SASTAMALAN SEURAKUNTA

Sastamalan seurakunnan tietosuojan toimintalinjaus

1.Toimintalinjauksen tarkoitus

Tietosuojan toimintalinjaus tarkoittaa järjestelmää, jossa on määritelty tietosuojan periaatteet, toimintatavat, vastuut, valvonta- ja seuraamusjärjestelmä. Seurakunnan tietosuojaa suunnitellaan, toteutetaan ja kehitetään linjauksen mukaisesti. Tämä toimintalinjaus koskee henkilötietojen käsittelyä, jossa seurakunta on rekisterinpitäjänä. Toimintalinjaus perustuu seurakunnan tehtävään. Seurakunnan tehtävänä on järjestää hengellistä toimintaa yhtäältä omaehtoisesti. Se perustuu kirkkolaissa ja kirkkojärjestyksessä määriteltyyn seurakunnan tehtävään. Toisaalta seurakunta ottaa huomioon seurakunnan jäsenten, vapaaehtoisten sekä muiden seurakunnan kanssa tekemisissä olevien henkilöiden hengelliset ja hengelliseen toimintaan liittyvät tarpeet. Tietosuojatoiminnasta vastaa rekisterinpitäjänä seurakunta. Tietosuojatoimintaa johtavat ja siitä vastaavat viranhaltijoina kirkkoherra, talousjohtaja ja tietosuojan vastuuhenkilö, sekä luottamuselinjohtona kirkkoneuvosto. Toimintalinjaus on lähtökohta tietosuojaa koskeville ohjeille. Ohjeet tarkentavat linjauksessa annettuja määräyksiä ja soveltamista. Toimintalinjaus koskee seurakunnan koko henkilöstöä ja hallintoa. Se koskee myös seurakunnan sidosryhmien edustajia, jotka käsittelevät seurakunnan omistamia tai hallinnoimia henkilötietoja (mm. luottamushenkilöitä ja vapaaehtoisia). Tietosuojaselosteissa määritellään tarkemmin tiedon omistaja. Toimintalinjaus kattaa seurakunnan omistaman tiedon riippumatta sen esitystavasta, muodosta, suojaustasosta tai elinkaaren vaiheesta.

2.Tietosuojan määritelmä

Henkilötietojen suoja on perusoikeus. Henkilötietojen käsittelyn on oltava asianmukaista ja sen on tapahduttava tiettyä tarkoitusta varten. Henkilötietoja voidaan käsitellä asianomaisen henkilön suostumuksella tai muun laissa säädetyn perusteen nojalla (kts. kohta Tietosuojan toteuttaminen). Henkilötietojen suojalla tarkoitetaan myös oikeutta tutustua tietoihin, joita henkilöstä itsestään on kerätty, ja tarvittaessa saada hänestä kerätyt tiedot oikaistuiksi tai poistetuiksi.

3.Tietosuojan tavoitteet ja periaatteet

Tietosuojan arvioinnin lähtökohta on riskien arviointi. Tietosuojariski tarkoittaa vaaraa, että henkilötietoja tuhoutuu, häviää tai muuttuu, henkilötietoja luovutetaan luvattomasti, niihin päästään oikeudettomasti käsiksi tai tietojen käytettävyys häviää. Tietoturvaloukkauksesta voi seurata esimerkiksi henkilötietojen valvomiskyvyn menettäminen, identiteettivarkaus tai petos, maineen vahingoittuminen sekä pseudonymisoitujen tai salassapitovelvollisuuden alaisten henkilötietojen

