SUOMEN EV.LUT. KIRKKO
EV.LUTH. KYRKAN I FINLAND
Kirkkohallitus
Kyrkostyrelsen

Kirkkohallituksen yleiskirje nro 6/2017

27.2.2017

VARAUTUMINEN EUROOPAN UNIONIN YLEISEEN TIETOSUOJA-ASETUKSEEN

Euroopan unionin henkilötietojen käsittelyä sääntelevä yleinen tietosuoja-asetus (EU 2016/679) tulee sovellettavaksi 25.5.2018 lukien. Asetus tulee sovellettavaksi sekä julkisella että yksityisellä sektorilla, ja se korvaa vuoden 1995 henkilötietodirektiivin sekä sen kansalliseksi täytäntöön panemiseksi annetun henkilötietolain (523/1999) säännökset niiltä osin kuin henkilötietojen käsittely kuuluu asetuksen soveltamisalaan.

Vaikka kyseessä on kansallisesti suoraan sovellettava asetus, se jättää jäsenvaltioille jonkin verran liikkumavaraa. Asetuksen puitteissa on mahdollista antaa kansallista lainsäädäntöä, jolla tarkennetaan asetuksen säännöksiä tai mahdollisesti jossain määrin myös poiketaan asetuksen velvoitteista. Oikeusministeriö asetti helmikuussa 2016 työryhmän selvittämään Euroopan unionin tietosuoja-asetuksen edellyttämien kansallisten lainsäädäntötoimenpiteiden tarvetta. Mahdollisen esityksen henkilötietolainsäädännön muuttamiseksi arvioidaan valmistuvan vuoden 2017 loppukeväällä.

Asetus on tuomassa rekisterinpitäjille uusia hallinnollisia tehtäviä, joihin on syytä varautua hyvissä ajoin. Tässä yleiskirjeessä kuvataan asetuksen keskeisiä seikkoja. Asetus on kokonaisuudessaan luettavissa sähköisenä osoitteessa:
http://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=OJ:L:2016:119:FULL&from=FI

Tietosuoja-asetuksen soveltamisala ja keskeisimmät määritelmät

Tietosuoja-asetusta sovelletaan henkilötietojen käsittelyyn, joka on osittain tai kokonaan automaattista, sekä sellaisten muutoin kuin automaattisesti käsiteltävien henkilötietojen käsittelyyn, jotka muodostavat tai joiden on tarkoitus muodostaa rekisterin osa. Luonnollisen henkilön yksinomaan henkilökohtaisessa toiminnassa tapahtuva henkilötietojen käsittely jää asetuksen soveltamisalan ulkopuolelle.

Keskeisimmät määritelmät:

Henkilötieto	Kaikki tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyvät tiedot (esim. nimi, henkilötunnus, kuva, sijaintitiedot, verkkotunnistetiedot tai henkilölle tunnusomaiset taloudelliset ja kulttuuriset tekijät).
Henkilötietojen erityiset tietoryhmät (arkaluontoiset henkilötiedot)	Tiedot, joista ilmenee rotu tai etninen alkuperä, poliittisia mielipiteitä, uskonnollinen tai filosofinen vakaumus, ammattiliiton jäsenyys, geneettisiä tietoja, terveyttä koskevia tietoja tai seksuaaliseen käyttäytymiseen ja suuntautumiseen liittyviä tietoja. Erityisiä tietoryhmiä koskeva käsittely on erikseen säänneltyä.
Henkilötietojen käsittely	Toiminnot, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti: tietojen kerääminen, tallentaminen, järjestäminen, jäsentäminen, säilyttäminen, muokkaaminen tai muuttaminen, hakeminen, kyselyjen tekeminen, käyttäminen, tietojen luovuttaminen siirtämällä, levittämällä tai asettamalla ne

