voisivat harkita nimittää valtakunnallisen tietosuojavastaavan lisäksi tietosuojavastaavan omaan seurakuntaan. Rajan määritteleminen seurakunnan suuruudesta ja oman tietosuojavastaavan tarpeesta on hankalaa, eikä tietosuoja-asetuskaan sitä tee. Jäsenseurakuntien ei ole pakko nimittää ollenkaan seurakuntaan tietosuojavastaavaa. Ehdotetaan, että esimerkiksi 500 hengen tai isompaan seurakuntaan tietosuojavastaavan voisi nimittää.

### 6.15 Tietosuoja-asetuksen tulkinta ja tuleva ohjeistus

Helluntaikirkon tulisi seurata viranomaisten viestintää tietosuoja-asetuksen soveltamisesta ja päivittää tarvittaessa ohjeistustaan. Erityisesti tulisi seurata JUHTA ja VAHTI -hankkeita ja niiden tuottamaa materiaalia tietosuoja-asetuksesta (Valtionvarainministeriö 2018a, 2018b). Lisäksi tulisi seurata erityisesti Tietosuojavaltuutetun toimiston ohjeistusta (Tietosuoja 2018).

Tietosuojakäytännöstä vastaa Helluntaikirkon hallitus, joka tarkastelee tietosuojan toteutumisen kokonaisuutta vuosittain sekä päivittää ohjeistuksia ja tietosuojaratkaisuja tarvittaessa.

## 7 Yhteenveto, pohdinta ja jatkokehitys

Edellisessä kappaleessa on kerrottu suurin osa asioista, joita ehdotetaan otettavaksi huomioon Helluntaikirkon tietosuojakäytännössä. Tässä kappaleessa pohditaan, kuinka hyvän henkilötietojen tietosuojan saisi jalkautettua jokapäiväiseen toimintaan ja kuinka kehittää prosessia jatkossa. Kriittistä on johdon sitoutuminen valtakunnallisella ja paikallisella tasolla. Tähän auttaa esimerkiksi asian pitäminen esillä helluntailiikkeen yhteisissä tapahtumissa ja liikkeen medioissa. Lisäksi kriittistä on materiaalin ja dokumentaation tuottaminen. Voisi esimerkiksi koota ”Rekisteröidyn oikeudet Helluntaikirkossa” -dokumenttia, jossa olisivat tiedot, jotka tulee toimittaa henkilötietoja kerättäessä. Lisäksi Officen 365 -ympäristön jalkauttaminen ja laaja käyttö jäsenseurakunnissa tarvitsee suunnittelua ja resursseja. Koulutusten pitämistä on myös hyvä jatkaa.

Nykyinen jäsenrekisteriohjelma on toteutettu hieman vanhanaikaisesti, vaikka se onkin nykyisen lainsäädännön mukainen. Jotta se vastaa tulevaisuudenkin tarpeisiin, ehdotetaan koko ohjelman suunnittelemista nykyaikaiselle alustalle siten, että siinä on sähköinen liittymä Maistraattiin ja Väestörekisterikeskukseen, jolloin henkilötietojen käsittely sekä jäsenen liittymis- ja mahdollinen eroamisprosessi seurakunnassa saataisiin digitalisoitua. Liittyvä jäsen voisi tunnistautua pankkitunnusten avulla ja seurakunnan edustaja vahvistaa liittymisen seurakunnan sähköisillä tunnuksilla. Samaan ympäristöön voisi tuoda ratkaisuja jäsenten eli rekisteröityjen oikeuksien toteuttamista varten esimerkiksi mobiilisovelluksen avulla sekä perustaa tietosuoja-asetuksen mukaisia ilmoittautumislomakkeita leiri- ja muuta toimintaa varten siten, että ohjelma varmistaa esimerkiksi huoltajan luvan lasten henkilötietoja käsiteltäessä.

Yhtenä ratkaisuna ehdotetaan tietosuojamallin käyttöönottoa. Kyseessä on maksullinen nettisivusto, joka ohjaa tietosuojaprosessia kysymällä kysymyksiä ja on opastava digityökalu tietosuojan hallintaan. Kun kysymyksiin vastaa järjestelmällisesti, organisaation tietosuojaa parannetaan samalla tehokkaasti. Kyse on ammattilaisten työkalusta, jota pörssi- ja muut yhtiöt käyttävät. Kysymyksiin vastaaminen teettää työtä, mutta on varmasti toimiva työkalu, jos tietosuojaa halutaan parantaa. Helluntaikirkon kokoiselle organisaatiolle käyttöoikeus ohjelmaan maksaa 1330 € + alv vuodessa. (Tietosuojamalli 2018a.)

Yhteenvetona voi todeta, että Helluntaikirkon toimistossa tietosuoja on hoidettu melko hyvin. Jatkon kannalta haasteena ovat resurssit, sillä toimistossa on kokonaisuudessaan vain kaksi työntekijää. Seurakunnissa isoimman henkilörekisterin eli jäsenrekisterin osalta tietosuoja on pääsääntöisesti hoidettu hyvin. Tällöin käytetään suljettua sähköistä järjestelemää, jonka suojauksesta on huolehdittu. Muita henkilötietorekistereitä on pohdittu melko vähän. Tietosuoja-asetus tuo kuitenkin uusia haasteita, joista edellä on kerrottu. Seuraavassa on vielä tiivistetty luettelo asioista, joita ehdotetaan Helluntaikirkolle toimenpiteiksi uuden tietosuoja-asetuksen johdosta (Taulukko 1).

| **Numero** | **Toimenpide-ehdotus** | **Selitys tai perustelu** |
|---|---|---|
| 1 | Toimenpide-ehdotusten hyväksyttäminen yhdyskuntaa sitovaksi hallituksessa ja vuosikokouksessa. | Ehdotetaan tässä opinnäytetyössä esitetyt toimenpiteet toteutettavaksi. Olisi hyvä olla olemassa päätös, että toimenpiteitä voidaan edellyttää. Mikäli yhdyskunnan omistajaseurakunnat vuosikokouksessa tai muussa yhteydessä eivät sitoudu viemään uudistusprosessia läpi, toteutus tuskin onnistuu. |
| 2 | Resurssien hankkiminen | Tietosuoja-asetuksen mukaisia muutoksia ei saada aikaan ilman henkilö- ja muita resursseja. Näiden hankkiminen vapaaehtoisorganisaatiossa voi olla haastavaa, mutta sitäkin kriittisempää. |
| 3 | Valtakunnallisen tietosuojavastaavan nimeäminen Helluntaikirkolle | Tätä tarvitaan, koska organisaatiossa on tuhansia rekisteröityjä, käsitellään tietoa rekisteröidyn uskonnosta sekä käsitellään lasten tietoja.<br><br>Vaihtoehtona tai lisäksi helluntailiike voi halutessaan pohtia helluntaiseurakuntien yhteisille rekisteröidyille yhteisöille yhteisen tietosuojavastaan hankkimista ostopalveluna, jolloin kustannuksia saisi jaettua. |
| 4 | Valtakunnallisen tietosuojavastaavan roolin määrittely | Koska seurakunnat ovat itsenäisiä, järjestelyistä sovittaessa olisi samalla sopimalla määriteltävä tietosuojavastaavan oikeudet päästä perehtymään seurakunnan tietosuojajärjestelyihin tai tarkastamaan niitä. |