paljastuminen. Seurakunta rekisterinpitäjänä arvioi henkilötietojen käsittelyyn liittyvät riskit ja valitsee arvioidun riskitason mukaan tarvittavat tietojen hallinnan tavat. Tietosuojariskien hallinta on osa seurakunnan yleistä riskienhallintaa. Merkittävän tason riskit raportoidaan johdolle saakka. Riskilähtöisyys ohjaa organisaation henkilötietojen käsittelyä ja on osa rekisterinpitäjän osoitusvelvollisuuden toteuttamista. Riskilähtöisestä toimintaperiaatteesta seuraa, että seurakunta arvioi sellaisten henkilötietojen käsittelytoimien vaikutuksia, joissa jo suunnitteluvaiheessa arvioidaan todennäköiseksi, että käsittelytoimiin liittyy yksilöiden oikeuksien ja vapauksien kannalta merkittäviä riskejä. Vaikutusarvioinnin tuloksien avulla määritellään hallintakeinot, joilla pyritään pienentämään henkilötietojen käsittelyn riskitasoa. Tavoitteena on varmistaa tietosuoja-asetuksen vaatimusten toteutuminen. Seurakunnan toiminnassa toteutetaan sisäänrakennetun ja oletusarvoisen tietosuojan periaatetta. Tietosuoja otetaan huomioon monipuolisesti perustoiminnassa (eri toiminnoissa, johtamisessa, hankinnoissa ja kehitystyössä). Tietosuojaa toteutetaan käyttämällä riskiarvion mukaisia ja tarkoituksenmukaisia teknisiä ja hallinnollisia ratkaisuja. Seurakunnan tavoitteena on huolehtia tietosuoja-asetuksen mukaisten rekisteröityjen oikeuksien toteutumisesta. Tämä tehdään kuvaamalla ja ohjeistamalla henkilötietojen käsittelyn käytännöt sekä huolehtimalla henkilötietojen käyttäjien koulutuksesta.

4.Tietosuojan toteuttaminen

Henkilötietojen käsittely toteutetaan noudattamalla seuraavia periaatteita:

- henkilötietoja käsitellään lainmukaisesti, asianmukaisesti ja läpinäkyvästi
- henkilötietoja käsitellään suunnitellun käyttötarkoituksen mukaisesti
- henkilötietoja kerätään käyttötarkoituksen mukainen määrä, ei enempää
- henkilötietojen käsittely toteutetaan täsmällisesti
- henkilötietoja säilytetään käyttötarkoituksen kannalta tarkoituksenmukainen aika
- henkilötietojen käsittelyssä toteutetaan henkilötietojen eheyden ja luottamuksellisuuden
- periaatetta

Seurakunta toteuttaa sisäänrakennetun ja oletusarvoisen tietosuojan periaatetta. Tämä tarkoittaa, että

- tietosuojaperiaatteet ja -vaatimukset sisältyvät jo tietosuojajärjestelmien suunnitteluun
- tietosuoja on alusta alkaen osa henkilötietojen käsittelyn tapoja
- tekniset ratkaisut vastaavat henkilötietojen käsittelyn riskitasoa
- käytännön toimintatavat ja sisäinen hallinto toteutetaan turvaamaan henkilötietojen suojaa.

Näillä toimenpiteillä huolehditaan tietosuojasta niin, että:

- kerätään vain henkilötietoja, jotka ovat välttämättömiä käsittelytarkoituksen kannalta
- tietoja ei kerätä eikä säilytetä suurempia määriä eikä kauemmin kuin on tarpeellista
- kyseiseen käsittelytarkoitukseen
- henkilötietoja ei saateta henkilöiden saataville, joille niiden käsittely ei kuulu
- henkilötiedot ovat teknisesti turvassa
- tietosuojalainsäädännön vaatimukset toteutuvat käsiteltävien henkilötietojen koko elinkaaren ajan.

