TIETOSUOJA PÄHKINÄNKUORESSA

Tietosuojaopas yrityksille

ISBN: 978-952-5620-92-4
Minna Aalto-Setälä ja Mikko Viitaila
Tietosuoja pähkinänkuoressa. Tietosuojaopas yrityksille.
Helsinki: Keskuskauppakamari, 2018

1. ESIPUHE

Euroopan unionin tietosuoja-asetuksen soveltaminen alkoi 25.5.2018. Se on kaikissa EU-maissa suoraan sovellettavaa lainsäädäntöä. Mitään erillisiä kansallisia päätöksiä ei siis tarvita. Suomen uudella tietosuojalailla voidaan kuitenkin käyttää tietosuoja-asetuksen sallima liikkumavara täydentämällä ja täsmentämällä asetuksen säännöksiä. Sen avulla voidaan saada aikaan jatkuvuutta suhteessa aiemmin voimassa olleeseen henkilötietolakiin, esimerkiksi henkilötunnuksen käsittelyn osalta. Tämä helpottaa yritysten ja muiden organisaatioiden sopeutumista uusiin tietosuojavaatimuksiin.

Yksilön suojelu henkilötietojen käsittelyn yhteydessä on perusoikeus. Tietosuoja-asetuksen tavoitteena on saattaa henkilötietojen suoja kaikissa EU-maissa samalle tasolle, digitaaliseen maailmaan sopivaksi. Se on osa kokonaisuutta, jolla pyritään yhdenmukaistamaan EU:n digitaalisen sisämarkkinan säännöksiä ja toimintatapoja sekä parantamaan eurooppalaisten yritysten mahdollisuuksia toimia nykyaikaisessa digitaalisessa ympäristössä. Lisäksi pyritään edistämään hyviä, turvallisia henkilötietojen käsittelyn menettelytapoja sekä parantamaan kuluttajien luottamusta digitaaliseen markkinaan.

Tietosuoja-asetus tuo yrityksille uusien velvollisuuksien lisäksi myös uusia mahdollisuuksia. Velvollisuuksien täyttäminen edellyttää suunnitelmallista tietojen hallinnan toteuttamista, voisi sanoa laatujärjestelmän käyttöönottamista tietojen hallinnassa. Vastapainona yrityksillä on mahdollisuus laajentaa markkina-aluettaan koko Euroopan alueelle. Kun vaatimukset täyttyvät yhdessä EU-jäsenvaltiossa, ne täyttyvät muissakin.

Tämän oppaan tarkoituksena on antaa lukijalle yleiskuva tietosuoja-asetuksen sisällöstä ja asetuksen vaatimista keskeisistä toimenpiteistä sekä niistä mahdollisuuksista, joita asetuksen toteuttaminen antaa liiketoiminnan kehittämiseen. Lähtökohtana on aktiivinen ja ennakoiva vaatimusten toteuttaminen, sillä se antaa mielestämme parhaat mahdollisuudet menestykselliseen toimintaan nopeasti muuttuvassa digitaalisessa maailmassa. Huomioithan opasta käyttäessäsi, että tietosuojaa on oppaassa käsitelty suppeasti ja yleisellä tasolla aiheeseen perehtymisen helpottamiseksi. Konkreettisissa käytännön kysymyksissä on syytä kääntyä tietosuojavaltuutetun toimiston tai muun tietosuojaa osaavan ammattilaisen puoleen.

Tämän oppaan tarkoituksena ei ole olla kattava opas tietoturvan hallintaan ja toteuttamiseen. Tietoturvallisuuden hallinnasta ja toteuttamisesta löytyy lisätietoja esimerkiksi kansainvälisen kauppakamarin tietoturvaoppaasta yrityksille (ICC Cyber security guide for business © 2015, International Chamber of Commerce).

Kiitämme lämpimästi oppaan tekemiseen saamastamme avusta tietosuojavaltuutettua Reijo Aarniota, viestintäjohtaja Anna Lauttamus-Kauppilaa, dosentti Max Oker-Blomia, lakimies Minna Frändeä, pääsihteeri Paula Palorantaa ja OTM Ninni Hambergia.

Minna Aalto-Setälä ja Mikko Viitaila

2. MIKSI TIETOSUOJA ON TÄRKEÄ?

Tietosuoja osana jokaisen arkea

EU:n perusoikeuskirjan henkilötietojen suojaa koskevan säännöksen mukaan jokaisella on oikeus henkilötietojen suojaan. Tietojen käsittelyn on oltava asianmukaista ja sen on tapahduttava tiettyä tarkoitusta varten ja asianomaisen henkilön suostumuksella tai muun laissa säädetyn oikeuttavan perusteen nojalla. Jokaisella on oikeus tutustua tietoihin, joita hänestä on kerätty ja saada mahdolliset virheelliset tiedot oikaistuksi. Viranomainen valvoo näiden sääntöjen noudattamista.

Tietosuojalla tarkoitetaan siis yksilön oikeutta omiin henkilötietoihin ja hänen yksityisyytensä suojaamista käsiteltäessä henkilötietoja. Tietosuojan merkitys kasvaa jatkuvasti digitalisoituvassa ja verkottuvassa maailmassamme. Informaatioteknologia ja digitalisoituminen vaikuttavat keskeisesti siihen, miten henkilötietoja käsitellään ja miten kunkin yksilön ja yrityksen tulisi omassa toiminnassaan tähän suhtautua. Joudumme lähes päivittäin tekemään päätöksiä siitä, mihin annamme tai emme anna itseämme koskevia tietoja.

Vaikka tämä opas on erityisesti pyritty kirjoittamaan yrityksille selventämään ja auttamaan keskeisten tietosuojaan liittyvien käsitteiden ja periaatteiden ymmärtämisessä, aivan yhtä tärkeää on hahmottaa se, että tietosuoja koskee meitä kaikkia. Kyse on meidän kaikkien, sinun ja minun, lapsiemme, vanhempiemme, lastenlastemme ja isovanhempiemme tiedoista ja siitä, miten niitä käsitellään niin yhteiskunnassa kuin myös osana yritysten liiketoimintaa. Tosiasia on, ettei kukaan meistä voi enää päättää, ettei halua olla mukana verkottuneessa ympäristössä ja antaa ainakin joitakin tietoja sähköisiin palveluihin. Yhä isompi osa päivittäisestä viestinnästä ja viranomaisten hallussa olevista tiedoista on olemassa ainoastaan sähköisessä muodossa.

Tietosuoja kilpailutekijänä

Viime vuosien tietomurrot ja niistä aiheutuneet vahingot yrityksille ja organisaatiolle ovat olleet todella merkittäviä. Asiakkaat, olivatpa ne yritysasiakkaita tai yksityishenkilöitä, ovat viime vuosien tapahtumien seurauksena entistä kiinnostuneempia siitä, missä ja miten heidän henkilötiedoistaan huolehditaan. Asiakkaiden luottamus on monelle yritykselle olemassaolon ja menestyksen edellytys ja menetettyä luottamusta on vaikea, joskus jopa mahdotonta, rakentaa uudelleen. Tietosuoja-asetuksen perimmäisenä tarkoituksena on taata tämän luottamuksen perusedellytykset ja asettaa organisaatiolle ja yrityksille lähtökohtaiset säännöt, miten tietosuojasta tulee huolehtia. Voidaankin väittää, että tulevaisuudessa parhaiten menestyvät ne yritykset ja organisaatiot, jotka toiminnallaan onnistuvat saavuttamaan maineen tietosuojasta ja -turvallisuudesta hyvin huolehtivina toimijoina.