| | | |
|---|---|---|
| 5 | Muut tietosuojavastaavat | Yhdyskunnan hallitus voi halutessaan pohtia, haluaako se ohjata tai suositella tietyn kokoisille jäsenseurakunnilleen omien tietosuojavastaavien nimittämistä; esimerkiksi yli 500 jäsenen seurakunnille. |
| 6 | Tietosuojaselosteen luominen | Kappaleessa 6.4 kuvattu uusi tietosuojaseloste olisi hyvä dokumentti rekisteriselostetta laajempana huomioimaan rekisteröityjen oikeudet. |
| 7 | Tukidokumentaation tuottaminen | Dokumentaatiota olisi hyvä olla laajasti. Esimerkiksi:<br><br>a) Helluntaikirkko voisi luoda käytännöllisen ohjeen ja valmiin pohjadokumentin, kuinka jäsenseurakunta voi toteuttaa rekisteröidyn oikeudet paikallistasolla. Siinä kerrotaan, mitä dokumentteja annetaan missäkin vaiheessa, mihin kuuluu pyytää nimi ja lupa sekä milloin dokumentti hävitetään.<br><br>b) Ohjeet ja tarkennukset rekisteriselosteista ja mahdollisesti valmiita esimerkkejä. Esimerkiksi valvontakameran tallenteen muodostama henkilörekisterin rekisteriseloste.<br><br>c) Ohjeita huomioitavista asioista lapsityöhön, hallituksille, vanhimmistoille sekä muille vastuunkantajille. |
| 8 | Varsinaisen tietosuojakäytännön luominen | Tässä opinnäytetyössä on koottuna asioita tietosuojasta. Tietosuojakäytännön luominen tarvitsee erillisen projektin, jossa kootaan Helluntaikirkon oma kirjallinen Tietosuojakäytäntö-dokumentti. Työssä voi käyttää suoraan hyväksi tämän opinnäytetyön kappaleita kuusi ja seitsemän. |
| 9 | Viestintäprosessin suunnittelu ja toteutus | Liikkeen medioita voisi hyödyntää yleisessä tiedottamisessa ja asian esillä pitämisessä. Erilaisia seurakunnille suunnattuja videoita ja muuta tukimateriaalia voisi luoda Usko tv:lle tai Youtube-kanaville. |
| 10 | Koulutusten jatkaminen | Markku Luoman ”rautalankamallia” ja muuta koulutusten pitämistä voisi jatkaa. |

| | | |
|---|---|---|
| 11 | Jalkauttamisprosessi | Helluntaikirkko voisi valita jonkun ottamaan yhteyttä jokaiseen jäsenseurakuntaan erikseen ja varmistaa, että tietosuojaprosessi on aloitettu, tarvittaessa tukea prosessia sekä varmistaa sen vieminen päätökseen. Valtakunnallinen tietosuojavastaava voi muuten ehkä tehdä tämän, mutta hänen tekemänään se ei ole välttämättä kustannustehokkain ratkaisu. |
| 12 | Lisätuen antaminen tarvittaessa | Helluntaikirkko voisi (tarjota itse tai) sopia etukäteen haluamansa tahon kanssa siitä, kuinka tarjota korvausta vastaan tarvittaessa paikan päällä lisäapua seurakunnille. |
| 13 | Office 365 -ympäristön käyttöönotto | Tietoturvallinen kommunikointi valtakunnallisesti ja paikallisesti on mahdollista toteuttaa Microsoftin Nonprofit Office 365 -ympäristön avulla maksutta. Tätä voisi hyödyntää ja halutessaan edellyttää. Tässä isoin työ on luultavasti seurakuntien toimistohenkilökunnan perehdytys, jotta opitaan uusi työtapa. |
| 14 | Tietojenkäsittelysopimus | Ehdotetaan, että tehdään tai tarvittaessa päivitetään Helluntaikirkon ja jäsenseurakuntien välinen tietojenkäsittelysopimus. Koska henkilötietoja käsitellään Helsingin toimistossa sekä jäsenseurakunnissa, roolit olisi hyvä määritellä erillisellä sopimuksella. |
| 14 | Agoran asetuksenmukaisen toiminnan varmistaminen | Jäsenrekisteriohjelma Agoran toimittajalta tulisi pyytää erikseen selvitys ratkaisuista, joilla on varmistettu se, että järjestelmästä varmuudella saadaan mahdollisen tietoturvaloukkauksen sattuessa 72 tunnin kuluessa raportti viranomaisille.<br><br>Lisäksi voi pyytää selvityksen, millä ratkaisuilla kokonaisuudessaan ohjelma on toimittajan mukaan tietosuoja-asetuksen mukainen. |
| 15 | Sopimus tai sen GDPR liite Agoran toimittajan kanssa | Tietosuoja-asetus edellyttää kirjallista sopimusta rekisterinpitäjän eli Helluntaikirkon sekä henkilötietojen käsittelijän eli palveluntarjoajan välillä. |

| | | |
|---|---|---|
| 16 | Agora-järjestelmän uusiminen | Vaikka jäsenrekisteriohjelma Agora on tai olisi lainmukainen, se on jäykkä ja vanhahko käyttää. Helluntaikirkko voisi sidosryhmiltään kartoittaa mahdollisuutta uusia järjestelmä. |
| 17 | Tietotilinpäätöksen tekeminen | Kun tarvittavat toimenpiteet kokonaisuudessaan on tehty, vuosittain voisi tehdä tietotilinpäätöksen, jossa tarkastellaan tehtyjä tietosuojaratkaisuja ja niiden toteutumista. |
| 18 | Tietosuojamalli | Tietosuojamallin opastavan digityökalun käyttö tietosuojan hallintaan auttaa parantamaan tietosuojaa, mutta on ehkä hiukan työläs käyttää. Tämä voisi toimia esimerkiksi tietosuojavastaavan työkaluna. |

Taulukko 1: Ehdotetut toimenpiteet

Lähteet

Sähköiset

Aarnio R. 2017. Johdon ja esimiesten tietosuojakoulutusvideo. Arjen tietosuoja. Viitattu 9.3.2018.
https://vimeo.com/234313084/f874f6b947

Cisco. 2018. Cisco Security Solutions for GDPR. Viitattu 19.3.2018.
https://www.cisco.com/c/dam/en/us/services/collateral/se/security-gdpr-aag.pdf?dtid=osscdc000283

Euroopan parlamentin ja neuvoston asetus 2016/679. Viitattu 19.12.2017
http://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016R0679&qid=1492570626059&from=en

Euroopan parlamentti. 2017. Vuoropuhelu uskonnollisten ja ei-tunnustuksellisten järjestöjen kanssa. Viitattu 19.12.2017.
http://www.europarl.europa.eu/atyourservice/fi/20160919PVL00112/Uskonnollinen-ja-ei-tunnustuksellinen-vuoropuhelu

F-Secure. 2018a. F-Secure Key. Viitattu 12.3.2018.
https://www.f-secure.com/fi_FI/web/home_fi/key

F-Secure. 2018b. F-Secure radar. Viitattu 19.3.2018.
https://www.f-secure.com/fi_FI/web/business_fi/radar

F-Secure 2018c. F-Secure radar. Powerful, Scalable vulnerability management
https://www.f-secure.com/documents/10192/1566545/Radar+brochure/af7a9062-eeca-4287-8714-0600400085cd

Henkilötietolaki 22.4.1999/523. Viitattu 19.10.2017.
http://www.finlex.fi/fi/laki/ajantasa/1999/19990523

IK opisto. 2018. Tietosuojakoulutus. viitattu 19.3.2018.
https://www.ikopisto.fi/tietosuojakoulutus

Laki uskontokuntien jäsenrekistereistä 614/1998. Viitattu 19.10.2017.
http://www.finlex.fi/fi/laki/alkup/1998/19980614

Microsoft. 2018a. Microsoftin tietosuojalauseke. Viitattu 19.3.2018.
https://privacy.microsoft.com/fi-fi/privacystatement