Seurakunta voi rekisterinpitäjänä ulkoistaa valitsemansa osan henkilötietojen käsittelystä henkilötietojen käsittelijälle. Seurakunta valitsee sopimuskumppanikseen vain sellaisia henkilötietojen

käsittelijöitä, jotka sitoutuvat noudattamaan hyvää henkilötietojen käsittelytapaa sekä täyttävät tietosuoja-asetuksen vaatimukset ja pystyvät huolehtimaan rekisteröidyn oikeuksien toteutumisesta. Seurakunnan ja erikseen valitun henkilötietojen käsittelijän välille laaditaan kirjallinen sopimus. Tietosuoja-asetuksen mukaan sopimuksessa tulee määritellä henkilötietojen käsittelyn kohde, tarkoitus ja kesto sekä sopia käsiteltävät henkilötiedot. Sopimuksen sisältö vaatimuksineen tulee määritellä mahdollisimman tarkasti. Seurakunta on rekisterinpitäjänä järjestelmissä, joiden tekninen toteutus tulee annettuna lain nojalla muilta viranomaisilta.

5.Rekisteröityjen tietopyyntöprosessi

Seurakunnassa on määritelty menettelytapa ja -ohje siihen, kun rekisteröity käyttää oikeuttaan saada pääsy rekisteröityihin henkilötietoihinsa. Ohje on nimeltään ”Tietopyyntö henkilörekisteristä”. Menettelytapaa noudatetaan, kun rekisteröidyt haluavat saada nähtäväkseen omia rekistereissä olevia henkilötietojaan. Kirkon jäsentietojärjestelmää koskevat tietopyynnöt tehdään Tampereen aluekeskusrekisteristä.

6.Henkilöstön tietosuojakoulutus

Seurakunta huolehtii henkilöstön riittävästä tietosuojaosaamisesta ja välittämällä tarpeellista tietoa. Uudet työntekijät perehdytetään tietosuoja-asioihin järjestelmällisesti perehdyttämisen yhteydessä.

7.Toiminta tietoturva-ja tietosuojapoikkeamatilanteissa sekä ilmoitusvelvollisuus

Seurakunnassa on määritelty toimintaohje tilanteeseen, jossa tapahtuu tietoturvaloukkaus. Tämän prosessin mukaista toimintatapaa noudatetaan tietosuojapoikkeamien sattuessa. Henkilötietojen tietoturvaloukkauksen sattuessa seurakunnalla on rekisterinpitäjänä ilmoitusvelvollisuuksia valvontaviranomaisen ja rekisteröidyn suuntaan. Valvontaviranomaiselle tehdään ilmoitus tietosuoja-asetuksen mukaisesti 72 tunnin kuluessa siitä, kun henkilötietojen tietoturvaloukkaus on tullut ilmi. Rekisteröidylle henkilötietojen tietoturvaloukkaus ilmoitetaan ilman aiheetonta viivytystä. Tietosuojarikkomukset käsitellään tapauskohtaisesti seurakunnan organisaation ja asian vakavuuden mukaisesti.

8.Valvonta

Tietosuoja on osa riskienhallintaa ja siihen sovelletaan tavanomaista sisäistä valvontaa. Kirkkoneuvosto hyväksyy seurakuntaa koskevat Sisäisen valvonnan ja riskienhallinnan periaatteet. Periaatteissa on kuvattu eri toimijoiden sisäisen valvonnan tehtävät ja vastuut.

Liitteet: Tietosuojavastuut (Liite 1.)

Keskeiset käsitteet (Liite 2.)

Toiminta tietoturvaloukkauksen yhteydessä (Liite 3.)

Ohje: Tietopyyntö henkilörekisteristä (seurakunnan kotisivut/Tampereen aluekeskusrekisteri)

Viitteet: Sisäisen valvonnan ohje

Liite 1.
Tietosuojavastuut Sastamalan seurakunnassa

Tässä liitteessä kuvataan tietosuojan vastuut ja velvollisuudet Sastamalan seurakunnassa. Tietosuojan vastuujärjestelyjä muutetaan seurakunnan toiminnan ja hallinnon muuttuessa. Jotkut vastuut voivat kuulua samalle henkilölle. Olennaista on, että näiden tehtävien hoito on järjestetty ja vastuilla on myös varahenkilöt.