	muutoin saataville, tietojen yhteensovittaminen tai yhdistäminen, rajoittaminen, poistaminen ja tuhoaminen. Alle 16-vuotiaan lapsen henkilötietojen käsittely ei ole sallittua ilman vanhemman/huoltajan suostumusta. Jäsenvaltiolla on mahdollisuus soveltaa alempaa ikärajaa, joka voi olla alimmillaan 13 vuotta.
Henkilötietojen käsittelijä	Luonnollinen henkilö, viranomainen, virasto tai muu elin, joka käsittelee henkilötietoja rekisterinpitäjän toimeksiannosta.
Rekisteri	Mikä tahansa jäsenneltyjä henkilötietoja sisältävä tietojoukko, josta tiedot ovat saatavilla tietyin perustein, oli tietojoukko sitten keskitetty, hajautettu tai toiminnallisin tai maantieteellisin perustein jaettu.
Rekisterinpitäjä	Luonnollinen henkilö tai oikeushenkilö, julkinen viranomainen, virasto tai muu elin, joka yksin tai yhteistyössä muiden kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Jos käsittelyn tarkoitus ja keinot määritellään lainsäädännössä, myös rekisterinpitäjä voidaan määritellä laissa.
Rekisteröity	Henkilö, jonka henkilötietoja käsitellään.
Rekisteröidyn suostumus	Mikä tahansa vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen tahdonilmaisu, jolla rekisteröity hyväksyy henkilötietojen käsittelyn antamalla suostumusta ilmaisevan lausuman tai toteuttamalla selkeästi suostumusta ilmaisevan toimen. Jos tietojen käsittely perustuu suostumukseen, rekisterinpitäjän on pystyttävä osoittamaan, että rekisteröity on antanut suostumuksen henkilötietojen käsittelyyn.
Kolmas osapuoli, sivullinen	Muu luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin kuin rekisteröity, rekisterinpitäjä, henkilötietojen käsittelijä tai henkilö, jolla on oikeus käsitellä henkilötietoja suoraan rekisterinpitäjän tai henkilötietojen käsittelijän välittömän vastuun alaisena.
Rekisteriseloste, tietosuojaseloste	Asiakirja, joka rekisterinpitäjän tulee laatia ja pitää yleisesti saatavilla. Sen tulee kuvata henkilötietojen käsittely tiiviisti esitetyssä, avoimessa ja helposti ymmärrettävässä muodossa.
Tietosuoja ja tietoturvallisuus	Tietosuoja on yksityisyyden suojaamista henkilötietoja käsiteltäessä. Tietoturvallisuus tarkoittaa tiedon luottamuksellisuuden, eheyden ja saatavuuden takaamista teknisten ja organisatoristen toimenpiteiden ja menettelyjen avulla.
Tietosuojavastaava	Viranomaisen tai julkishallinnon elimen, joka toimii rekisterinpitäjänä tai henkilötietojen käsittelijänä, tulee nimetä tietosuojavastaava, jonka aseman ja toimenkuvan määrittelee tietosuoja-asetus. Yksi tietosuojavastaava voidaan nimittää useampaa viranomaista tai julkishallinnon elintä varten.
Sisäänrakennettu ja oletusarvoinen tietosuoja	Tietosuojaperiaatteiden sisällyttäminen osaksi henkilötietojen käsittelyä. Periaatteiden huomioon ottaminen käsittelytapojen määrittelyn ja itse käsittelyn yhteydessä siten, että varmistetaan käsittelyn vastaavuus tietosuoja-asetuksen vaatimusten kanssa. Rekisterinpitäjän tulee toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet ja menettelyt, jotta: • oletusarvoisesti kerätään vain henkilötietoja, jotka ovat välttämättömiä ja tarpeellisia käsittelytarkoituksen kannalta, • henkilötietoja ei kerätä eikä säilytetä suurempia määriä eikä kauemmin kuin on tarpeellista kyseiseen tarkoitukseen, • henkilötietoja ei oletusarvoisesti saateta rajoittamattoman henkilömäärän saataville, • taataan rekisteröityjen oikeuksien toteutuminen.

	Tietosuoja-asetuksen vaatimusten toteutuminen tulee taata määrittelyvaiheesta lähtien koko käsiteltävien henkilötietojen elinkaaren loppuun.
Osoitusvelvollisuus	Osoitusvelvollisuus velvoittaa organisaation osoittamaan, että se on huolehtinut seuraavista henkilötietojen käsittelyä koskevista periaatteista: • lainmukaisuus, kohtuullisuus ja läpinäkyvyys, • käyttötarkoitussidonnaisuus, • tietojen minimointi, • täsmällisyys, • säilytyksen rajoittaminen ja • tietojen eheys ja luottamuksellisuus.

Rekisteröidyn oikeudet

Rekisteröidyn oikeuksien toteuttaminen kuuluu rekisterinpitäjän velvollisuuksiin. Tietosuoja-asetuksen määrittelemät rekisteröityjen oikeudet ovat osin vastaavia kuin nykyisessä henkilötietolaissa, mutta asetus tuo rekisteröidylle myös uusia oikeuksia. Rekisterinpitäjällä on velvollisuus tunnistaa rekisteröidyn henkilöllisyys, kun hän käyttää oikeuksiaan saadakseen pääsyn tietoihinsa, oikeuksiaan häntä koskevien tietojen oikaisuun tai poistamiseen tai siirtääkseen tietonsa järjestelmästä toiseen. Rekisteröidyn näitä oikeuksia koskeviin pyyntöihin tulee vastata kuukauden kuluessa pyynnön vastaanottamisesta. Tarvittaessa rekisterinpitäjä voi soveltaa kahden kuukauden jatkoaikaa, mikäli rekisteröidyn pyyntö on monimutkainen tai pyyntöjä on tullut määrällisesti useita. Tiedot toimitetaan pääsääntöisesti sähköisessä muodossa ja maksutta.