3. TIETOSUOJAA KOSKEVAT OIKEUSLÄHTEET

EU-lainsäädäntö

Yhteisölainsäädännöllä on Suomessa EU:n jäsenvaltiona hyvin suuri merkitys. Uusi tietosuoja-asetus on Suomessa tärkein henkilötietojen käsittelyä koskeva säädös. Se on sellaisenaan sovellettavaa oikeutta koko EU:n alueella. Sitä sovelletaan kaikkeen henkilötietojen käsittelyyn olipa kyse rekisterinpidosta yrityksessä tai henkilötietojen käsittelystä vaikkapa urheiluseurassa.

Uuden asetuksen taustalta löytyvät EU:n henkilötietodirektiivi ja EU:n perusoikeuskirjan säännökset yksityiselämän ja henkilötietojen suojasta. Henkilötietodirektiivin voimassaolo päättyi, kun tietosuoja-asetusta alettiin soveltaa 25.5.2018. Vaikka henkilötietojen käsittelyyn liittyvät yleiset periaatteet pääpiirteiltään säilyivät, asetus tuo mukanaan myös merkittäviä muutoksia. Tällaisia ovat muun muassa säännösten soveltaminen myös henkilötietojen käsittelijään, velvollisuus ilmoittaa tietoturvaloukkauksista, vaikutustenarvioinnin tekeminen, tietosuojavastaavan nimittäminen ja hallinnolliset sakot eli seuraamusmaksut.

Myös viranomaispuolella on tapahtunut muutoksia, sillä asetuksella perustettiin Euroopan tietosuojaneuvosto (European Data Protection Board, EDPB). Se soveltaa ja tulkitsee toiminnassaan asetusta. Tietosuojaneuvoston tehtävä on varmistaa, että tietosuoja-asetusta sovelletaan johdonmukaisesti koko EU:n alueella ja että valvontaviranomaisten välinen yhteistyö on tehokasta. Se antaa ohjeita asetuksen tulkinnasta ja tekee tietosuojaa koskevia päätöksiä riita-asioissa, joissa on kyse rajat ylittävästä henkilötietojen käsittelystä. Tietosuojaneuvosto pyrkii varmistamaan, että asetusta sovelletaan yhdenmukaisesti eri jäsenvaltioissa. Pyrkimyksenä on myös välttää saman asian käsittelyä eri jäsenmaissa.

Suomalainen lainsäädäntö

Uudella tietosuojalailla täsmennetään ja täydennetään tietosuoja-asetusta. Siinä säädetään esimerkiksi vastaavalla tavalla kuin aiemmassa henkilötietolaissa henkilötunnuksen käsittelystä. Tällä hetkellä suomalaista henkilötietojen käsittelyä koskevat säännökset ovat hyvin hajallaan, sillä tietosuojasta säädellään yli 800 laissa. Esimerkiksi henkilötietojen käsittelyä työsuhteessa säätelee työelämän tietosuojalaki (759/2004). Sähköisen viestinnän tietosuojaa taas koskee laki sähköisen viestinnän palveluista (917/2014). Kyseistä säännöstä ollaan parasta aikaa uudistamassa EU:ssa, sillä komissio on antanut ePrivacy-asetusehdotuksen (COM/2017/010) osana digitaalisten sisämarkkinoiden edistämisstrategiaa. Sillä on tarkoitus täydentää tietosuoja-asetusta.

Oikeuskäytäntö

Viimeisenä oikeuslähteenä tulee mainita oikeus- ja soveltamiskäytäntö. Suomessa viranomaisten ja tuomioistuinten ratkaisut ovat linjanneet tietosuojan soveltamista käytännössä. Tietosuojavaltuutetun kannanotot, lausunnot, päätökset ja monet valtuutetun toimiston oppaat ovat ohjanneet suomalaisia lain soveltamisessa. Tietosuojalautakunnan lausunnot ovat olleet tärkeitä tulkintaohjeita, sillä korkeimmalta oikeudelta ja korkeimmalta hallinto-oikeudelta ratkaisuja löytyy eri ongelmatilanteisiin niukasti.

Koska Suomen henkilötietolainsäädäntö perustuu EU:n säännöksiin, komission sekä neuvoston päätöksillä ja tiedonannoilla sekä Euroopan unionin tuomioistuimen (EUT) ratkaisuilla on merkittävä rooli. EUT on keskeinen tietosuojaa ja sitä koskevien säännösten tulkitsija. EU:ssa on käytössä ennakkoratkaisumenettely, jossa kansallinen tuomioistuin voi pyytää EUT:lta ratkaisua EU-oikeuden tulkintaa tai pätevyyttä koskevaan kysymykseen. Tällä pyritään varmistamaan EU-normien yhtenevä tulkinta ja soveltaminen koko unionissa.

Tärkeitä EUT:n ratkaisuja ovat esimerkiksi Google (C-131/12) ja Schrems (C-362/14). Ne ovat ohjanneet myös suomalaista oikeuskäytäntöä ja vaikuttaneet olennaisesti muun muassa uuden tietosuoja-asetuksen sisältöön. EU:n tietosuojaryhmän eli WP 29:n kannanotot ovat muovanneet eurooppalaista tietosuojaa. Jatkossa Euroopan tietosuojaneuvosto tulee ohjaamaan ja tulkitsemaan eurooppalaista tietosuojaa ja yksityisyyden suojaan liittyviä asioita. Myös Euroopan ihmisoikeustuomioistuin on antanut tietosuojaa koskevia ratkaisuja.

Kansainväliset sopimukset

Vaikka tietosuoja on oikeuden alana suhteellisen uusi, se on luonteeltaan hyvin kansainvälistä. Kansainväliset sopimukset ovat vaikuttaneet suomalaisen tietosuojan kehitykseen. Kansainvälisen yhteistyön tuloksena on syntynyt OECD:n suosituksia (muun muassa The 2013 OECD Privacy Guidelines), joiden pohjalta on syntynyt reilun tietosuojan periaatteet ja YK:n kansainvälinen sopimus koskien tietojenkäsittelytietojen säätämistä koskevia suuntaviivoja (U.N. Guidelines Concerning Computerized Data Files, 1990). Myös kansainvälisesti sovituilla standardeilla, kuten ISO/IEC 27001 ja ISO/EIC 27018, on iso vaikutus tietosuojan kehitykseen.

4. KESKEISET KÄSITTEET

Anonymisointi ja pseudonymisointi

Anonymisoinnilla tarkoitetaan henkilötiedon tunnistettavuuden poistamista siten, että rekisteröidyn tunnistaminen tai yksittäisen tiedon yhdistäminen häneen ei ole enää mahdollista. Tietosuoja-asetusta ei sovelleta anonymisoituihin tietoihin. Tällöin siis tietojen tunnistettavuus on lopullisesti poistettu siten, että rekisteröidyn suora tai epäsuora tunnistaminen ei ole mahdollista edes käyttämällä lisätietoja. Esimerkiksi tilastotieto on anonyymi tieto.

Pseudonymisoinnilla tarkoitetaan henkilötietojen julkaisemista ikään kuin salanimellä. Tällöin henkilötietoja käsitellään siten, ettei tietoja voida enää yhdistää tiettyyn rekisteröityyn käyttämättä lisätietoja. Tällaiset lisätiedot on säilytettävä erillään ja erilaisin toimenpitein varmistetaan, ettei henkilötietoja voida yhdistää tunnistettuun tai tunnistettavissa olevaan henkilöön. Tietosuoja-asetuksen mukaan pseudonymisoitu tieto on kuitenkin henkilötieto.