Yleinen vastuu tietosuojan valvonnasta ja ylläpitämisestä

Tietosuojatoimintaa johtaa seurakunnan ylin johto, johon kuuluvat kirkkoherra, talousjohtaja, tietosuojan vastuuhenkilö sekä luottamuselimenä kirkkoneuvosto.

Tietosuojan toteutuminen, valvonta ja ylläpitäminen kuuluvat jokaisen seurakunnan työntekijän ja järjestelmien käyttäjän tehtäviin osana yleistä työ- tai virkavastuutaan.

Tietosuoja on osa perustyötä

Suurin osa tietosuojan toteuttamiseksi tehdystä työstä sisältyy työntekijöiden tavallisiin tehtäviin.

Tietosuojan vastuutaulukko

Toimija	Vastuu
Kirkkoneuvosto	• Hyväksyy seurakunnan *Tietosuojan toimintalinjauksen*. • Vastaa seurakunnalle annettujen tietosuojaa koskevien määräysten ja ohjeiden noudattamisesta. • Huolehtii siitä, että seurakunnalle on nimetty tietosuojavastaava. • Huolehtii siitä, että seurakunnalle on tietosuojan yhdyshenkilö ja hänen varahenkilönsä. • Huolehtii riittävistä resursseista hoitaa tietosuojaa
Ylin johto	• Vastaa henkilötietojen käsittelyn lainmukaisuudesta • Huolehtii kirkkoneuvoston päätösten valmistelusta • Huolehtii riittävistä työntekijäresursseista • Vastaa tietosuojapoikkeamien viestinnästä tietosuojan yhdyshenkilön ja tietosuojavastaavan kanssa • Huolehtii esimiesten ja muun henkilöstön riittävästä koulutuksesta
Tietosuojavastaava	• Valvoo, että henkilötietojen käsittelyssä noudatetaan tietosuojasäännöksiä. • Antaa rekisterinpitäjälle ja sen työntekijöille tietoja ja neuvoja tieto-suojasäännösten mukaisista velvollisuuksista. • Tiedottaa tietosuojaan liittyviä ohjeita, suosituksia ja määräyksiä. • Ottaa vastaan havaintoja tietosuojaan liittyvistä tapahtumista tai poikkeamista ja raportoi ne asianmukaisesti eteenpäin tietosuojavaltuutetulle.

	• Raportoi rekisterinpitäjän ylimmälle johdolle (kirkkoneuvosto, kirkkoherra, talousjohtaja, tietosuojan vastuuhenkilö) • Tietosuojavastaava ei ole vastuussa rekisterinpitäjän henkilötietojen käsittelyn lainmukaisuudesta. Tämä vastuu kuuluu rekisterinpitäjälle ja sen organisaation johdolle. • Rekisteröidyt voivat ottaa yhteyttä tietosuojavastaavaan asioissa, jotka liittyvät heidän henkilötietojensa käsittelyyn ja tietosuoja-asetukseen perustuvien oikeuksiensa käyttöön.
Tietosuojan yhdyshenkilö	• Valvoo tietosuojavastaavan apuna, että henkilötietojen käsittelyssä noudatetaan tietosuojasäännöksiä. • Huolehtii saamiensa tietosuojaan liittyvien ohjeiden, suositusten ja määräysten tiedottamisesta työntekijöille. • Osallistuu esimiesten tukena uusien työntekijöiden perehdyttämiseen tietosuojaa koskevissa kysymyksissä. • Ottaa vastaan ilmoituksia seurakunnassaan havaituista tietosuojaan liittyvistä tapahtumista ja poikkeamista ja raportoi niistä tietosuojavastaavalle sekä oman seurakuntansa esimiehille.
Esimies	• Välittää tietoa tietosuojaan liittyvistä määräyksistä omille työntekijöilleen. • Järjestää uusien työntekijöiden tietosuojaperehdytyksen ja on velvollinen huolehtimaan siitä, että työntekijät hallitsevat tietosuojatoiminnan. • Huolehtii omalta osaltaan siitä, että työntekijät noudattavat annettuja ohjeita. • Vastaa omien työntekijöidensä osalta siitä, että tietojärjestelmien käyttöoikeudet vastaavat työtehtävien tarpeita. • Puuttuu kaikkiin tietosuojaa koskettaviin havaitsemiinsa epäkohtiin.
Työntekijä	• Perehtyy häntä koskeviin tietosuojaohjeisiin ja noudattaa niitä työssään. • Ottaa toiminnassaan huomioon tietosuoja-asetuksen ja tietosuojalain mukaisen huolellisuusvelvoitteen ja julkisuuslain mukaisen hyvän tiedonhallintatavan. • Raportoi esimiehelleen ja seurakunnan tietosuojayhdyshenkilölle havaitsemansa tietosuojaan liittyvät epäkohdat ja poikkeamat.