Rekisterinpitäjän tiedonantovelvollisuuteen kuuluu, että se tiedottaa avoimesti henkilötietojen käsittelystä ennen käsittelytoiminnan aloittamista. Lisäksi kuvaus henkilötietojen käsittelystä tulee pitää julkisesti saatavilla ja sen ajantasaisuus tulee tarkistaa säännöllisesti. Ennen henkilötietojen keräämistä rekisterinpitäjän tulee ilmoittaa rekisteröidylle helposti ymmärrettävässä muodossa seuraavista seikoista (rekisteriseloste/tietosuojaseloste):

- rekisterinpitäjän ja tietosuojavastaavan yhteystiedot;
- mihin tarkoituksiin henkilötietoja käsitellään ja mikä on käsittelyn oikeusperuste;
- jos tietoja luovutetaan kolmansille osapuolille, henkilötietojen vastaanottajat;
- jos henkilötietoja luovutetaan kolmanteen maahan, miten tietosuojan riittävyydestä on huolehdittu ja mistä rekisteröity voi saada siitä lisätietoja;
- henkilötietojen säilytysaika tai kriteerit sille, miten säilytysaika määräytyy;
- rekisteröidyn oikeudet ja miten rekisteröidyt voivat niitä käyttää;
- rekisteröidyn oikeudesta tehdä valitus valvontaviranomaiselle;
- mihin henkilötietojen antamisen vaatimus perustuu, onko rekisteröidyn pakko toimittaa tiedot ja mitkä ovat seuraukset tietojen antamatta jättämisestä;
- liittyykö käsittelyyn automaattista päätöksentekoa tai profilointia, ja jos liittyy, millainen käsittelylogiikka niihin liittyy, sekä niiden merkitys ja seuraukset rekisteröidylle.

Jos tietoja ei kerätä rekisteröidyltä itseltään vaan muista lähteistä, edellä mainittujen seikkojen lisäksi on ilmoitettava kerättävät tiedot, mistä henkilötiedot on saatu ja onko tiedot saatu yleisesti saatavilla olevista lähteistä.

Henkilötietolain tarkastusoikeutta vastaavasti rekisteröidyllä tulee asetuksen mukaan olemaan ***oikeus saada pääsy omiin henkilötietoihinsa***. Rekisterinpitäjän on rekisteröidyn pyytäessä ilmoitettava, käsitelläänkö häntä koskevia henkilötietoja vai ei sekä toimitettava jäljennös käsiteltävistä henkilötiedoista. Samalla hänelle on annettava ilmoitus käsiteltävistä henkilötietoryhmistä sekä edellä mainitut seikat sisältävä ilmoitus henkilötietojen käsittelystä (rekisteriseloste/tietosuojaseloste).

Nykysääntelyä vastaavasti rekisteröidyllä on ***oikeus tietojen oikaisemiseen***. Rekisteröidyllä on oikeus vaatia, että rekisterinpitäjä oikaisee rekisteröityä koskevat virheelliset henkilötiedot tai täydentää puutteellisia henkilötietoja.

Asetuksessa säädetty ***oikeus tulla unohdetuksi*** tarkoittaa rekisteröidyn oikeutta pyytää rekisterinpitäjää poistamaan häntä koskevat vanhentuneet henkilötiedot. Rekisteröidyllä on myös oikeus peruuttaa suostumuksensa, johon käsittely on perustunut. Suostumuksen peruuttamisen tulee olla yhtä helppoa kuin sen antamisen. Peruuttamisen yhteydessä rekisteröity voi esittää pyynnön häntä koskevien tietojen poistamisesta järjestelmistä. Rekisterinpitäjän on tällöin poistettava tiedot, jollei tietojen käsittelylle ole ollut muuta laillista perustetta. Tietojen poisto voidaan teknisesti toteuttaa esimerkiksi siten, että kyseisiä tietoja ei enää päivitetä ja niihin pääsyä rajoitetaan salaamalla tai ylikirjoittamalla ne. Oikeutta tulla unohdetuksi ei sovelleta lakisääteisiin rekistereihin kuten kirkon yhteiseen jäsentietojärjestelmään.

Uusi rekisteröidyn oikeus on ***oikeus siirtää tiedot järjestelmästä toiseen***. Oikeuden käyttäminen edellyttää, että henkilötietojen käsittely perustuu suostumukseen tai sopimukseen ja käsittely tehdään automatisoidusti. Julkisessa viranomaisessa siirto-oikeutta sovelletaan niihin rekistereihin, jotka on kerätty viranomaisen vapaaehtoisten, ei-lakisääteisten tehtävien hoitamiseen. Siirto-oikeutta ei sovelleta käsittelyyn, joka on tarpeen yleistä etua koskevan tehtävän suorittamisessa tai käytettäessä julkista valtaa.