Arkaluonteiset henkilötiedot

Arkaluonteisia henkilötietoja ovat tiedot, joista ilmenee rotu tai etninen alkuperä, poliittinen mielipide, uskonnollinen tai filosofinen vakaumus, ammattiliiton jäsenyys, geneettinen tai biometrinen tieto, terveystieto tai seksuaaliseen suuntautumiseen taikka käyttäytymiseen liittyvä tieto. Pääsäännön mukaan näitä erityisiä henkilötietoryhmiä koskevien tietojen käsittely on kiellettyä. Asetuksessa on säännelty niiden käsittelystä tietyissä tilanteissa, kuten silloin, kun rekisteröity on antanut nimenomaisen suostumuksen tai kun käsittely on tarpeen tärkeästä yleistä etua koskevasta syystä.

Hallinnollinen sakko

Valvontaviranomainen voi määrätä hallinnollisen sakon tietosuoja-asetuksen rikkomisesta. Sakon määrä voi olla huomattava eli enintään 20 miljoonaa euroa tai 4 prosenttia yrityksen edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta. Viranomaisella on laajat toimivaltuudet ja harkintavalta seuraamuksista päätettäessä. Suomen tietosuojalaissa hallinnollisia sakkoja kutsutaan hallinnollisiksi seuraamusmaksuiksi. Niitä ei voi Suomessa tietosuojalain mukaan määrätä julkisen sektorin toimijalle.

Henkilötieto

Henkilötiedolla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan yksityishenkilöön liittyviä tietoja, joita voivat olla muun muassa nimi, henkilötunnus, kuva, biometrinen tai geneettinen tieto.

Tunnistettavissa olevana yksityishenkilönä pidetään henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen tai yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurisen tai sosiaalisen tekijän perusteella.

Henkilötietodirektiivi

EU:n henkilötietojen suojaa koskeva direktiivi (Euroopan parlamentin ja neuvoston direktiivi yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta; 95/46/EY, 24.10.1995), jonka voimassaolo päättyi tietosuoja-asetuksen soveltamisen alkaessa 25.5.2018.

Henkilötietojen käsittelijä

Henkilötietojen käsittelijällä tarkoitetaan yksityishenkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka käsittelee henkilötietoja rekisteripitäjän lukuun.

Henkilötietojen käsittely

Henkilötietojen käsittely tarkoittaa laajasti kaikenlaisia toimintoja, joita kohdistetaan henkilötietoihin automaattisella tietojenkäsittelyllä tai manuaalisesti. Käsittelyä ovat esimerkiksi henkilötietojen kerääminen, tallentaminen, järjestäminen, jäsentäminen, säilyttäminen, muokkaaminen, muuttaminen, hakeminen, kysely, käyttäminen, luovuttaminen, siirtäminen, levittäminen, saataville saattaminen, yhteensovittaminen, yhdistäminen, rajoittaminen, poistaminen tai hävittäminen.

Henkilötietojen tietoturvaloukkaus

Henkilötietojen tietoturvaloukkaus tarkoittaa tietoturvaloukkausta, jonka seurauksena vahingossa tai lainvastaisesti aiheutuu henkilötietojen tuhoutumista, häviämistä, muuttumista, luvatonta paljastumista tai niihin pääsyä. Tietoturvaloukkauksesta aiheutuu usein henkilötietojen lainvastaista käyttöä.

Lapsen henkilötietojen käsittely

Kun alle 16-vuotiaalle lapselle tarjotaan tietoyhteiskunnan palveluja, lapsen henkilötietojen käsittely on sallittua vain vanhemman suostumuksella. Jäsenvaltio voi säätää alemman ikärajan, joka saa minimissään olla 13 vuotta. Suomi noudattaa tietosuojalain mukaan 13 vuoden ikää.

Tietoyhteiskunnan palvelulla tarkoitetaan sähköisenä etäpalveluna vastaanottajan henkilökohtaisesta pyynnöstä toimitettavaa palvelua. Tällaisia ovat esimerkiksi käyttäjän sähköinen tunnistaminen verkossa, sosiaalisen median käyttäminen ja videoiden katselu netissä.

Rekisterinpitäjän on toteutettava kohtuulliset toimenpiteet tarkistaakseen, että vanhemman suostumus on olemassa ottaen huomioon käytettävissä olevan teknologian. Esimerkiksi pilvipalveluissa vanhemman suostumus vaaditaan ennen kuin lapsen tili tai käyttäjätunnus voidaan perustaa. Yksi yleisesti käytetty menetelmä varmistaa asia on vaatimus luottokortin käyttämisestä. Tällöin kortilta veloitetaan pieni summa, jonka voi usein käyttää muihin tarkoituksiin. Tarkoitus on siis tarkistaa vanhemman suostumuksen olemassaolo eikä tehdä suostumuksen antamisesta maksullista.

Luonnollinen henkilö

Lainsäädännössä käytetään termiä “luonnollinen henkilö” tarkoitettaessa ihmistä ja termiä “oikeushenkilö” tarkoitettaessa yrityksiä ja yhteisöjä. Tässä oppaassa käytetään lukemisen helpottamiseksi termiä “yksityishenkilö” viitattaessa luonnolliseen henkilöön.

Osoitusvelvollisuus

Rekisterinpitäjä vastaa siitä, että se noudattaa henkilötietojen käsittelyssä tietosuoja-asetuksen mukaisia periaatteita, joita ovat

1. lainmukaisuus, kohtuullisuus ja läpinäkyvyys
2. käyttötarkoitussidonnaisuus
3. tietojen minimointi
4. täsmällisyys
5. säilytyksen rajoittaminen, sekä
6. eheys ja luottamuksellisuus.

Rekisterinpitäjän on pystyttävä osoittamaan, että näitä periaatteita on noudatettu. Tätä kutsutaan osoitusvelvollisuudeksi. Henkilötietojen käsittelyä koskevista periaatteista ja osoitusvelvollisuudesta tarkemmin kohdassa 5.

Profilointi

Profilointi tarkoittaa mitä tahansa henkilötietojen automaattista käsittelyä, jossa henkilötietoja käyttämällä arvioidaan yksityishenkilön tiettyjä ominaisuuksia analysoimalla tai ennakoimalla näkökohtia, jotka liittyvät kyseisen henkilön työsuoritukseen, taloudelliseen tilanteeseen, terveyteen, henkilökohtaisiin mieltymyksiin, kiinnostuksen kohteisiin, luotettavuuteen, käyttäytymiseen, sijaintiin tai liikkeisiin.

Profilointi on lähtökohtaisesti sallittua. Jos profiloinnin avulla tehdään automatisoituja päätöksiä, tulee noudattaa erityisedellytyksiä. Jos profilointi liittyy suoramarkkinointiin, sen voi aina kieltää. Rekisteröidyllä voi myös olla oikeus vastustaa profilointia vedoten henkilökohtaiseen erityiseen tilanteeseen. Rekisteröidylle on kerrottava vastustamisoikeudesta. Vastustamisoikeudesta tarkemmin kohdassa 6.6.

Rekisteröity

Yksityishenkilö, jonka henkilötietoja käsitellään.

Rekisterinpitäjä

Rekisterinpitäjällä tarkoitetaan yksityis- tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka yksin tai yhteistyössä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.

Seloste käsittelytoimista

Rekisterinpitäjän ja henkilötietojen käsittelijän on ylläpidettävä selostetta, joka vastaa pitkälti henkilötietolain mukaista rekisteriselostetta. Selosteessa on informoitava henkilötietojen vastaanottajista ja tietojen siirroista EU:n tai Euroopan talousalueen ulkopuolelle.

Yrityksen tai muun yhteisön, jossa on alle 250 työtekijää, ei tarvitse laatia selostetta paitsi, jos käsittely aiheuttaa todennäköisesti riskin rekisteröidyn oikeuksille ja vapauksille, käsittely ei ole satunnaista tai käsittely kohdistuu arkaluonteisiin tietoihin.