Microsoft 2018b. Missä tietojasi säilytetään? Viitattu 19.3.2018.
https://products.office.com/fi-FI/where-is-your-data-located?ms.officeurl=data-maps&geo=Europe#Europe

Mäntsälän seurakunta. 2013. Rekisteriseloste. Viitattu 13.1.2018.
http://www.mantsalanseurakunta.fi/seurakunta/rekisteriseloste

Oikeusministeriö 2018. Tietosuojalaki täydentäisi EU:n tietosuoja-asetusta. Viitattu 30.3.2018.
http://oikeusministerio.fi/artikkeli/-/asset_publisher/tietosuojalaki-taydentaisi-eu-n-tieto-suoja-asetusta

Oikeusministeriö. 2017. Miten valmistautua EU:n tietosuoja-asetukseen? Viitattu 19.12.2017

http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/1Em8rT7IF/Miten_valmistautua_EUn_tietosuoja-asetukseen.pdf

Pohjannoro, H. Taijala, B. 2007. Näkökulmia toiminnalliseen opinnäytetyöhön. Opettajankoulutuksen kehittämishanke. Tampereen ammattikorkeakoulu. Viitattu 25.4.2018
https://www.theseus.fi/bitstream/handle/10024/8232/Pohjannoro.Hannu.Taijala.Beata.pdf?sequence=2

Tietosuojamalli. 2018a. Viitattu 21.4.2018.
https://www.tietosuojamalli.fi/

Tietosuojamalli. 2018b. Viitattu 21.4.2018.
https://akatemia.tietosuojamalli.fi/artikkeli/yhteenveto-turvallisuuskaytannot

Tietosuojavaltuutetun toimisto. 2018a. Viitattu 22.1.2018.
http://www.tietosuoja.fi/fi/

Tietosuojavaltuutetun toimisto. 2018b. Tietosuojaseloste. Viitattu 16.4.2018.
http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/lomakkeet/rekisteri-jatietosuojaselosteet/wVT4RvRTr/Tietosuojaseloste.pdf

Tietosuojavaltuutetun toimisto. 2014. Rekisteröidyn oikeudet. Viitattu 26.1.2018
http://www.tietosuoja.fi/fi/index/rekisteroidylle.html

Tietosuojavaltuutetun toimisto. 2012. Laadi tietotilinpäätös. Viitattu 16.4.2018.
www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/6JfpzNVCh/Laadi_tietotilinpaatos.pdf

Töyrylä, M. Ylärakkola, J. 2016. Seuraavan sukupolven palomuuri ja sen konfigurointi. Opinnäytetyö. KYAMK. Viitattu 16.4.2018.
https://www.theseus.fi/bitstream/handle/10024/113446/Toyryla_Ylarakkola.pdf?sequence=1&isAllowed=y

Valtionvarainministeriö. 2018a. Tietosuojaa ja tietoturvaa edistetään uusin keinoin – tutustu videokoulutukseen ja nettitestiin. Viitattu 22.1.2018.
http://vm.fi/artikkeli/-/asset_publisher/tietosuojaa-ja-tietoturvaa-edistetaan-uusin-keinoin-tutustu-videokoulutukseen-ja-nettitestiin

Valtionvarainministeriö. 2018b. Yhteishankkeiden materiaalit. Viitattu 22.1.2018.
http://vm.fi/juhta-vahti-yhteishankkeiden-materiaalit

Veritas. 2017. Veritas Introduces New Classification Engine for Intelligent Data Management Across its Portfolio. Viitattu 13.4.2018.
https://www.veritas.com/news-releases/2017-07-25-veritas-introduces-new-classification-engine-for-intelligent-data-management-across-its-portfolio

Yhdistyslaki 26.5.1989/503. Viitattu 30.3.2018.
https://www.finlex.fi/fi/laki/ajantasa/1989/19890503#L1P1

Julkaisemattomat

Juuti, E. 2018. Haastattelu 15.3.2018

Korhonen, H. 2018. Haastattelu 15.3.2018

Koski, J. 2018. Vaitiolositoumus.

Luoma, M. 2018. Tietosuoja-asetuksen toteutus, toimenpiteet seurakunnassa. Rautalanka-malli.

Matikainen, E. 2018. Haastattelu 13.2.2018

Microsoft. 2018a. O365 - GDPR Product Mapping

Microsoft. 2018b. Microsoft protecting.

Microsoft. 2018c. Microsoft – Prepare for the GDPR.

Suomen Helluntaikirkko. 2017. Suomen Helluntaikirkon jäsenrekisterin rekisteriseloste. Päivitetty 5.9.2017.

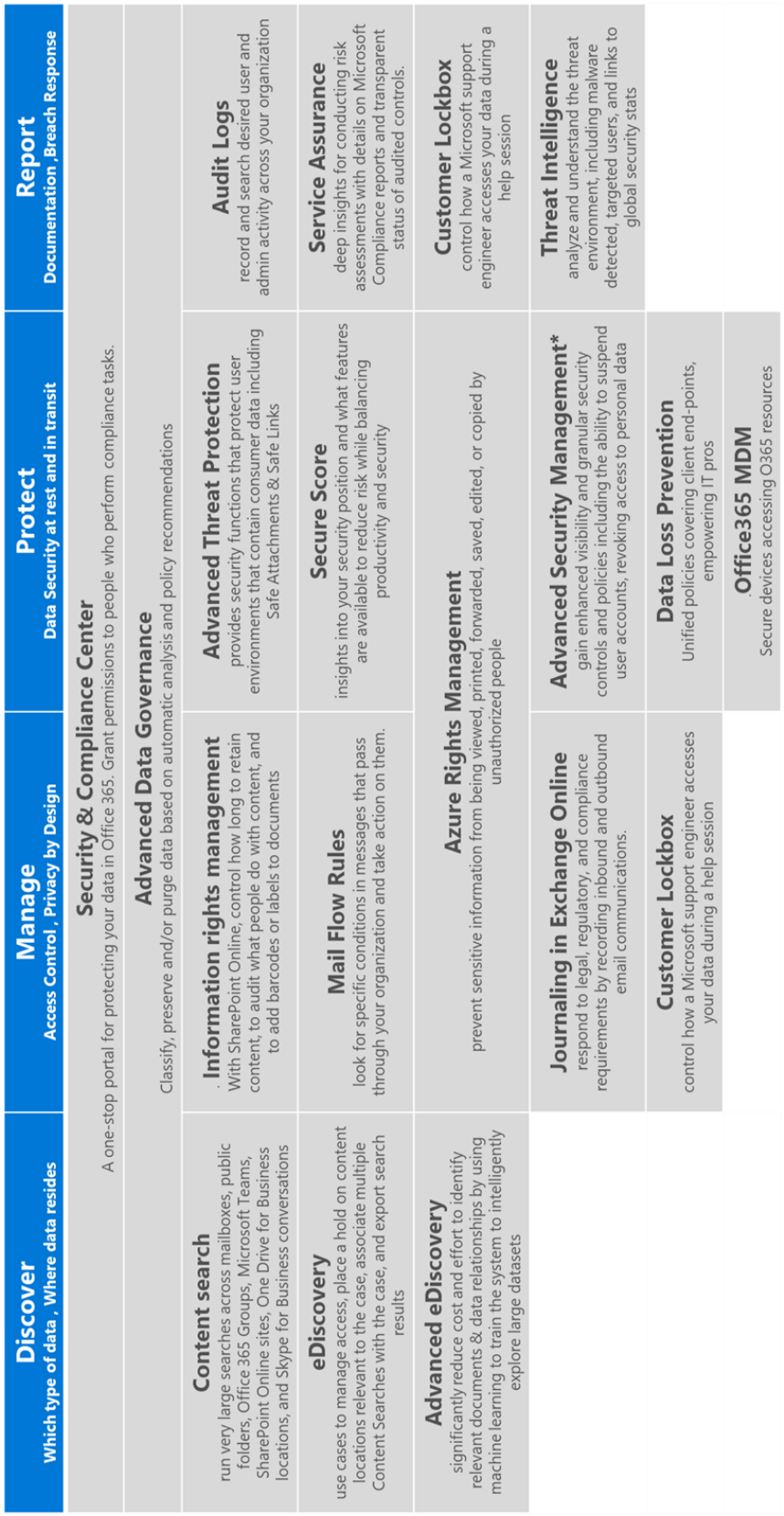
Tietosuojavaltuutetun toimisto. 2018b. Näin kysyt neuvoa tietosuojavaltuutetun toimistolta. Puhelinkeskustelu 12.1.2018
http://tietosuoja.fi/fi/index/yhteystiedot/nainkysytneuvoa.html