Rekisteröidyllä on ***oikeus vastustaa henkilötietojen käsittelyä, automaattista päätöksentekoa ja profilointia***. Rekisteröidyllä on oikeus henkilökohtaisen erityisen tilanteensa perusteella milloin tahansa vastustaa häntä koskevien henkilötietojen käsittelyä, joka perustuu asetuksen 6 artiklan 1 kohdan e tai f alakohtaan, kuten näihin säännöksiin perustuvaa profilointia. Rekisterinpitäjä ei saa tällöin enää käsitellä henkilötietoja, jollei se voi osoittaa, että käsittelyyn on olemassa huomattavan tärkeä ja perusteltu syy, joka syrjäyttää rekisteröidyn edut, oikeudet ja vapaudet, tai jos käsittely on tarpeen oikeusvaateen laatimiseksi, esittämiseksi tai puolustamiseksi. Jos rekisteröity vastustaa henkilötietojen käsittelyä suoramarkkinointia varten, niitä ei saa enää käsitellä tähän tarkoitukseen. Tämä rekisteröidyn oikeus ei kuitenkaan koske julkisen viranomaisen lain perusteella pitämää henkilörekisteriä.

Lisäksi rekisteröidyllä on oikeus olla joutumatta sellaisen päätöksen kohteeksi, joka perustuu pelkästään automaattiseen käsittelyyn, kuten profilointiin, ja jolla on häntä koskevia oikeusvaikutuksia tai joka vaikuttaa häneen merkittävästi vastaavalla tavalla. Oikeutta ei sovelleta, jos päätökseen on asetuksessa säädetty perusteltu syy.

Uutena oikeutena rekisteröidylle asetus säätää ***oikeuden saada ilmoitus henkilötietojen tietoturvaloukkauksista***. Rekisterinpitäjällä on velvollisuus ilmoittaa henkilötietojen tietoturvaloukkauksesta henkilökohtaisesti niille rekisteröidyille, joiden tietoja loukkaus koskettaa. Ilmoitus on tehtävä, jos loukkaus todennäköisesti aiheuttaa suuren riskin yksilön oikeuksille ja vapauksille, esimerkiksi identiteettivarkauksien, maksuvälinepetosten tai muun rikollisen toiminnan muodossa. Rekisteröidylle annettavassa ilmoituksessa tulee vähintään antaa selkeä ja yksinkertainen kuvaus tapahtuneesta, kertoa tietosuojavastaavan yhteystiedot ja mahdollisuudesta saada lisätietoja, kertoa millaisia vaikutuksia henkilötietojen tietoturvaloukkauksesta voi rekisteröidylle olla sekä kuvata niitä toimenpiteitä, joita rekisterinpitäjä alkaa toteuttaa tai jotka se on jo toteuttanut haittavaikutuksen lieventämiseksi ja tilanteen ratkaisemiseksi.

Rekisterinpitäjän velvollisuudet

Rekisteröityjen oikeuksien toteuttamisen lisäksi tietosuoja-asetus määrittelee muita rekisterinpitäjän velvollisuuksia. Tietosuoja-asetuksen tultua voimaan asetuksessa säädettyjen vaatimusten mukaisuus ei enää riitä, vaan rekisterinpitäjän on pystyttävä osoittamaan, miten se on toiminnassaan varmistanut tietosuojavelvollisuuksien toteutumisen tarvittavin teknisin, hallinnollisin ja organisatorisin toimenpitein (***osoitusvelvollisuus***).

Henkilötietojen ***käsittely on lainmukaista*** ainoastaan asetuksen määrittelemin edellytyksin. Rekisterinpitäjä on vastuussa siitä, että henkilötietoja ei käsitellä ilman asianmukaista oikeusperustaa. Asetuksen mukaan lainmukaista käsittelyn edellytyksiä ovat muun muassa:

- rekisteröidyn vapaaehtoisesti, yksilöidysti, tietoisesti ja yksiselitteisesti antama suostumus, jonka rekisterinpitäjä pystyy osoittamaan;
- sellaisen sopimuksen täytäntöönpano, jossa rekisteröity on osapuolena;
- rekisterinpitäjän lakisääteinen velvoite – asetus sallii kansallista liikkumavaraa;
- rekisteröidyn ja toisen luonnollisen henkilön elintärkeiden etujen suojaaminen;
- rekisterinpitäjälle kuuluvan julkisen vallan käyttäminen – asetus sallii kansallista liikkumavaraa.