Sertifiointi

Tietosuoja-asetus tuo mukanaan uusia sertifiointitapoja, joita ovat sertifikaatti, tietosuojasinetti ja -merkki. Tarkoituksena on lisätä läpinäkyvyyttä ja tehostaa lainsäädännön noudattamista, jotta rekisteröidyt voisivat nopeasti arvioida tarjotun tuotteen tai palvelun tietosuojan tason. Eri sertifiointitapojen avulla rekisterinpitäjä ja henkilötietojen käsittelijä voivat puolestaan osoittaa noudattavansa vaadittua tietosuojaa ja hyvää tietojenkäsittelytapaa.

Monet isot palvelutarjoajat ovat osoittaneet vaatimustenmukaisuutensa kansainvälisillä standardeilla. Tällaisia ovat esimerkiksi ISO27018 (yksityisyyden suoja pilvipalveluissa) tai ISO27001 (tietoturvallisuuden hallintajärjestelmä). Tätä kirjoitettaessa erillistä tietosuoja-asetuksen vaatimusten mukaisuuden osoittavaa standardia ei ole vielä olemassa. Sertifioituja palveluntarjoajia käyttämällä organisaatiot voivat varmistua siitä, että heidän käyttämänsä palvelut ovat myös käsittelijälle asetettujen tietosuoja-asetuksen vaatimusten mukaisia.

Suostumus

Suostumuksen tulee olla vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen tahdonilmaisu. Rekisterinpitäjän on pystyttävä osoittamaan, että rekisteröity on antanut suostumuksen henkilötietojensa käsittelyyn. Suostumuksen antamista koskeva pyyntö tulee esittää selvästi erillään muista asioista ja helposti ymmärrettävässä muodossa. Rekisteröidyllä on oikeus peruuttaa suostumuksensa milloin tahansa, mistä rekisterinpitäjän tulee ilmoittaa ennen suostumuksen antamista.

Tietosuoja-asetus

Yleinen tietosuoja-asetus eli General Data Protection Regulation (Euroopan parlamentin ja neuvoston asetus luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (EU) 2016/679, 27.4.2016; yleinen tietosuoja-asetus, GDPR). Tässä oppaassa käytetään luettavuuden helpottamiseksi yleiseen tietosuoja-asetukseen viitattaessa termejä "tietosuoja-asetus" tai "asetus" .

Tietosuojavastaava

Rekisterinpitäjän ja henkilötietojen käsittelijän on nimettävä tietosuojavastaava, kun niiden toiminnan ydintehtävät muodostuvat henkilötietojen käsittelytoimista, jotka luonteensa, laajuutensa tai tarkoituksensa vuoksi edellyttävät laajamittaista rekisteröityjen säännöllistä ja järjestelmällistä seurantaa. Samoin on myös silloin, kun ydintehtävänä on henkilötietojen laajamittainen käsittely, joka kohdistuu arkaluonteisiin henkilötietoihin, rikostuomioihin tai rikoksia koskeviin tietoihin. Viranomaisille ja julkishallinnon elimille, jotka käsittelevät henkilötietoja, tietosuojavastaavan nimittäminen on aina pakollista (ei koske tuomioistuinta).

Yritysryhmä voi nimittää yhden yhteisen tietosuojavastaavan ja vastaavasti yksi tietosuojavastaava voidaan määrätä hoitamaan useamman viranomaisen tai julkishallinnon elimen kyseisiä tehtäviä.

Tietoturva

Tietoturvalla tarkoitetaan tietojen, palvelujen, järjestelmien ja tietoliikenteen suojaamista. Keskeisiä tietoturvan käsitteitä ovat saatavuus tai käytettävyys, luottamuksellisuus ja eheys. Saatavuudella tai käytettävyydellä tarkoitetaan sitä, että tieto on saatavilla, kun sitä tarvitaan. Luottamuksellisuudella tarkoitetaan sitä, että tietoa saavat käsitellä vain sellaiset henkilöt, joilla on tähän oikeus. Eheydellä taas tarkoitetaan sitä, että tieto ei saa muuttua vahingossa tai hyökkäyksen seurauksena taikka muutos pitää ainakin pystyä havaitsemaan.

Vaikutustenarviointi

Vaikutustenarvioinnilla tarkoitetaan suunniteltujen henkilötietojen käsittelytoimien vaikutusten arviointia suhteessa tietosuojaan ja yksilön oikeuksiin. Jos käsittely todennäköisesti aiheuttaa rekisteröidyn kannalta korkean riskin, rekisterinpitäjän on ennen käsittelyä toteutettava tietosuojan vaikutustenarviointi ja määriteltävä toimia, joilla riskiä voidaan hallita.

Vaikutustenarviointi vaaditaan erityisesti, kun tehdään 1) ihmisten henkilökohtaisten ominaisuuksien järjestelmällistä, kattavaa ja automaattista arviointia (kuten profilointia), joka johtaa oikeusvaikutuksia sisältäviin päätöksiin tai joka muuten vaikuttaa ihmiseen merkittävästi, 2) arkaluonteisten henkilötietojen laajamittaista käsittelyä tai 3) yleisölle avoimen alueen järjestelmällistä ja laajamittaista valvontaa. Valvontaviranomainen voi myös määritellä käsittelytyyppejä, jolloin on tehtävä vaikutustenarviointi.

Tietosuojan vaikutustenarvioinnissa tulee olla vähintään kuvaus suunnitelluista käsittelytoimista ja käsittelyn tarkoituksista, arvio käsittelytoimien tarpeellisuudesta ja oikeasuhteisuudesta tarkoituksiin nähden, arvio rekisteröityjen oikeuksia ja vapauksia koskevista riskeistä ja suunnitellut toimenpiteet riskeihin puuttumiseksi. Tarvittaessa rekisterinpitäjän on tehtävä uudelleentarkastelu. Rekisterinpitäjän on kuultava valvontaviranomaista ennen käsittelyä, jos vaikutustenarviointi osoittaa, että käsittely aiheuttaisi korkean riskin rekisteröidylle ja rekisterinpitäjä ei ole toteuttanut toimenpiteitä riskin pienentämiseksi.

Valvontaviranomaiset

Suomessa kansallisena valvontaviranomaisena toimii tietosuojavaltuutettu. Hän toimii tietosuojavaltuutetun toimiston päällikkönä. Toiminnassaan tietosuojavaltuutettu on itsenäinen ja riippumaton. Tietosuojavaltuutettu on Euroopan tietosuojaneuvoston jäsen.

Usean EU:n jäsenvaltion alueella toimiva rekisterinpitäjä tai henkilötietojen käsittelijä asioi pääsääntöisesti päätoimipaikkansa valvontaviranomaisen kanssa henkilötietojen käsittelyyn liittyvien asioiden osalta. Tämä viranomainen toimii johtavana valvontaviranomaisena suhteessa toisiin tietosuojaviranomaisiin, joiden alueilla rekisterinpitäjä tai henkilötietojen käsittelijä toimii. Näin poistuu tarve asioida erikseen usean jäsenvaltion valvontaviranomaisen kanssa.

WP 29

WP 29 tai *Working Party 29* nimillä on kutsuttu EU:n tietosuojatyöryhmää, joka toimi riippumattomana neuvoa-antava työryhmänä, koska siitä säädettiin henkilötietodirektiivin 29 artiklassa. Se koostui jäsenvaltioiden ja komission edustajista sekä Euroopan tietosuojavaltuutetusta. Se on antanut lukuisia lausuntoja ja suosituksia tietosuojasta ja yksityisyyden suojaan liittyvistä kysymyksistä. Sen työtä jatkaa Euroopan tietosuojaneuvosto.