Tervo, A. 2018. Tietoturvakoulutus. Fida International. 18.1.2018.

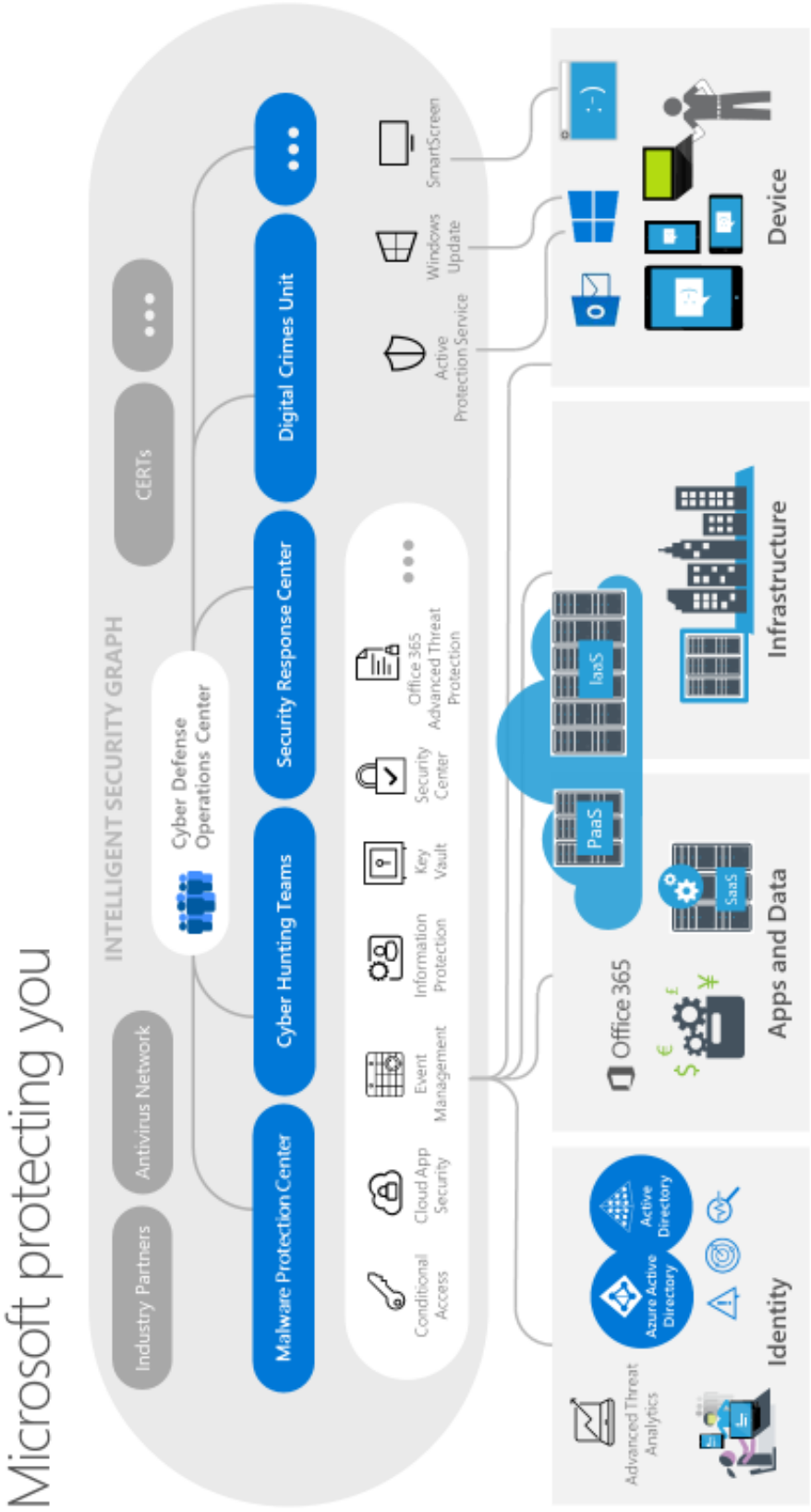
Yrjölä, M. 2018. Haastattelu 7.2.2018

Liitteet

Liite 1: O365 - GDPR Product Mapping (Microsoft 2018c.)



Liite 2: Microsoft Protecting You (Microsoft 2018d.)



Liite 3: Prepare for the GDPR (Microsoft 2018e.)

Liite 4: Haastattelukysymykset

Haastattelukysymykset – aiheena uusi tietosuoja-asetus Helluntaikirkon näkökulmasta

1. Tietosuojavaltuutettu Reijo Aarnio on sanonut, että usein valitettavasti organisaation tietosuojan heikoin lenkki on sen johto. Millainen yleistuntuma sinulla on, miten asian laita on kotiseurakunnassasi, Helluntaikirkon toimistossa ja hallituksessa sekä muissa Helluntaikirkon jäsenseurakunnissa?
    a. Jos heikoin lenkki ei ole johto, mikä mielestäsi on tietosuojan heikoin lenkki Helluntaikirkossa?

2. Helluntaikirkko on päivittämässä tietosuojakäytäntöään. Mitä tietosuojakäytäntöjä Helluntaikirkossa tulisi ainakin olla?
    a. Mitä muita tietosuoja-asioita pidät tärkeänä?
    b. Mitä asioita tietosuojakäytännössä ei tulisi olla?

3. Asetuksessa painotetaan oletusarvoista tietosuojaa, eli sellaista läpileikkaavaa suhtautumista asiaan siten, että kaikissa asioissa sen kaikissa vaiheissa huomioitaisiin tietosuoja. Kuinka oletusarvoinen tietosuoja voisi toteutua Helluntaikirkossa? *(Helluntaikirkko = Helluntaikirkko kokonaisuutena, joka tarkoittaa samaan aikaan omaa kotiseurakuntaa, yhdyskunnan toimistoa ja hallitusta sekä muita jäsenseurakuntia)*

4. Asetuksessa painotetaan myös riskiperusteista lähestymistapaa tietosuojaan. Se tarkoittaa, että tulisi arvioida eri työtapoja henkilötietojen käsittelyssä, ohjelmistoja, työtiloja, avaimia, salasanoja, it-tietoturvaratkaisuja, tietosuojakoulutusta ja -osaamista, valvontaa, tarkistuksia ja auditointeja jne. sen perusteella, millaisia tietoturvariskejä niissä on ja pyrkiä parantamaan tietosuojaa. Kuinka riskiperusteisen lähestymistavan tietosuojaan voisi käytännössä toteuttaa Helluntaikirkossa?