Kuten nykyinen henkilötietolaki myös asetus asettaa tietyt henkilötiedot erityisasemaan, jolloin niiden käsittely on pääsääntöisesti kielletty, jollei käsittelylle ole asetuksessa säädettyjä perusteita. Tällainen tieto on esimerkiksi tieto henkilön uskonnollisesta vakaumuksesta. Tiedon käsittely on kuitenkin mahdollista rekisteröidyn nimenomaisella suostumuksella. Lisäksi käsittely on sallittua esimerkiksi silloin, jos käsittely tapahtuu voittoa tavoittelemattoman yhteisön laillisen toiminnan yhteydessä ja asianmukaisin suojatoimin. Lisäksi edellytetään, että käsittely koskee ainoastaan yhteisön jäseniä tai entisiä jäseniä tai henkilöitä, joilla on yhteisöön säännölliset, yhteisön tarkoituksiin liittyvät yhteydet ja ettei henkilötietoja luovuteta yhteisön ulkopuolelle ilman rekisteröidyn suostumusta.

Henkilötietojen käsittely asiallisin edellytyksin tulee huomioida myös uusia käsittelytapoja tai henkilörekistereitä suunniteltaessa. Henkilötietojen käsittelyn tulee olla myös tarkoitussidonnaista, eli rekisterinpitäjän tulee ennakkoon määritellä ne tarkoitukset, joihin henkilötietoja käsitellään, ja varmistua, ettei henkilötietoja käsitellä muihin tarkoituksiin.

Asetuksessa säädetyt ***tietosuojavelvollisuudet*** koskevat kaikkia seurakunnan, seurakuntayhtymän, hiippakunnan tai muun kirkon viranomaisen käsittelemiä henkilötietoja, olipa kyseessä seurakunnan jäsenten tai asiakkaiden (esimerkiksi diakoniatyö) taikka yhteistyökumppaneiden tai oman organisaation henkilöstön tai luottamushenkilöiden tiedot.

Kun tietoja käsittelee viranomainen tai muu julkishallinnon elin, on sen asetuksen mukaan nimettävä ***tietosuojavastaava***. Sama tietosuojavastaava voidaan nimetä useamman seurakunnan tai seurakuntayhtymän tai muun kirkon viranomaisen yhteiseksi tietosuojavastaavaksi. Tietosuojavastaavan tulee olla organisaatiossa riippumattomassa asemassa, ja hän on raportointivelvollinen rekisterinpitäjän tai tietojen käsittelijän ylimmälle johdolle. Tietosuojavastaava tulee ottaa asianmukaisesti ja riittävän ajoissa mukaan kaikkiin tietosuojaan liittyviin kysymyksiin, ja hänellä tulee olla riittävä tietosuojalainsäädännön tuntemus, lain vaatimusten soveltamisosaaminen sekä alan käytäntöjen tuntemus. Rekisterinpitäjä tai tietojen käsittelijä voi toimia tietosuojavastaavan työnantajana, mutta toiminta voidaan myös ulkoistaa palvelutuottajalle. Tietosuojavastaavalle on tehtäviensä hoitamiseksi taattava tarvittavat resurssit sekä asianmukainen pääsy henkilötietoihin ja niiden käsittelytoimiin. Tietosuojavastaava toimii julkisena yhdyshenkilönä sekä valvontaviranomaisen että rekisteröityjen suuntaan. Hän on velvollinen noudattamaan tehtävässään salassapitosäännöksiä, eikä häntä voi erottaa tai rangaista asiallisesti hoidettujen tietosuojavastaavan tehtävien hoitamisen vuoksi. Tietosuojavastaavalle voidaan antaa organisaatiossa muitakin tehtäviä, mutta ne eivät saa olla ristiriidassa tietosuojavastaavan tehtävien tai riippumattoman aseman kanssa.

Tietosuojavastaavan tehtävänä on antaa rekisterinpitäjälle sekä henkilötietoja käsitteleville viranhaltijoille ja työntekijöille tietoja ja neuvoja tietosuoja-asetuksen ja muun tietosuojalainsäädännön mukaisista velvollisuuksista. Tietosuojavastaavan tulee seurata, että viranomaisessa noudatetaan tietosuoja-asetusta ja muuta tietosuojalainsäädäntöä sekä rekisterinpitäjän henkilötietojen suojaan liittyviä toimintamenettelyjä kuten vastuunjakoa, henkilöstön koulutusta ja tarkistustoimenpiteitä. Hänen tulee antaa pyydettäessä neuvoja tietosuojaa koskevasta vaikutusarvioinnista ja valvoa sen toteutusta. Sen lisäksi, että tietosuojavastaava tekee yhteistyötä valvontaviranomaisten kanssa, hän toimii rekisteröityjen tukihenkilönä. Rekisteröidyt voivat ottaa yhteyttä tietosuojavastaavaan kaikissa asioissa, jotka liittyvät heidän henkilötietojensa käsittelyyn sekä tietosuoja-asetukseen perustuvien oikeuksien käyttöön.