Liite 2.
Tietosuojan toimintalinjauksen keskeiset käsitteet

Tietosuoja

Tietosuojalla tarkoitetaan toimenpiteitä, joiden tarkoituksena on suojata henkilön yksityiset henkilötiedot niiden käsittelyssä.

Tietoturva

Järjestelyt, joilla pyritään varmistamaan tiedon käytettävyys, eheys ja luottamuksellisuus. Tietoturva on riskienhallintaa ja osa organisaation turvallisuutta.

Tietosuojan toimintalinjaus

Johdon hyväksymä näkemys tietosuojan päämääristä, periaatteista ja toteutuksesta.

Henkilötieto

Kaikki tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyvät tiedot (esim. nimi, henkilötunnus, kuva, biometrinen tai geneettinen tieto). Tunnistettavissa olevana pidetään henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, sijaintitiedon, verkkotunnistetietojen tai yhden tai useamman henkilölle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella.

Henkilörekisteri

Mikä tahansa jäsennelty henkilötietoja sisältävä tietojoukko, josta tiedot ovat saatavilla tietyin perustein, oli tietojoukko sitten keskitetty, hajautettu tai toiminnallisin tai maantieteellisin perustein jaettu. Henkilörekisteri voi olla käsirekisteri tai sähköinen joko kokonaan tai osittain.

Henkilötietojen erityiset tietoryhmät, arkaluonteiset henkilötiedot

Tiedot, joista ilmenee rotu tai etninen alkuperä, poliittisia mielipiteitä, uskonnollinen tai filosofinen vakaumus, ammattiliiton jäsenyys, geneettisiä tietoja, terveyttä koskevia tietoja, tai seksuaaliseen käyttäytymiseen liittyviä tietoja. Erityisiä tietoryhmiä koskeva käsittely on erikseen säänneltyä.

Henkilötietojen käsittelijä

Luonnollinen tai oikeushenkilö, viranomainen, virasto tai muu elin, joka käsittelee henkilötietoja rekisterinpitäjän toimeksiannosta.

Henkilötietojen käsittely

Kaikenlaiset toiminnot, joita kohdistetaan henkilötietoihin joko käsin ryhmitellen tai automaattista tietojenkäsittelyä hyödyntäen. Käsittelyä ovat esimerkiksi henkilötietojen kerääminen, tallentaminen, järjestäminen, jäsentäminen, säilyttäminen, muokkaaminen, haku, käyttö, luovuttaminen, levittäminen tai saattaminen muutoin saataville, yhteensovittaminen, yhdistäminen, rajoittaminen, poistaminen ja hävittäminen.

Henkilötietojen tietoturvaloukkaus

Tapahtuma, jossa henkilötietoja on käsitelty lainvastaisesti. Loukkauksesta seuraa siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen tai saanti.