5. Miten osoitusvelvollisuuden voisi käytännössä toteuttaa Helluntaikirkossa?

6. Kuinka rekisteröityjen (seurakuntalaisten) oikeudet voisivat toteutua Helluntaikirkossa? (*Oikeus saada läpinäkyvää informaatiota henkilötietojen käsittelystä, oikeus saada pääsy tietoihin, oikeus tietojen oikaisemiseen ja oikeus tulla unohdetuksi, oikeus käsittelyn rajoittamiseen ja rekisterinpitäjän (seurakunnan) velvollisuus ilmoittaa rajoituksesta, oikeus siirtää tiedot järjestelmästä toiseen, Vastustamisoikeus, automatisoitujen yksittäispäätösten ja profiloinnin liittyvät oikeudet)*

7. Pitäisikö Helluntaikirkossa ja/tai jäsenseurakunnassa olla tietosuojavastaava? Kuka?

8. Kuinka varmistutaan siitä, että seurakuntien henkilötietoja käsittelevät henkilöt tekevät työnsä tietosuoja-asetuksen mukaisesti? Kenen vastuulla on toteuttaa ratkaisu?

9. Mitä pitäisi tehdä, jotta Helluntaikirkossa valtakunnallisesti aidosti toteutuisi hyvä henkilötietojen tietosuoja?

10. Mitä muuta haluaisit sanoa? (tietosuojasta, Helluntaikirkon tietosuojakäytännöstä tai jostain muusta asiasta)

Liite 5: Rekisteriseloste

**REKISTERISELOSTE**
**Henkilötietolaki (523/1999) 10 §**

Lue täyttöohjeet ennen rekisteriselosteen täyttämistä. Käytä tarvittaessa liitettä.

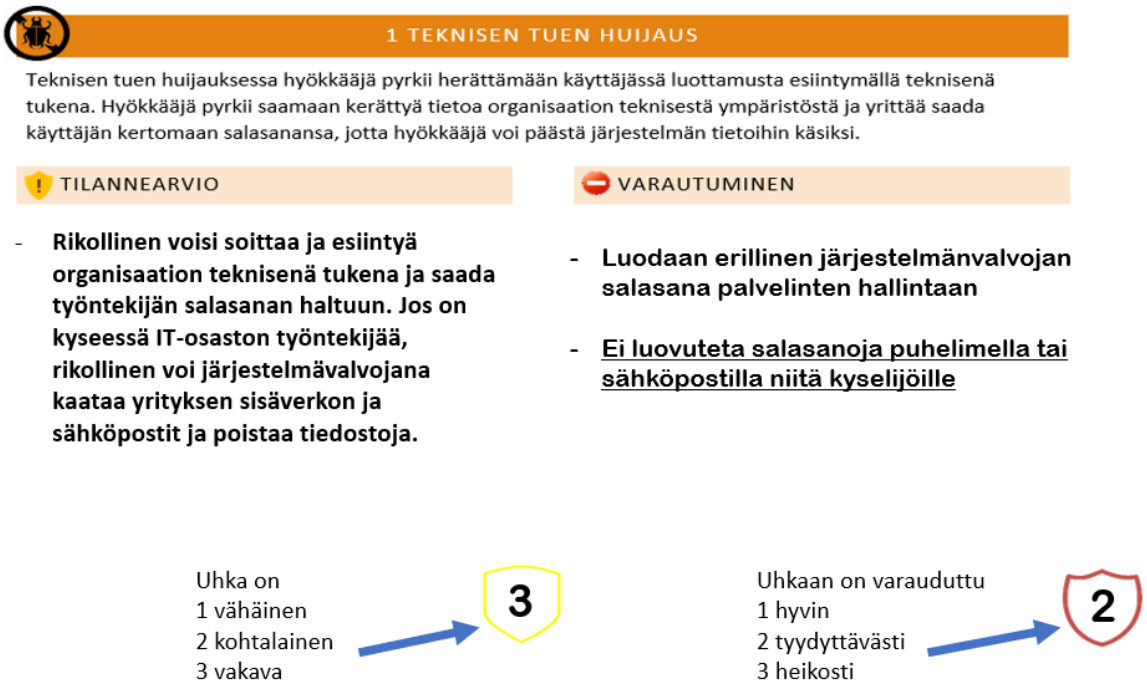
Laatimispäivä
18.1.2018

| | |
|---|---|
| **1 Rekisterinpitäjä** | Nimi<br>Suomen Helluntaikirkko |
| | Osoite<br>Tulppatie 20, 00880 Helsinki |
| | Muut yhteystiedot (esim. puhelinvaihde-aikana, sähköpostiosoite)<br>Puh. 045-6327848, toimisto@helluntaikirkko.fi |
| **2 Yhteyshenkilö rekisteriä koskevissa asioissa** | Nimi<br>Esko Matikainen |
| | Osoite<br>Tulppatie 20, 00880 Helsinki |
| | Muut yhteystiedot (esim. puhelinvaihde-aikana, sähköpostiosoite)<br>Puh. 050-3251918, esko.matikainen@helluntaikirkko.fi |
| **3 Rekisterin nimi** | Suomen Helluntaikirkon henkilörekisterin rekisteriseloste |
| **4 Henkilötietojen käsittelyn tarkoitus** | Henkilötietoja käytetään Suomen Helluntaikirkon yhdyskuntajärjestyksessä määritellyn toiminnan järjestämiseksi.<br><br>Yhdyskuntajärjestyksen mukaan: "Yhdyskunta ja sen seurakunnat voivat järjestää jumalanpalvelus- ja julistustilaisuuksia ja muita tilaisuuksia, kuten juhlia, kokouksia, konsertteja ja koulutustilaisuuksia, Yhdyskunta ja sen seurakunnat voivat harjoittaa koulutus- ja julkaisutoimintaa, levittää painotuotteita ja äänitteitä, harjoittaa radio- ja TV-toimintaa ja sähköistä tiedonvälitystä, harjoittaa sosiaalista avustustoimintaa, lähetys- ja kehitysaputyötä sekä muuta aatteellista toimintaa sanomansa levittämiseksi." |
| **5 Rekisterin tietosisältö** | Sukunimi ja etunimet; henkilötunnus tai syntymäaika; osoite ja kotikunta; uskontokuntaan liittymisajankohta; uskontokunnasta eroamisajankohta; uskontokunnan jäsenen syntymäkotikunta; kansalaisuus ja äidinkieli; uskontokunnan jäsenen seurakunnasta toiseen siirtymisen ajankohta; tiedot uskontokunnan jäsenen siviilisäädystä, perheoikeudellisesta asemasta ja toimivaltaisuudesta; uskontokunnan jäsenen puolison nimi ja henkilötunnus tai syntymäaika; uskontokunnan jäsenen huollossa olevan alaikäisen lapsen nimi ja henkilötunnus tai syntymäaika; uskontokunnan jäsenen kastetta, vihkimistä, hautaamista tai muuta vastaavaa toimitusta koskevat tiedot; uskontokunnan jäsenen uskontokuntaan liittyvää luottamustehtävää tai siihen verrattavaa tehtävää koskevat tiedot. |
| **6 Säännönmukaiset tietolähteet** | Henkilörekisterin tiedot päivitetään väestötietojärjestelmästä sekä henkilörekisteriohjelma Agoran Helluntaikirkkoon rekisteröityjen henkilöiden tietokannasta. |

**REKISTERISELOSTE** 2

| | |
|---|---|
| **7 Tietojen säännönmukaiset luovutukset** | Henkilörekisterin tietoja ei luovuteta ulkopuolisille. |
| **8 Tietojen siirto EU:n tai ETA:n ulkopuolelle** | Tietoja ei luovuteta tai siirretä EU:n tai ETA-alueen ulkopuolelle. |
| **9 Rekisterin suojauksen periaatteet** | A Manuaalinen aineisto<br>Manuaalinen aineisto säilytetään lukitussa tilassa.<br><br>B ATK:lla käsiteltävät tiedot<br>Tietoja käsitteleviä työntekijöitä koskee vaitiolovelvollisuus, joka jatkuu palvelussuhteen päätyttyä. Sähköisen rekisterin käyttöön tarvitaan henkilökohtainen käyttäjätunnus ja salasana ja niiden käyttöä valvotaan. Käyttöoikeudet rekistereihin myönnetään tehtäväkohtaisesti. Ulkoista yhteyttä valvotaan palomuurein ja palvelinlaitteistoa ylläpidetään hyvän ylläpitotavan mukaisesti. |

Liite 6: Riskiarviointi (Tervo 2018.)