Tietosuoja-asetuksen lähtökohtana on riskien tunnistaminen ja niiden hallinnointi. Rekisterinpitäjä ja henkilötietojen käsittelijä ovat velvollisia arvioimaan henkilötietojen käsittelyyn liittyviä riskejä ja valitsemaan arvioidun

riskitason mukaan tarvittavat hallintatoimenpiteet. Asetus määrittää ***tietosuojan vaikutusarvioinnin*** pakolliseksi toimenpiteeksi sellaisille henkilötietojen käsittelytoimenpiteille, joiden suunnitteluvaiheessa on todennäköistä, että käsittelytoimiin liittyy yksilöiden oikeuksien ja vapauksien kannalta merkittäviä riskejä. Vaikutusarvioinnin tuloksia käytetään niiden hallintakeinojen määrittelemisessä, joilla pyritään pienentämään riskitasoa sekä samalla varmistamaan asetuksen vaatimusten toteutumista. Jos riskitaso on suuri eikä rekisterinpitäjä pysty sitä pienentämään, on otettava yhteyttä valvontaviranomaiseen (*ennakkokuuleminen)*. Vaikutusarviointi kohdistetaan suunnitteluvaiheessa olevaan järjestelmään, sovellukseen, palveluun tai hankkeeseen, jossa tullaan käsittelemään henkilötietoja. Vaikutusarviointi tehdään tietosuoja-asetuksessa ja muussa tietosuojalainsäädännössä säädettyjen vaatimusten pohjalta, ja sen tekemistä suositellaan kaikille rekisterinpitäjille.

Asetus velvoittaa käsitteillä ***sisäänrakennettu ja oletusarvoinen tietosuoja*** rekisterinpitäjää sisällyttämään tietosuojaperiaatteet ja -vaatimukset aikaisessa vaiheessa osaksi henkilötietojen käsittelyä. Tietosuoja-asetuksen vaatimusten toteutuminen tulee taata määrittelyvaiheessa koko käsiteltävien henkilötietojen elinkaaren ajan. Elinkaarella tarkoitetaan ajanjaksoa henkilötietojen keräämisestä niiden hävittämiseen tai poistoon asti; 1) suostumus tai muu laillinen peruste, 2) tietojen kerääminen, 3) käsittely, 4) tietojen mahdollinen luovuttaminen, 5) arkistointi ja 6) hävittäminen tai muu poistaminen. Käytännössä tämä tarkoittaa tietosuojan sisällyttämistä sekä järjestelmä- ja sovelluskehitykseen että hankintoihin ja projektinhallintaan.

Asetuksen mukaan rekisterinpitäjällä on siis ***velvollisuus huolehtia tietoturvallisuudesta*** koko henkilötietojen elinkaaren ajan, joten rekisterinpitäjän tulee toteuttaa asianmukaiset tekniset ja organisatoriset toimenpiteet, jotta henkilötietojen käsittely on turvattua. Henkilötiedot tulee suojata siirron, tallennuksen ja käsittelyn aikana oikeudettomalta tai vahingossa tapahtuvalta tuhoamiselta, muuttamiselta, luovuttamiselta tai niihin pääsyltä. Tietoturvallisuuden toteuttaminen riippuu organisaation koosta ja muusta toiminnasta, ja se tulee suhteuttaa toimintaan ja suojeltaviin tietoihin.

Asetuksen astuessa voimaan rekisterinpitäjälle tulee uutena velvollisuutena ***ilmoitusvelvollisuus*** tietoturvaloukkauksista. Ilmoitusvelvollisuus kohdistuu sekä rekisteröityihin että valvontaviranomaiseen. Ilmoitus henkilötietojen tietoturvaloukkauksesta tulee tehdä valvontaviranomaiselle 72 tunnin kuluessa siitä, kun loukkaus on havaittu. Ilmoituksessa tulee vähintään antaa kuvaus tapahtuneesta; kertoa niiden rekisteröityjen ryhmät ja lukumäärät, joita loukkaus koskee; kertoa tietosuojavastaavan yhteystiedot ja mahdollisuudesta saada lisätietoja; kertoa millaisia vaikutuksia henkilötietojen tietoturvaloukkauksesta voi todennäköisesti olla rekisteröidylle; sekä kuvata niitä toimenpiteitä, joita rekisterinpitäjä aikoo toteuttaa tai jotka se on jo toteuttanut haittavaikutuksen lieventämiseksi ja tilanteen ratkaisemiseksi. Jotta ilmoitusvelvollisuus on mahdollista täyttää, rekisterinpitäjällä tulisi olla keinot havaita poikkeamat henkilötietojen käsittelyssä sekä mahdollisuus selvittää havaitun poikkeaman syyt ja seuraukset sekä vaikutukset yksityisyyden suojaan. Samoin tulisi kyetä estämään poikkeaman leviäminen ja tarvittaessa varmistaa ulkopuolisen avun saaminen sekä analysoida, onko tarvetta asetuksen mukaisille ilmoituksille. Tilanteen korjaannuttua tulisi tunnistaa tarvittavat muutokset ja kehitystoimenpiteet sekä huolehtia tapahtuman dokumentaation ja todisteiden säilyttämisestä. Tarvittaessa tietoturvapoikkeamasta on tehtävä tutkintapyyntö poliisille ja mahdollisesti myös ilmoitus Viestintävirastossa toimivalle Kyberturvallisuuskeskukselle.