Osoitusvelvollisuus

Osoitusvelvollisuuden (accountability) avulla organisaatio osoittaa, että se on huolehtinut seuraavista henkilötietojen käsittelyn osa-alueista:

- lainmukaisuus, kohtuullisuus ja läpinäkyvyys
- käyttötarkoitussidonnaisuus
- tietojen minimointi
- täsmällisyys
- säilytyksen rajoittaminen
- eheys ja luottamuksellisuus.

Rekisterinpitäjä

Luonnollinen tai oikeushenkilö, julkinen viranomainen, virasto tai muu elin, joka yksin tai yhteistyössä muiden kanssa hallinnoi tallettamansa henkilötiedot ja määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.

Rekisteröity

Henkilö, jonka henkilötietoja käsitellään.

Tietosuojavastaava

Tietosuoja-asetuksen määrittelemä tehtävä, jonka rekisterinpitäjän ja henkilötiedon käsittelijän on nimettävä. Asetus määrittelee tietosuojavastaavan aseman ja toimenkuvan. Organisaatioryhmä voi nimittää yhden tietosuojavastaavan samoin kuin yksi tietosuojavastaava voidaan nimittää useampaa viranomaista tai julkishallinnon elintä varten.

Hallinnollinen sakko

Valvontaviranomainen voi määrätä rekisterinpitäjälle tai henkilötietojen käsittelijälle sakon tietosuoja-asetuksen vaatimusten laiminlyönnistä. Sakon suuruus määräytyy rikkomuksen luonteen perusteella.

Hallinnolliset seuraamukset

Valvontaviranomaisen määräämät seuraamukset koskien tietosuoja-asetuksen vaatimusten laiminlyöntejä.

Anonymisointi

Henkilötiedon tunnistettavuuden poistaminen siten, että tiedon yhdistäminen rekisteröityyn ei enää ole mahdollista.

Pseudonymisointi

Henkilötietojen käsittelemistä niin, että tietoja ei voida enää suoraan yhdistää tiettyyn rekisteröityyn käyttämättä lisätietoja. Tällaiset lisätiedot tulee säilyttää erillään ja niihin sovelletaan teknisiä ja organisatorisia toimenpiteitä, joilla varmistetaan, ettei tällaista yhdistämistä tunnistettuun tai tunnistettavissa olevaan henkilöön tapahdu.

Tietosuojaseloste, rekisteriseloste

Asiakirja, jossa kuvataan henkilötietojen käsittely tiiviisti esitetyssä, avoimessa ja helposti ymmärrettävässä muodossa. Rekisterinpitäjän tulee laatia ja pitää se yleisesti saatavilla.

Tietotilinpäätös

Tietotilinpäätös on organisaation laatima vapaaehtoinen raportti, joka antaa kokonaiskuvan organisaation tietojenkäsittelyn nykytilasta. Raportti on tarkoitettu johdon työkaluksi ja lisäämään sidosryhmien luottamusta siihen, että organisaatio noudattaa hyvää sääntelyn mukaista tietojenkäsittelytapaa henkilötietojen käsittelyssä. Tietotilinpäätöstä voidaan käyttää yhtenä keinona tietosuoja-asetuksen osoitusvelvollisuudentoteuttamisessa.

Vaikutustenarviointi

Arviointi siitä, kuinka suunnitellut henkilötietojen käsittelytoimet vaikuttavat tietosuojaan ja yksilön vapauksiin. Jos käsittely todennäköisesti aiheuttaa yksilön oikeuksien ja vapauksien kannalta suuren riskin, rekisterinpitäjän on ennen käsittelytoimien aloittamista toteutettava tietosuojan vaikutustenarviointi ja määriteltävä toimenpiteitä, joilla riskiä voidaan hallita. Valvontaviranomainen tulee julkaisemaan luettelon käsittelytoimista, jotka vaativat vaikutustenarvioinnin laatimisen.

Lapsen henkilötietojen käsittely

Alle 13-vuotiaiden lasten henkilötietojen käsittely ei ole sallittua ilman vanhemman tai huoltajan suostumusta.