Yhdenmukaisuusmekanismi

Tietosuoja-asetus on suoraan sovellettavaa oikeutta koko EU:n alueella ja sillä pyritään yhdenmukaistamaan eurooppalaista tietosuojaa. Tästä syystä kaikkia yhteisöalueella toimivia koskee samat säännöt. Jäsenvaltioiden valvontaviranomaisten ja komission on tehtävä yhteistyötä varmistaakseen lainsäädännön yhteydenmukainen soveltaminen EU:ssa. Euroopan tietosuojaneuvosto voi muun muassa antaa tietosuoja-asetuksen soveltamisesta sitovia päätöksiä. Tällä tavoin se varmistaa tietosuojan yhdenmukaisuutta EU:ssa.

5. HENKILÖTIETOJEN KÄSITTELYÄ KOSKEVAT PERIAATTEET

5.1 Tietosuoja-asetuksessa on määritelty henkilötietojen käsittelyä koskevat periaatteet, jotka ohjaavat rekisterinpitäjää käsittelemään henkilötietoja rekisteröidyn oikeuksia ja vapauksia kunnioittavalla tavalla. Nämä periaatteet ovat:

Lainmukaisuus, kohtuullisuus ja läpinäkyvyys

Henkilötietoja on käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi.

Käyttötarkoitussidonnaisuus

Henkilötiedot on kerättävä tiettyä, nimenomaista ja laillista tarkoitusta varten, eikä niitä saa käsitellä myöhemmin näiden tarkoitusten kanssa yhteensopimattomalla tavalla.

Jos tietoja käsitellään myöhemmin yleisen edun mukaisen arkistoinnin, tieteellisen tai historiallisen tutkimuksen tai tilastoimisen vuoksi, tällainen käyttö ei ole yhteensopimatonta alkuperäisen tarkoituksen kanssa.

Tietojen minimointi

Henkilötietojen on oltava asianmukaisia ja olennaisia sekä rajoituttava siihen, mikä on tarpeellista suhteessa niihin tarkoituksiin, joita varten niitä käsitellään.

Täsmällisyys

Henkilötietojen on oltava täsmällisiä ja tarvittaessa päivitettyjä. Rekisterinpitäjän on toteutettava kaikki mahdolliset kohtuulliset toimenpiteet sen varmistamiseksi, että käsittelyn tarkoituksiin nähden epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä.

Säilytyksen rajoittaminen

Henkilötiedot on säilytettävä sellaisessa muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoituksen toteuttamista varten. Henkilötietoja voidaan säilyttää pidempiä aikoja, jos henkilötietoja käsitellään ainoastaan yleisen edun mukaisia arkistointitarkoituksia taikka tieteellisiä tai historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten edellyttäen, että tietosuoja-asetuksen edellyttämiä asianmukaisia teknisiä ja organisatorisia toimenpiteitä on pantu täytäntöön rekisteröidyn oikeuksien ja vapauksien turvaamiseksi.

Rekisterinpitäjällä on siis oikeus säilyttää rekisterissä tunnistettavassa muodossa olevia henkilötietoja vain niin kauan kuin on tarpeen tietojenkäsittelyn tarkoituksen toteuttamista varten. Käytännössä tämä asia toteutetaan henkilötietojen elinkaaren hallinnalla.

Eheys ja luottamuksellisuus

Henkilötietoja on käsiteltävä tavalla, jolla varmistetaan henkilötietojen asianmukainen turvallisuus. Tämä pitää sisällään tietojen suojaamisen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta käyttäen asianmukaisia teknisiä tai organisatorisia toimia.

Henkilötietojen suojaamisesta on huolehdittava käsittelyn kaikissa vaiheissa eli tietojen keräämisestä tietojen poistamiseen. Tietojen suojaaminen edellyttää henkilötietojen käsittelyn seuraamista ja valvontaa.

Rekisterinpitäjä vastaa siitä, että edellä luetellut henkilötietojen käsittelyä koskevat periaatteet on otettu huomioon sen toiminnassa, ja sen on pystyttävä myös osoittamaan se. Tätä kutsutaan osoitusvelvollisuudeksi. Käytännössä rekisterinpitäjä voi toteuttaa tämän dokumentoimalla omat toimenpiteensä.

5.2 Osoitusvelvollisuus

Rekisterinpitäjä vastaa osoitusvelvollisuuden toteuttamisesta. Osoitusvelvollisuudesta käytetään englanninkielistä termiä accountability. Sen mukaan rekisterinpitäjän on pystyttävä jälkikäteen osoittamaan, että tietosuoja-asetuksen mukaisia henkilötietojen käsittelyä koskevia periaatteita on noudatettu käytännössä. Tämä edellyttää henkilötietojen käsittelyyn liittyvien prosessien sekä tieto-suojaperiaatteiden käytännön toteuttamisen dokumentointia sekä teknisiä ja organisatorisia toimenpiteitä. Yrityksen on rekisterinpitäjänä pystyttävä näyttämään, että henkilötietojen käsittelyä koskevia periaatteita noudatetaan.

Tietosuojaa koskevilta toimilta edellytetään ennakoitavuutta, mikä voidaan toteuttaa suunnittelemalla, varautumalla ja kyvykkyydellä osoittaa toteutetut toimenpiteet. Yrityksen käytännön toimintaa auttavat selkeästi etukäteen määritellyt vastuut ja toimintatavat sekä menetelmät siitä, miten henkilötietoja käsitellään. Yrityksen tulee pystyä jälkikäteen osoittamaan, että lainsäädännön vaatimukset ja riskit on otettu sen toiminnassa asianmukaisesti huomioon. Dokumentointi on olennainen osa tätä.

5.3 Käsittelyn lainmukaisuus

Henkilötietojen käsittelylle ja henkilörekisterin pitämiselle on aina oltava asetuksessa säädetty käsittelyn oikeusperuste. Käsittely on lainmukaista ainoastaan, jos ja vain siltä osin kuin vähintään yksi seuraavista edellytyksistä täyttyy:

- Rekisteröity on antanut suostumuksen henkilötietojensa käsittelyyn yhtä tai useampaa erityistä tarkoitusta varten
- Käsittely on tarpeen sopimuksen täytäntöön panemiseksi tai sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä
- Käsittely on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi
- Käsittely on tarpeen rekisteröidyn tai toisen yksityishenkilön elintärkeiden etujen suojaamiseksi
- Käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi
- Kyse on oikeutetusta edusta.

Oikeutettu etu käsittelyn oikeusperustana

Tällöin käsittely on tarpeen rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi, elleivät tietosuojan edellyttämät rekisteröidyn edut tai perusoikeudet ja -vapaudet syrjäytä tällaista oikeutettua etua, erityisesti silloin, kun rekisteröity on lapsi. Tällöin tehdään intressipunninta eri osapuolten välillä.

Oikeutettuun etuun vetoaminen edellyttää tilanteen kokonaisarviointia. Oikeutettua etua ei sovelleta silloin, kun viranomainen käsittelee tietoja. Henkilötietojen käsittely suoramarkkinointitarkoituksissa kuuluu oikeutetun edun piiriin eli oikeutetun edun perusteella yritys voi esimerkiksi markkinoida tuotteitaan ja palveluitaan potentiaalisille asiakkaille.