Liite 7: Järjestelmän tietoturvakortti (Tervo 2018.)

Liite 8: Vaitiolositoumus

## SALASSAPITO- JA VAITIOLOSITOUMUS

_____ -seurakunnan jäsenten sekä toiminnassa mukana olevien henkilöiden (asiakkaiden) tiedot ovat salassa pidettäviä Henkilötietolain sekä Euroopan Unionin Tietosuoja-asetuksen perusteella.

Seurakunnassa tai sen tiloissa palkattuna tai vapaaehtoisena työskentelevä henkilö on salassapito- ja vaitiolovelvollinen Henkilötietolain 33 § sekä Tietosuoja-asetuksen 28 § 3b momentin perusteella. Hän ei saa paljastaa asiakirjan salassa pidettävää sisältöä tai tietoa, joka asiakirjaan merkittynä olisi salassa pidettävä, eikä muutakaan seurakunnassa toimiessaan tietoonsa saamaa seikkaa, josta lailla on säädetty vaitiolovelvollisuus. Vaitiolovelvollisuuden piiriin kuuluvaa tietoa ei saa paljastaa senkään jälkeen, kun toiminta seurakunnassa on päättynyt.

Toimiessani seurakunnassa sitoudun ylläpitämään ja käsittelemään asiakirjoja, tietoja, laitteita, valokuvia, piirustuksia, tiedonsiirtovälineitä ja muita salassa pidettäviä tietoja siten, etteivät ne joudu oikeudettomasti ulkopuolisten haltuun, tutkittavaksi tai tietoon. Sitoudun käyttämään tietojärjestelmiä, joihin minulle on annettu käyttöoikeus, pelkästään työtehtävien hoitamiseksi enkä tee hakuja niihin missään muussa tarkoituksessa kuin yksittäisen minulle kuuluvan työtehtävän hoitamista varten. Sitoudun myös siihen, etten käyttäydy työ- enkä vapaa-aikana tavalla, joka heikentää minun tai muiden työntekijöiden mahdollisuuksia hoitaa työtä häiriöittä, tai joka vaikuttaa seurakunnan toimintamahdollisuuksiin. Salassapitovelvollisuuteni on voimassa senkin jälkeen, kun en enää ole seurakunnan palveluksessa tai työskentele seurakunnan tiloissa.

Olen velvollinen ilmoittamaan esimiehelleni tai vapaaehtoistyön johtajalle potentiaalisen tietoturvariskin sisältävästä toimesta, yhteydenotosta tai muusta tietoturvallisuutta vaarantavasta seikasta.

Salassa pidettävien asiakirjojen ja luottamuksellisten tietojen jäljentäminen, tallentaminen tai siihen verrattava toiminta muussa laajuudessa kuin palvelussuhteeni perusteella on ehdottomasti kielletty.

Minulle on kerrottu seurakunnassa käsiteltävien asioiden, asiakirjojen ja toiminnassa mukana olevien tietojen salassa pidosta ja olen ymmärtänyt, että minua koskee salassapito- ja vaitiolovelvollisuus ja sitoudun yllä mainittuihin seikkoihin.

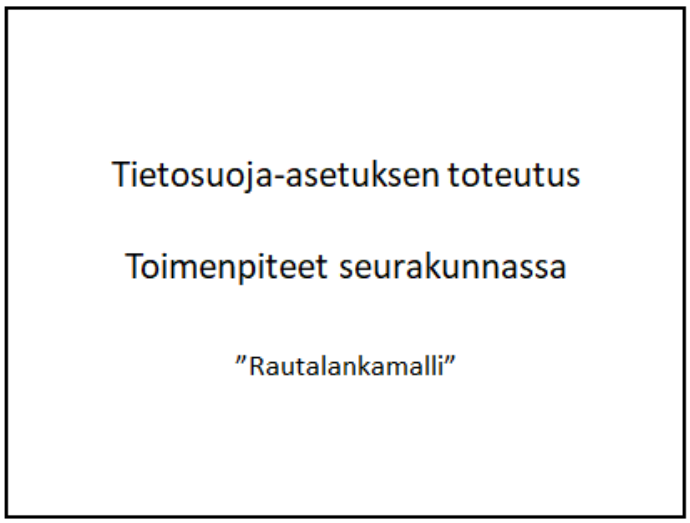
Henkilötietojen käsittelijänä sitoudun noudattamaan tietosuoja-asetusta sekä rekisterinpitäjän ohjeita.

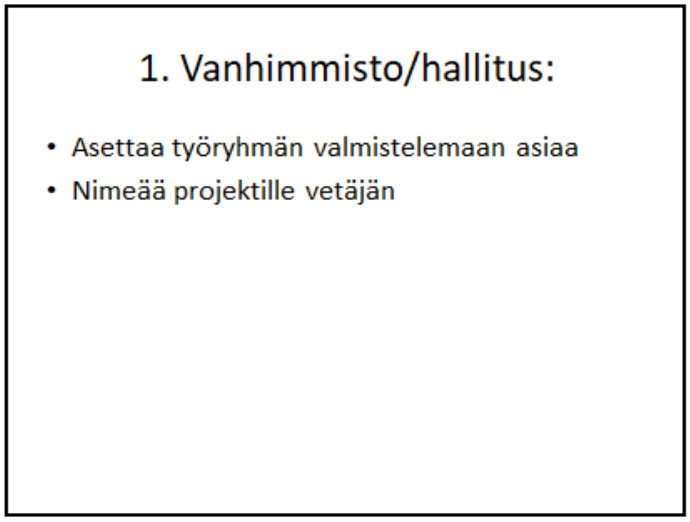
Paikka ja päiväys Allekirjoitus ja nimen selvennys

_____

Sitoumus annetaan kahtena kappaleena, joista toinen jää työntekijälle/vapaaehtoiselle ja toinen seurakunnalle

Liite 9: Rautalankamalli (Luoma 2018.)