Rekisterinpitäjällä tai nimetyllä tietosuojavastaavalla on ***velvollisuus tehdä yhteistyötä valvontaviranomaisen kanssa*** valvontaviranomaisen niin pyytäessä tai mahdollisen valvontaviranomaisen ennakkokuulemisen yhteydessä. Tietosuoja-asetus tuo valvontaviranomaiselle uutena asiana oikeuden määrätä rekisterinpitäjälle ja/tai henkilötietojen käsittelijälle sakkoja tai hallinnollisia seuraamuksia tietosuoja-asetuksen velvoitteiden laiminlyönnistä. Valvontaviranomaisella on myös oikeus auditoida rekisterinpitäjän tietosuojan toteutusta. Julkishallinnon osalta käytettävät menettelyt tarkentuvat osana lainsäädäntötyön etenemistä.

Suosituksia toimenpiteistä

Rekisterinpitäjinä toimivien seurakuntien, seurakuntayhtymien, tuomiokapitulien ja kirkon muiden viranomaisten on syytä aloittaa asetuksen voimaantuloon valmistautuminen.

Organisaation johdon osallistuminen ja tuki tietosuojatyölle on yksi tärkeimmistä ensisijaisista toimenpiteistä. Sekä virkamies- että luottamushenkilöjohdon vastuulla on varata tarvittavat resurssit tietosuojan nykytilan arvioimiseksi sekä valtuuttaa ja mahdollistaa arvioinnin pohjalta tunnistettujen kehitystoimenpiteiden toteuttaminen. Jatkossakin johdon tietoisuus organisaation tietosuojan tilasta on osa rekisterinpitäjän osoitusvelvollisuuden toteutumista. Nimitettävän tietosuojavastaavan vastuulle on syytä osoittaa säännöllinen raportointi esimerkiksi kirkkoneuvostolle tai yhteiselle kirkkoneuvostolle taikka vähintään vuosiraportin laatiminen.

Ensisijaisesti tulee tehdä myös arvio henkilötietojen käsittelyn ja tietosuojan toteutumisen nykyisestä tilanteesta ja nykytilan suhteesta tietosuoja-asetuksen vaatimuksiin (***nykytila-analyysi***). Arviointiin tulee sisällyttää erityisesti rekisteröityjen oikeuksien ja riskilähtöisyyden toteutuminen. Arvioinnin perusteella voidaan tunnistaa puutteet ja kehityskohteet sekä suunnitella toimenpiteet, joilla nykytilaa on syytä kehittää.

Tärkeä osa nykytila-analyysia on organisaation keräämien ja käsittelemien henkilötietojen kokonaiskuvan selvittäminen; mitä henkilörekistereitä organisaatiossa on sekä missä ja kenen toimesta henkilötietoja käsitellään. Myös sopimusten tietoturvavaatimukset tulee arvioida henkilötietojen suojaamisen näkökulmasta, ja tarvittaessa sopimuksia tulee täydentää vastaamaan tietosuoja-asetuksen vaatimuksia. Yhtenä apuvälineenä henkilötieto- ja sopimusinventaarion selvittämiseksi on mallintaa henkilötietojen tietovirrat eli kuvata käsiteltävät henkilötietotyypit, henkilötietojen lähteet, henkilötietoja käsittelevät sovellukset, järjestelmät ja käsittelijöiden roolit sekä miten henkilötiedot siirtyvät edellä mainittujen välillä, käsittelyn fyysiset sijainnit sekä luovutetaanko tai siirretäänkö henkilötietoja edelleen kolmansille osapuolille sekä kuinka kauan henkilötietoja käsitellään ja kuinka ne tullaan hävittämään.

Tietojärjestelmiä ja sopimuksia läpi käytäessä on syytä päivittää rekisteriselosteet ajan tasalle vastaamaan asetuksessa säädettyä rekisterinpitäjän tiedonantovelvollisuuden sisältöä. Samalla varmistetaan, mitä henkilötietojen luovuttamisesta etenkin ETA-alueen ulkopuolelle on sovittu ja onko tämä huomioitu myös mahdollisessa palvelutoimittajan kanssa tehdyssä sopimuksessa. Lisäksi huolehditaan siitä, että henkilötietojen käsittelystä on ajantasaiset ja asianmukaiset kuvaukset tietosuojaselosteessa ja käytössä olevissa viestintäkanavissa, esimerkiksi internet-sivuilla. On myös syytä varmistaa, onko mahdolliset tietosuojaloukkaukset otettu huomioon organisaation valmius- ja kriisiviestintäsuunnitelmassa asetuksen vaatimalla tavalla.
Kun henkilötietojen käyttötarkoitukset, henkilötietoja käsittelevät sovellukset ja järjestelmät sekä henkilötietojen siirtotilanteet ovat selvillä, on suositeltavaa tehdä **riskianalyysi**, jotta tarvittavat hallintatoimenpiteet voidaan tunnistaa ja mitoittaa sekä luoda tarvittaessa riskienhallintamalli.