Myös henkilön asemaa julkisyhteisössä tai elinkeinoelämässä kuvaavien tietojen käsittely perustuu oikeutettuun etuun. Tämä on huomioitu henkilötietolaissa. Tällöin henkilötietoja voidaan käyttää, kun kyse on henkilön asemaa, tehtäviä ja niiden hoitoa julkisyhteisössä, elinkeinoelämässä, järjestötoiminnassa tai muussa vastaavassa toiminnassa kuvaavista tiedoista siltä osin, kun käsittelyn tavoite on yleisen edun mukainen ja käsittely on oikeasuhtaista sillä tavoiteltuun oikeutettuun päämäärään nähden.

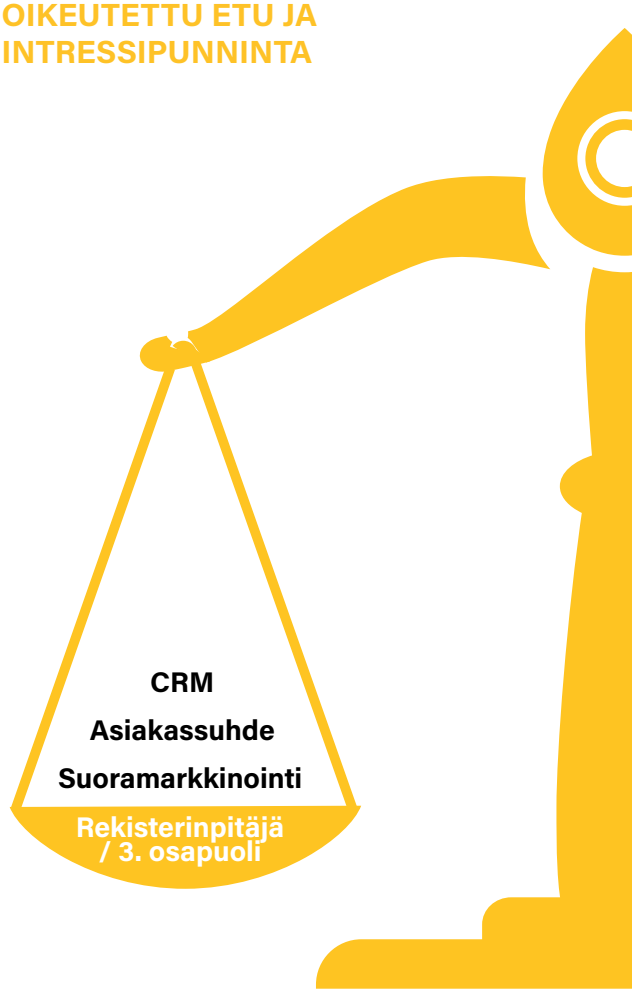
Jos käsittely tapahtuu muuta tarkoitusta varten kuin sitä, jonka vuoksi tiedot on kerätty, eikä käsittelyyn ole rekisteröidyn suostumusta tai se ei perustu lakiin, rekisterinpitäjän on varmistettava, että käsittely on tällöin yhteensopiva alkuperäisen käsittelytarkoituksen kanssa.

5.4 Rekisterinpitäjän ilmoitusvelvollisuus

Rekisterinpitäjän on toimitettava rekisteröidylle tietosuoja-asetuksen mukaiset käsittelyä koskevat tiedot tiiviisti, läpinäkyvästi ja helposti ymmärrettävästi ja saatavilla olevassa muodossa selkeällä ja yksinkertaisella kielellä. Tämä velvollisuus korostuu erityisesti, kun tiedot on tarkoitus antaa lapselle.

Tiedot on annettava kirjallisesti tai muulla tavoin. Tiedot voidaan antaa myös sähköisesti. Jos rekisteröity pyytää, tiedot voidaan antaa suullisesti. Tällöin edellytetään, että rekisteröidyn henkilöllisyys voidaan vahvistaa. Rekisteröidyllä on oltava mahdollisuus tietää, miten ja missä määrin häntä koskevia tietoja kerätään ja käytetään. Ilmoitusvelvollisuuden käytännön toteutus on tärkeää, koska tällöin rekisteröityä informoidaan tietojen käsittelystä ja koska se on suostumuksen edellytys, mutta myös sen vuoksi, että se vaikuttaa rekisteröidyn odotuksiin ja siten intressipunnintaan.

OIKEUTETTU ETU JA INTRESSIPUNNINTA



Toimitettavat tiedot, kun henkilötietoja kerätään rekisteröidyltä

Kun rekisteröidyltä kerätään häntä koskevia henkilötietoja, rekisterinpitäjän on toimitettava rekisteröidylle kaikki seuraavat tiedot:

- Rekisterinpitäjä ja hänen yhteystietonsa
- Mahdollisen tietosuojavastaavan yhteystiedot
- Henkilötietojen käsittelyn tarkoitukset ja käsittelyn oikeusperuste
- Rekisterinpitäjän tai kolmannen osapuolen oikeutetut edut, jos käsittely perustuu intressipunnintaan
- Henkilötietojen vastaanottajat tai vastaanottajaryhmät
- Tiedot siirroista kolmansiin maihin

Edellä mainittujen tietojen lisäksi rekisterinpitäjän on annettava rekisteröidylle seuraavat lisätiedot, jotka ovat tarpeen asianmukaisen ja läpinäkyvän käsittelyn takaamiseksi:

- Henkilötietojen säilytysaika tai, jos se ei ole mahdollista, ajan määrittämiskriteerit
- Rekisteröityjen oikeudet
- Oikeus peruuttaa suostumus
- Oikeus tehdä valitus valvontaviranomaiselle
- Onko henkilötietojen antaminen lakisääteistä, sopimukseen perustuvaa tai edellyttääkö sopimuksen tekeminen sitä
- Onko rekisteröidyn pakko toimittaa tiedot
- Tietojen antamatta jättämisen mahdolliset seuraukset
- Automaattisen päätöksenteon olemassaolo ja merkitykselliset tiedot käsittelyn logiikasta.

Jos rekisterinpitäjä aikoo käsitellä henkilötietoja muuhun tarkoitukseen kuin siihen, johon henkilötiedot kerättiin, sen tulee ilmoittaa rekisteröidylle ennen jatkokäsittelyä muusta tarkoituksesta ja antaa kaikki tarvittavat lisätiedot.

Jos rekisteröity on jo saanut tiedot, tietoja ei tarvitse antaa.

Toimitettavat henkilötiedot, kun tietoja ei ole saatu rekisteröidyltä

Kun tietoja ei ole saatu rekisteröidyltä itseltään, rekisterinpitäjän on toimitettava rekisteröidylle lähtökohtaisesti vastaavat tiedot kuin edellä on mainittu ja lisäksi:

- Kyseessä oleva henkilötietoryhmä
- Mistä henkilötiedot on saatu sekä tarvittaessa tieto siitä, onko tiedot saatu yleisesti saatavilla olevista lähteistä.

Rekisterinpitäjän on annettava tiedot kuukauden kuluessa henkilötietojen saamisesta tai kun rekisteröityyn ollaan yhteydessä. Jos henkilötietoja on tarkoitus luovuttaa toiselle vastaanottajalle, tiedot on annettava viimeistään silloin, kun tietoja luovutetaan ensimmäisen kerran.

Rekisterinpitäjä voi poiketa tiedonantovelvollisuudestaan, jos rekisteröity on jo saanut tiedot, tai tietojen yksilöllinen toimittaminen osoittautuu mahdottomaksi. Samoin jos tietojen toimittaminen vaatisi kohtuutonta vaivaa tai tietojen hankinnasta taikka luovuttamisesta säädetään nimenomaisesti. Myös tilanne, jossa tietoja koskee lainsäädäntöön perustuva vaitiolovelvollisuus, oikeuttaa poikkeamiseen tiedonantovelvollisuudesta.