## 2. Työryhmä

- Kartoittaa nykyiset henkilörekisterit
- Kartoittaa henkilörekisterien tietosisällöt
- Kokoaa/toteaa nykyisen dokumentaation ja ohjeistot
- Suunnittelee henkilörekisterien tietosisällöt
- Suunnittelee tarvittavat tietoturvallisuustoimenpiteet
- Suunnittelee toimenpiteet rekisteröityjen pyyntöihin vastaamiseksi
- Laatii (päivittää) dokumentit
  - Rekisteriselosteet
  - Tietosuojakäytännöt
  - Ohjeet henkilökunnalle
  - Lomakkeet
- Esittää henkilön tietosuojavastaavaksi tai vastuuhenkilöksi
- Esittää nimettävät henkilötietojen käsittelijät

## 3. Vanhimmisto/hallitus

- Käsittelee työryhmän esityksen
- Hyväksyy/vahvistaa työryhmän laatimat dokumentit
- Nimeää tietosuojavastaavan tai vastuuhenkilön
- Nimeää henkilötietojen käsittelijät
- Päättää muista tarvittavista toimenpiteistä

## 4. Tietosuojavastaava tai vastuuhenkilö

- Vastaa sovittujen toimenpiteiden toteuttamisesta
- Huolehtii tietosuojan ylläpitämisestä
- Raportoi vanhimmistolle/hallitukselle
- Tekee tarvittavat ilmoitukset tietosuojaviranomaiselle

Liite 10: Tietojenkäsittelyyn liittyviä erityistilanteita koskevat säännökset

EU:n jäsenvaltioiden on lainsäädännöllä sovitettava yhteen tietosuoja-asetuksen mukainen oikeus henkilötietojen suojaan sekä oikeus sananvapauteen ja tiedonvälityksen vapauteen, mukaan lukien käsittely journalistisia tarkoituksia ja akateemisen, taiteellisen tai kirjallisen ilmaisun tarkoituksia varten. Jäsenvaltioiden tulee säätää käsittelylle vapautuksia tai poikkeuksia periaatteisiin, rekisteröidyn oikeuksiin, rekisterinpitäjään ja henkilötietojen käsittelijään, henkilötietojen siirtoon kolmansiin maihin tai kansainvälisille järjestöille, riippumattomiin valvontaviranomaisiin, yhteistyöhön ja yhdenmukaisuuteen sekä tietojenkäsittelyyn liittyvien erityistilanteiden säännöksiin, jos ne ovat tarpeen henkilötietojen suojaa koskevan oikeuden sovittamiseksi yhteen sananvapauden ja tiedonvälityksen vapauden kanssa. (85 Artikla.) Jäsenvaltiot voivat määritellä tarkemmin kansallisen henkilönumeron tai muun yleisen tunnisteen käsittelyn edellytykset. Kansallista henkilönumeroa tai muuta yleistä tunnistetta tulee käyttää ainoastaan noudattaen rekisteröidyn oikeuksia ja vapauksia koskevia asianmukaisia suojatoimia tietosuoja-asetuksen mukaisesti. (87 Artikla.)

EU:n jäsenvaltiot voivat lakisääteisesti tai työehtosopimuksilla antaa yksityiskohtaisempia sääntöjä työntekijöiden henkilötietojen käsittelystä työsuhteen yhteydessä oikeuksien ja vapauksien suojan varmistamiseksi, erityisesti palvelukseen ottamista tai työsopimuksen täytäntöönpanoa varten. Tähän kuuluu myös lakisääteisten tai työehtosopimukseen perustuvien velvollisuuksien suorittaminen, työn johto, suunnittelu ja organisointi, yhdenvertaisuus ja monimuotoisuus työpaikalla, työterveys ja -turvallisuus, työnantajan tai asiakkaan omaisuuden suoja, sekä työntekoon liittyvien oikeuksien ja etuuksien yksilöllistä tai kollektiivista käyttöä sekä työsuhteen päättämistä varten. Näihin sääntöihin tulee sisällyttää asianmukaisia toimenpiteitä rekisteröidyn ihmisarvon, oikeutettujen etujen ja perusoikeuksien suojaamiseksi siten, että erityistä huomiota kiinnitetään tietojenkäsittelyn läpinäkyvyyteen, henkilötietojen siirtoihin saman konsernin tai yritysryhmän sisällä ja työpaikalla käytössä oleviin valvontajärjestelmiin. (88 Artikla.)

Yleisen edun mukaisia arkistointitarkoituksia tai tieteellisiä ja historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten tapahtuvaan käsittelyyn tulee soveltaa asianmukaisia suojatoimia tietosuoja-asetuksen mukaisesti. Näillä suojatoimilla tulee varmistaa tekniset ja organisatoriset toimenpiteet, joilla taataan varsinkin tietojen minimoinnin periaatteen noudattaminen. Tällä tarkoitetaan esimerkiksi pseudonymisointia, jos tarkoitus voidaan täyttää tällä tavoin. Jos nämä tarkoitukset voidaan täyttää käsittelemällä myöhemmin tietoja, minkä johdosta ei ole - tai ei enää ole mahdollista tunnistaa rekisteröityjä, nämä tarkoitukset tulee täyttää tällä tavoin. (89 Artikla.)

Jos EU:n jäsenvaltion kirkot ja uskonnolliset yhdistykset tai yhdyskunnat soveltavat tietosuoja-asetuksen tullessa voimaan kattavia sääntöjä, jotka koskevat henkilöiden suojaamista

henkilötietojen käsittelyssä, näitä sääntöjä voidaan soveltaa edelleen, jos ne saatetaan tietosuoja-asetuksen mukaisiksi. Kattavia sääntöjä soveltavat kirkot ja uskonnolliset yhdistykset ovat sellaisen riippumattoman valvontaviranomaisen valvonnassa, joka voi olla erityisviranomainen edellyttäen, että se täyttää tietosuoja-asetuksen riippumattoman valvontaviranomaisen edellytykset. (91 Artikla.)

Liite 11: Oikeus siirtää tiedot järjestelmästä toiseen, vastustamisoikeus sekä profilointi

Rekisteröidyllä on oikeus saada rekisterinpitäjälle toimittamansa henkilötiedot jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa ja oikeus siirtää kyseiset tiedot toiselle rekisterinpitäjälle, jos käsittely perustuu suostumukseen tai sopimukseen ja käsittely suoritetaan automaattisesti. Jos rekisteröity käyttää oikeuttaan siirtää tiedot järjestelmästä toiseen, hänellä on oikeus saada henkilötiedot siirrettyä suoraan rekisterinpitäjältä toiselle, jos se on teknisesti mahdollista. Tätä oikeutta ei sovelleta käsittelyyn, joka on tarpeen yleistä etua koskevan tehtävän suorittamista tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämistä varten. Oikeus ei saa vaikuttaa haitallisesti muiden oikeuksiin ja vapauksiin. (20 Artikla.)

Jos henkilötietoja käsitellään suoramarkkinointia varten, rekisteröidyllä on oikeus vastustaa henkilötietojen käsittelyä tätä tarkoitusta varten, mukaan lukien profilointia suoramarkkinointitarkoituksiin. Jos rekisteröity vastustaa suoramarkkinointiin liittyvän henkilötietojen käsittelyä, niitä ei saa enää käsitellä. Viimeistään silloin, kun rekisteröityyn ollaan yhteydessä ensimmäisen kerran, vastustamisoikeus on nimenomaisesti saatettava rekisteröidyn tietoon ja esitettävä selkeästi ja muusta tiedotuksesta erillään. Jos henkilötietoja käsitellään tieteellisiä tai historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten, rekisteröidyllä on oikeus henkilökohtaiseen tilanteeseensa liittyvällä perusteella vastustaa häntä itseään koskevien henkilötietojen käsittelyä, paitsi jos käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi. (21 Artikla).