Tietosuojavastaava on hyvä nimittää ajoissa. Tietosuojavastaavalla on oltava riittävä osaaminen ja toimivalta tehtävänsä hoitamiseen. Tarvittaessa henkilölle tulee järjestää koulutusta. Tietosuojavastaavan riippumattomuuden takaamiseksi häntä nimitettäessä on syytä arvioida huolella, mihin kohtaan hän organisaatiossa sijoittuu. Tehtävä voidaan myös ulkoistaa, tai seurakunnat tai seurakuntayhtymät sekä tuomiokapitulit voivat nimittää yhteisen tietosuojavastaavan. Jos henkilötietojen omistajuus ja käsittely on hajautettu usealle seurakunnan tai seurakuntayhtymän tehtäväalueelle tai yksikölle, on tarkoituksenmukaista lisäksi perustaa sisäinen tietosuojaorganisaatio, johon valitaan edustajat kyseisiltä tehtäväalueilta tai yksiköistä.

Kirkon viranomaisen tulee huolehtia siitä, että niillä viranhaltijoilla ja työntekijöillä, jotka käsittelevät henkilötietoja tai jotka osallistuvat rekisteröityjen oikeuksien toteuttamiseen luotuihin prosesseihin, on riittävästi tietosuoja- ja tietoturvaosaamista. Etukäteen on syytä pohtia myös ne menettelyprosessit, joilla turvataan rekisteröityjen oikeuksien toteutuminen kuten esimerkiksi rekisterinpitäjän tiedonantovelvollisuus, suostumuksen pyytäminen tietojen keräämiseen ja oikeus saada pääsy omiin tietoihin.

Tietosuoja-asetus tulee myös ottaa huomioon meneillään olevissa järjestelmähankkeissa ja sovelluskehityksissä sekä uusissa järjestelmähankkeissa niiden kilpailutuksesta lähtien. Asetuksen mukaan organisaatiolla on velvollisuus järjestää henkilötietojen käsittely tavalla, jonka avulla asetus, tietosuojaperiaatteet ja rekisteröityjen oikeudet tulevat tehokkaasti otetuiksi huomioon kaikessa tietojenkäsittelyssä.

Lisätietoja

Lisätietoa Euroopan unionin yleisen tietosuoja-asetuksen täytäntöönpanosta on muun muassa tietosuojavaltuutetun sivuilla www.tietosuoja.fi, sekä valtiovarainministeriön alaisuudessa toimivan Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmän (VAHTI) sivuilla www.vm.fi/vahti. Tämä yleiskirje pohjautuu osittain kyseisillä sivuilla julkaistuun VAHTI-raporttiin 1/2016, EU-tietosuojan kokonaisuudistus.

Meneillään olevasta lainsäädäntöhankkeesta löytyy lisätietoja oikeusministeriön sivulta http://oikeusministerio.fi/fi/index/valmisteilla/lakihankkeet/informaatio-oikeus/henkilotietojensuojakansallisenlainsaadannontarkistaminen_0.html.

Tämän yleiskirjeen sisällöstä lisätietoja antavat kirkkoneuvos Pirjo Pihlaja ja tietoturvapäällikkö Jussi Mukari, etunimi.sukunimi@evl.fi. Kirkkohallituksessa seurataan tietosuoja-asetuksen täytäntöönpanoa, ja se pyrkii tiedottamaan asetuksen täytäntöönpanoa koskevista seikoista sekä täsmentämään asiaan liittyvää ohjeistusta seuraavan puolentoista vuoden aikana.

KIRKKOHALLITUS

Jukka Keskitalo

Pirjo Pihlaja

ISSN 1797-0326

Suomen evankelis-luterilainen kirkko
Evangelisk-lutherska kyrkan i Finland
Kirkkohallitus / Kyrkostyrelsen

Eteläranta 8 / Södra Kajen 8
PL / PB 210
00131 Helsinki / Helsingfors

vaihde / växel 09 180 21 / faksi / fax 09 180 2350
kirkkohallitus@evl.fi / kyrkostyrelsen@evl.fi
evl.fi

Y-tunnus / FO-nummer 0118950-3
IBAN: FI47 8000 1000 0676 87
BIC: DABAFIHH