6. REKISTERÖIDYN OIKEUDET

Tietosuoja kohdistuu yksityishenkilön yksityiselämään ja sen suojaamiseen. Yksilöllä on oikeus omiin henkilötietoihin. Rekisteröidyn oikeuksien taustalla on ajatus suojata yksilön henkilötietoja niiden oikeudetonta ja vahingollista käyttöä vastaan. Tietosuoja-asetus turvaa rekisteröidyn seuraavat oikeudet.

6.1 Oikeus saada pääsy tietoihin

Rekisteröidyllä on oikeus saada rekisterinpitäjältä tieto siitä, käsitelläänkö häntä koskevia tietoja ja mitä käsiteltävät tiedot ovat. Hänellä on oikeus saada jäljennös kyseisistä tiedoista. Tältä osin rekisteröidyn oikeudet säilyvät pitkälti samanlaisina kuin ne ovat olleet jo aiemmin voimassa olleen henkilötietolain mukaisesti.

Samalla rekisterinpitäjän tulee ilmoittaa rekisteröidylle seuraavat tiedot:

- Henkilötietojen käsittelyn tarkoitus
- Kyseessä olevat henkilötietoryhmät
- Henkilötietojen vastaanottaja, jos henkilötietoja luovutetaan kolmannelle osapuolelle
- Henkilötietojen säilytysaika tai kriteeri, jolla säilytysaika määräytyy
- Rekisteröidyn oikeudet koskien henkilötietojen oikaisemista, poistamista, käsittelyn rajoittamista tai vastustamisoikeuden käyttämistä
- Oikeus tehdä valitus valvontaviranomaiselle
- Jos henkilötietoja ei kerätä rekisteröidyltä itseltään, kaikki tietojen alkuperästä käytettävissä olevat tiedot
- Liittyykö käsittelyyn automaattisen päätöksentekoa tai profilointia sekä niiden käsittelylogiikasta ja tämän merkityksestä ja seurauksista rekisteröidylle
- Jos henkilötietoja siirretään EU:n ulkopuoliseen maahan, tieto siitä miten tietosuojasta on huolehdittu, eli mitä suojatoimia on käytetty.

Jos rekisteröity pyytää tietojaan sähköisesti, rekisterinpitäjän on annettava tiedot yleisesti käytetyssä sähköisessä muodossa. Tämä rekisterinpitäjän on hyvä ottaa huomioon niin tietojärjestelmiensä kuin myös henkilötietojen käsittelijöiden kannalta. Jos pyydetyt tiedot ovat hajallaan, pääsyoikeuden toteuttaminen voi viedä paljon aikaa. Rekisterinpitäjän kannattaa luoda määrämuotoinen toimintatapa rekisteröityjen pyyntöihin vastaamiseen ja tietojen keräämiseen.

6.2 Oikeus tietojen oikaisemiseen

Tietyt rekisteröidyn oikeudet ovat säilyneet voimassa aivan kuten aiemmin; rekisteröidyillä on oikeus tarkastaa itseään koskevat tiedot ja jos virheitä tai puutteita havaitaan, rekisterinpitäjän on oikaistava tiedot.

Rekisteröidyllä on oikeus vaatia, että rekisterinpitäjä oikaisee rekisteröityä koskevat epätarkat ja virheelliset henkilötiedot ilman aiheetonta viivytystä. Rekisteröidyllä on oikeus täydentää puutteellisia henkilötietojaan muun muassa antamalla lisäselvitys.

6.3 Oikeus poistaa tiedot eli oikeus tulla unohdetuksi

Rekisteröidyllä on oikeus saada rekisterinpitäjä poistamaan häntä koskevat henkilötiedot ja rekisterinpitäjällä on velvollisuus poistaa nämä tiedot ilman aiheetonta viivytystä. Tämä edellyttää, että jokin seuraavista perusteista soveltuu:

- Henkilötietoja ei tarvita niihin tarkoituksiin, joita varten ne kerättiin tai käsiteltiin
- Rekisteröity peruuttaa suostumuksen, eikä käsittelyyn ole muuta laillista perustetta
- Rekisteröity vastustaa käsittelyä vastustusoikeutensa perusteella (vastustusoikeutta käsitellään kohdassa 6.6)
- Tietoja on käsitelty lainvastaisesti
- Tiedot on poistettava rekisterinpitäjää koskevan lakisääteisen velvoitteen noudattamiseksi
- Tiedot on kerätty lapselta tietoyhteiskunnan palvelun yhteydessä.

Jos rekisterinpitäjä on julkistanut poistettavat henkilötiedot ja sillä on velvollisuus poistaa nämä tiedot, sen on ryhdyttävä kohtuullisiin toimenpiteisiin ilmoittaakseen tietoja käsitteleville muille rekisterinpitäjille, että rekisteröity on pyytänyt poistamaan henkilötietoihin liittyvät linkit, tietojen jäljennökset tai kopiot. Vaadittujen toimenpiteiden osalta voidaan ottaa huomioon käytettävissä oleva tekniikka ja aiheutuvat kustannukset.

Käytännössä oikeus tulla unohdetuksi voi tarkoittaa rekisteröidyn oikeutta peruuttaa antamansa suostumus. Suostumuksen peruuttamisen tulisi olla yhtä helppoa kuin sen antaminen. Tämä luonnollisesti asettaa rekisterinpitäjän käyttämälle järjestelmälle vaatimuksia.

Poikkeuksia oikeuteen tulla unohdetuksi voivat aiheuttaa sananvapaus, rekisterinpitäjän lakisääteinen velvoite, yleinen etu tai julkisen vallan käyttäminen, kansanterveyteen liittyvä yleinen etu, arkistointi, tieteellinen tai historiallinen tutkimus- tai tilastointitarkoitus taikka oikeudellisen vaatimuksen esittäminen.

OIKEUS TULLA UNOHDETUKSI

HENKILÖTIETOJA EI TARVITA NIIHIN TAREOITUKSIIN, JOITA VARTEN NE KERÄTTIIN TAI KÄSITELTIIN

REKISTERÖITY PERUUTTAA SUOSTUMUKSEN, EIKÄ KÄSITTELYYN OLE MUUTA LAILLISTA PERUSTETTA

REKISTERÖITY VASTUSTAA KÄSITTELYÄ VASTUSTUSOIKEUTENSA PERUSTEELLA

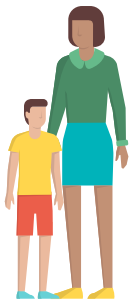
6.4 Oikeus siirtää tiedot järjestelmästä toiseen

Rekisteröidyllä on oikeus saada häntä koskevat tiedot jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa ja oikeus siirtää nämä tiedot toiselle rekisterinpitäjälle. Tämä edellyttää, että käsittely perustuu suostumukseen tai sopimukseen ja että käsittely tehdään automatisoidusti. Lähtökohtaisesti siirto-oikeus koskee henkilötietoja, jotka rekisteröity on toimittanut rekisterinpitäjälle.

Käytännössä rekisteröidyllä on oikeus saada häntä koskevat henkilötiedot yleisesti käytössä olevassa ja siirrettävässä muodossa ja siirtää nämä tiedot toiselle rekisterinpitäjälle. Oikeuteen kuuluu tietojen siirtäminen suoraan rekisterinpitäjältä toiselle ja järjestelmästä toiseen, jos se vain on teknisesti mahdollista. Siirto-oikeus ei edellytä, että rekisterinpitäjän oma järjestelmä olisi yhteensopiva toisen, esimerkiksi kilpailevan rekisterinpitäjän järjestelmän kanssa. Jos kahden rekisterinpitäjän järjestelmät ovat erilaisia, siirto voidaan tehdä esimerkiksi käyttämällä siirrettävää muistia, josta tiedot voidaan siirtää edelleen toiseen järjestelmään. Siirto-oikeus on oikeutena uusi. Vasta konkreettiset siirtopyynnöt tulevat näyttämään, miten sitä käytännössä toteutetaan.