Rekisteröidyllä on oikeus välttyä joutumasta pelkästään automaattisen käsittelyn kohteeksi, kuten profilointiin, kun käsittelyllä on häntä koskevia oikeusvaikutuksia tai joka vaikuttaa häneen vastaavalla merkittävällä tavalla. Edellä olevaa ei sovelleta, jos päätös on välttämätön rekisteröidyn ja rekisterinpitäjän välisen sopimuksen tekemistä tai täytäntöönpanoa varten. Lisäksi edellä olevaa ei sovelleta, jos asia on hyväksytty lainsäädännössä, jossa vahvistetaan myös asianmukaiset toimenpiteet rekisteröidyn oikeuksien ja vapauksien sekä oikeutettujen etujen suojaamiseksi tai jos se perustuu rekisteröidyn nimenomaiseen suostumukseen. Rekisterinpitäjän on toteutettava asianmukaiset toimenpiteet rekisteröidyn oikeuksien ja vapauksien sekä oikeutettujen etujen suojaamiseksi. Tämä koskee vähintään oikeutta vaatia tietojen käsittelijäksi luonnollista henkilöä sekä oikeutta esittää kantansa ja riitauttaa päätös. Edellä tarkoitetut päätökset eivät saa perustua erityisiin henkilötietoryhmiin ja tietoihin, joita ovat mm. uskonnollinen vakaumus, rotu tai etninen alkuperä tai poliittiset mielipiteet, paitsi jos rekisteröity on antanut suostumuksensa, tai käsittely on tarpeen yleisen edun vuoksi lainsäädännön nojalla ja asianmukaiset toimenpiteet rekisteröidyn oikeuksien ja vapauksien sekä oikeutettujen etujen suojaamiseksi on toteutettu. (22 Artikla). Käytännössä artiklassa on kyse

esimerkiksi siitä, että jos automaattisesti käsiteltyyn sähköiseen lainahakemukseen tulee kielteinen päätös, henkilöllä on oikeus riitauttaa asia ja vaatia luonnollista henkilöä käsittelemään hakemus.

Liite 12. Tarkennuksia henkilötietojen käsittelijän toimintaan

Jos henkilötietojen käsittelijä käyttää toisen henkilötietojen käsittelijän palveluksia, kyseiseen toiseen henkilötietojen käsittelijään sovelletaan samoja tietosuojavelvoitteita kuin ne, jotka on vahvistettu rekisterinpitäjän ja henkilötietojen käsittelijän välisessä sopimuksessa tai muussa oikeudellisessa asiakirjassa. Jos toinen henkilötietojen käsittelijä ei täytä tietosuojavelvoitteitaan, alkuperäinen henkilötietojen käsittelijä on edelleen täysimääräisesti vastuussa toisen henkilötietojen käsittelijän velvoitteiden suorittamisesta suhteessa rekisterinpitäjään. (28 Artikla.)

Henkilötietojen käsittelijän on toteutettava riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet. Näitä ovat henkilötietojen pseudonymisointi ja salaus, kyky taata käsittelyjärjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus, kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa sekä menettely, jolla testataan, tutkitaan ja arvioidaan säännöllisesti teknisten ja organisatoristen toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi. Asianmukaisen turvallisuustason arvioimisessa on huomioitava käsittelyn riskit, erityisesti siirrettyjen, tallennettujen tai muutoin käsiteltyjen henkilötietojen vahingossa tapahtuvan tai laittoman tuhoamisen, häviämisen, muuttamisen, luvattoman luovuttamisen tai henkilötietoihin pääsyn vuoksi. (32 Artikla.)

Jos tietoturvaloukkauksen tapahtuessa tietoja ei voida toimittaa samanaikaisesti, tiedot voidaan toimittaa vaiheittain ilman aiheetonta viivytystä. Rekisterinpitäjän tulee dokumentoitava kaikki henkilötietojen tietoturvaloukkaukset, sisältäen siihen liittyvät seikat, vaikutukset ja korjaavat toimet. Valvontaviranomaisen tulee kyetä dokumentoinnin avulla tarkistamaan tietoturvaloukkaukset. (33 Artikla.)

Kun henkilötietojen tietoturvaloukkaus todennäköisesti aiheuttaa korkean riskin henkilöiden oikeuksille ja vapauksille, rekisterinpitäjän tulee ilmoittaa tietoturvaloukkauksesta rekisteröidylle ilman aiheetonta viivytystä. Ilmoituksessa kuvataan selkeästi tietoturvaloukkauksen luonne, kerrotaan tietosuojavastaavan nimi ja yhteystiedot tai muu yhteyspiste, josta voi saada lisätietoa, kuvataan todennäköiset seuraukset sekä toimenpiteet, joita rekisterinpitäjä on ehdottanut tai jotka se on toteuttanut tapahtuman johdosta ja/tai sen haittavaikutusten lieventämiseksi. Ilmoitusta ei tarvitse tehdä, jos rekisterinpitäjä on toteuttanut asianmukaiset tekniset ja organisatoriset suojatoimenpiteet, kuten salauksen, tai jos rekisterinpitäjä on toteuttanut varmistavia jatkotoimenpiteitä joiden johdosta riski edelliseen ei enää todennäköisesti toteudu tai jos se vaatisi kohtuutonta vaivaa. Tällaisissa tapauksissa on käytettävä julkista tiedonantoa tai vastaavaa toimenpidettä, jolla rekisteröidyille tiedotetaan yhtä tehokkaalla tavalla. (34 Artikla.)

Jos tietyntyyppinen käsittely etenkin uutta teknologiaa käytettäessä todennäköisesti aiheuttaa henkilön oikeuksien ja vapauksien kannalta korkean riskin, rekisterinpitäjän tulee ennen käsittelyä toteutettava arviointi käsittelytoimien vaikutuksista henkilötietojen suojalle. Yhtä arviota voidaan käyttää samankaltaisiin vastaavia korkeita riskejä aiheuttaviin käsittelytoimiin. (35 Artikla.) Rekisterinpitäjän tulee ennen käsittelyä kuulla valvontaviranomaista, jos vaikutustenarviointi osoittaa käsittelyn aiheuttavan korkean riskin ja jos rekisterinpitäjä ei ole toteuttanut asianmukaisia toimenpiteitä riskin pienentämiseksi. (36 Artikla.)

Liite 13: Henkilötietojen siirrot kolmansiin maihin tai kansainvälisille järjestöille sekä riippumattomat valvontaviranomaiset

Sellaisten henkilötietojen siirto, joita käsitellään tai joita on tarkoitus käsitellä kolmanteen maahan tai kansainväliselle järjestölle siirtämisen jälkeen, toteutetaan vain, jos rekisterinpitäjä ja henkilötietojen käsittelijä varmistavat tietosuojan toteutumisen tietosuoja-asetuksen artiklan 44-50 mukaisesti. Tämä koskee myös henkilötietojen siirtämistä edelleen kyseisestä kolmannesta maasta tai kansainvälisestä järjestöstä toiseen kolmanteen maahan tai toiselle kansainväliselle järjestölle. Kaikkia henkilötiedon siirron säännöksiä on sovellettava, jotta varmistetaan, ettei tietosuoja-asetuksen mukaisen henkilötietojen suojan tasoa vaaranneta. (44 Artikla.)

EU:n jäsenvaltioiden on varmistettava, että niiden valvontaviranomaisten kaikki jäsenet nimitetään läpinäkyvää menettelyä noudattaen. Nimittäjänä toimii parlamentti, hallitus, valtionpäämies tai riippumaton elin, jolle nimittäminen lainsäädännön perusteella on siirretty. Kullakin jäsenellä on oltava tehtävien hoitamisessa ja valtuuksien käyttämisessä tarvittava pätevyys, kokemus ja ammattitaito erityisesti henkilötietojen suojaamisen alalta. Jäsenen tehtävät päättyvät toimikauden päättyessä tai kun hän eroaa tai kun hän jää pakolliselle eläkkeelle jäsenvaltion lainsäädännön mukaisesti. Jäsen voidaan erottaa ainoastaan vakavan väärinkäytöksen perusteella tai jos hän ei enää täytä tehtäviensä suorittamiseen tarvittavia edellytyksiä. (53 Artikla.)