Sisäänrakennettu ja oletusarvoinen tietosuoja

Tietosuojaperiaatteiden toteuttaminen sisällytetään aikaisessa vaiheessa osaksi henkilötietojen käsittelyä. Periaatteet otetaan huomioon henkilötietojen määrittelyssä ja varsinaisen käsittelyn yhteydessä niin, että käsittely vastaa tietosuoja-asetuksen vaatimuksia. Rekisterinpitäjän tulee toteuttaa tarvittavat tekniset ja hallinnolliset toimenpiteet ja menettelyt, jotta mm.

- kerätään vain henkilötietoja, jotka ovat välttämättömiä ja tarpeellisia käsittelytarkoituksen kannalta
- tietoja ei kerätä eikä säilytetä suurempia määriä eikä kauemmin kuin on tarpeellista kyseiseen tarkoitukseen
- henkilötietoja ei saateta rajoittamattoman henkilömäärän saataville
- taataan rekisteröityjen oikeuksien toteutuminen

Tietosuoja-asetuksen vaatimusten toteutuminen tulee taata määrittelyvaiheesta alkaen käsiteltävien henkilötietojen elinkaaren loppuun.

Liite 3.

Toiminta tietoturvaloukkauksen yhteydessä

Henkilötietojen tietoturvaloukkauksella tarkoitetaan tapahtumaa, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu, henkilötietoja luovutetaan luvattomasti, niihin päästään oikeudettomasti käsiksi tai tietojen käytettävyys häviää. Toiminta tietoturvaloukkauksen yhteydessä:

1. Tietoturvaloukkaus dokumentoidaan aina.
2. Tietoturvaloukkaukseen reagoidaan mahdollisimman nopeasti.
3. Estetään lisävahinkojen syntyminen.
4. Viestitetään loukkaus organisaation sisällä johdolle, tarpeellisille henkilöille ja tietosuojan yhdyshenkilölle.
5. Arvioidaan loukkauksen vaikutukset ja riskin suuruus loukkauksen kohteena oleville ihmisille kolmella asteikolla: ei aiheudu riskiä, aiheutuu riski, aiheutuu korkea riski.
6. Määritellään riskin perusteella välittömät toimenpiteet.
7. Ilmoitetaan tarvittaessa tietosuojavastaavalle ja valvontaviranomaisille.
8. Ilmoitetaan tarvittaessa rekisteröidyille.
9. Tietoturvaloukkaus arvioidaan ylimmässä johdossa ja tehdään tarpeelliset korjaustoimet.

Kaikki tietoturvaloukkaukset viestitään tietosuojan yhdyshenkilölle. Tietosuojan yhdyshenkilö välittää tiedon tietosuojavastaavalle. Tietosuojan yhdyshenkilön ei tarvitse tehdä ilmoitusta tietosuojavastaavalle, jos (1) loukkaus on merkitykseltään vähäinen, (2) se saadaan välittömästi korjattua, ja (3) rekisteröityjen tiedot eivät ole tosiasiassa vaarantuneet. Tietosuojan yhdyshenkilöllä on aina oikeus tehdä ilmoitus kaikista tietosuojaloukkauksista tietosuojavastaavalle.

Henkilötietojen tietoturvaloukkauksesta täytyy ilmoittaa valvontaviranomaiselle, jos loukkauksesta voi aiheutua riski luonnollisten henkilöiden oikeuksille ja vapauksille. Henkilötietojen tietoturvaloukkauksesta on ilmoitettava tietosuojavaltuutetun toimistolle ilman aiheetonta viivytystä 72 tunnin kuluessa. Henkilötietojen tietoturvaloukkauksesta on ilmoitettava rekisteröidylle, jos se todennäköisesti aiheuttaa korkean riskin tämän oikeuksille ja vapauksille.

Lisätiedot riskin arvioinnista ja ilmoitusvelvollisuudesta: tietosuojavaltuutetun toimisto.