TIETOJA ON KÄSITELTY LAINVASTAISESTI

TIEDOT ON POISTETTAVA REKISTERINPITÄJÄÄ KOSKEVAN LAKISÄÄTEISEN VELVOITTEEN NOUDATTAMISEKSI



TIEDOT ON KERÄTTY LAPSELTA TIETOYHTEISKUNNAN PALVELUN YHTEYDESSÄ.

Siirto-oikeuden käyttäminen ei saa rajoittaa oikeutta tulla unohdetuksi. Siirto-oikeutta ei sovelleta käsittelyyn, joka on tarpeen yleistä etua koskevan tehtävän suorittamista tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämistä varten. Siirto-oikeus ei saa myöskään vaikuttaa haitallisesti muiden oikeuksiin.

6.5 Oikeus käsittelyn rajoittamiseen

Rekisteröidyllä on oikeus vaatia, että rekisterinpitäjä rajoittaa hänen henkilötietojensa käsittelyä seuraavissa tilanteissa:

- jos rekisteröity kiistää tietojen paikkansapitävyyden. Tällöin käsittelyä rajoitetaan siksi, kunnes rekisterinpitäjä voi varmistua tietojen paikkansapitävyydestä
- käsittely on lainvastaista ja rekisteröity vastustaa henkilötietojen poistamista vaatien sen sijaan niiden käytön rajoittamista
- rekisterinpitäjä ei enää tarvitse kyseisiä henkilötietoja käsittelyn tarkoituksiin, mutta rekisteröity tarvitsee niitä oikeudellista vaadettaan varten
- rekisteröity on vedonnut vastustamisoikeuteensa ja odotetaan sen selvittämistä, syrjäyttävätkö rekisterinpitäjän oikeutetut perusteet rekisteröidyn perusteet.

Jos käsittelyä on rajoitettu, tietoja saa säilyttämistä lukuun ottamatta käsitellä vain rekisteröidyn suostumuksella, oikeudellisen vaatimuksen esittämistä varten, toisen henkilön oikeuksien suojaamiseksi tai yleistä etua koskevista syistä. Jos henkilötietojen käsittelyä on rajoitettu rekisteröidyn vaatimuksesta, rekisterinpitäjän on ilmoitettava rekisteröidylle ennen kuin rajoitus poistetaan.

6.6 Oikeus vastustaa käsittelyä, automaattista tietojen käsittelyä ja profilointia

Rekisteröidyllä on oikeus vastustaa tietojensa käsittelyä henkilökohtaiseen erityiseen tilanteeseensa liittyvällä perusteella, kun kyse on yleisestä edusta tai julkisen vallan käyttämisestä taikka oikeutetusta edusta, kuten profiloinnista. Rekisterinpitäjä ei saa tällöin enää käsitellä henkilötietoja, ellei hän voi osoittaa, että käsittelylle ole olemassa huomattavan tärkeä ja perusteltu syy, joka syrjäyttää rekisteröidyn oikeuden. Käsittely on myös mahdollista, jos se on tarpeen oikeudellisen vaatimuksen esittämisen vuoksi.

Rekisteröidyllä on aina oikeus vastustaa tietojensa käyttöä suoramarkkinointiin. Niin ikään rekisteröidyllä on oikeus kieltäytyä suoramarkkinointiin liittyvästä profiloinnista. Rekisteröidyllä on oikeus olla joutumatta sellaisen päätöksen kohteeksi, joka perustuu pelkästään automaattiseen tietojen käsittelyyn, kuten profilointiin, ja jolla on häntä koskevia oikeusvaikutuksia tai joka vaikuttaa häneen vastaavalla tavalla merkittävästi. Säännöstä automaattisesta tietojen käsittelystä ei sovelleta, jos päätös

- on välttämätön rekisteröidyn ja rekisterinpitäjän välisen sopimuksen vuoksi;
- on hyväksytty rekisterinpitäjään sovellettavassa lainsäädännössä, jossa vahvistetaan myös asianmukaiset toimenpiteet rekisteröidyn oikeuksien, vapauksien ja oikeutettujen etujen suojaamiseksi; tai
- perustuu rekisteröidyn nimenomaiseen suostumukseen.

Lähtökohtaisesti automaattista tietojen käsittelyä ei saa kohdistaa arkaluonteisiin tietoihin.

6.7 Rekisteröidyn oikeuksien käyttö

Rekisteröidylle on annettava maksutta tiedot viimeistään kuukauden kuluessa pyynnön vastaanottamisesta niistä toimenpiteistä, joihin rekisterinpitäjä ryhtynyt. Määräaikaa voidaan tarvittaessa jatkaa enintään kahdella kuukaudella, mutta tällöin rekisteröidylle on ilmoitettava viivästyksestä ja kerrottava viivästyksen syy.

Jos rekisteröity esittää pyynnön sähköisesti, tiedot on toimitettava mahdollisuuksien mukaan sähköisesti, ellei rekisteröity pyydä tietoja muussa muodossa. Tiedot on mahdollista antaa suullisesti, jos rekisteröity niin pyytää ja hänen henkilöllisyytensä voidaan vahvistaa.

Jos rekisteröidyn tekemät pyynnöt ovat ilmeisen perusteettomia tai kohtuuttomia, rekisterinpitäjä voi joko periä kohtuullisen maksun tai kieltäytyä suorittamasta pyydettyä toimea. Pyyntöjen esittämisen liiallisesta määrästä tai aikarajasta ei ole säännöstä, mutta pyyntöjen toistuva esittäminen on mainittu asetuksessa esimerkkinä kohtuuttomuudesta.

Jos rekisterinpitäjä ei toteuta rekisteröidyn pyytämiä toimenpiteitä, sen tulee ilmoittaa syyt tähän ja kertoa mahdollisuudesta tehdä valitus ja käyttää muita oikeussuojakeinoja.

Rekisterinpitäjän tulee ilmoittaa tietoihin tekemistään oikaisuista, poistoista tai käsittelyn rajoituksista kaikille, joille kyseisiä henkilötietoja luovutettu, ellei se ole mahdotonta tai vaadi kohtuutonta vaivaa.

7. REKISTERINPITÄJÄN VELVOLLISUUDET

7.1 Tietosuojan hallinnointi, roolit ja vastuut

7.1.1 Tietosuojavastaava

Tietosuojavastaavan nimittäminen koskee erityisesti julkista sektoria, sillä aina kun viranomainen käsittelee henkilötietojen, tulee olla tietosuojavastaava. Poikkeuksen muodostavat tuomioistuimet, joilla tätä velvollisuutta ei ole.

Yksityisellä sektorilla ainoastaan tiettyjen toimijoiden on nimettävä tietosuojavastaava. Tällöin edellytyksenä on, että rekisterinpitäjän ja henkilötietojen käsittelijän ydintehtävät muodostuvat

- käsittelytoimista, jotka ovat luonteeltaan sellaisia, että ne edellyttävät rekisteröityjen laajamittaista, säännöllistä ja järjestelmällistä seurantaa, tai
- laajamittaisesta käsittelystä, joka kohdistuu arkaluonteisiin henkilötietoihin ja rikostuomioita tai rikkomuksia koskeviin henkilötietoihin.

Konserni voi nimittää yhden ainoan tietosuojavastaavan. Vastaavasti julkisella puolella voidaan nimittää yksi tietosuojavastaava ottaen huomioon toimijan organisaatiorakenne ja koko. Tietosuojavastaavaa nimitettäessä ratkaisevia tekijöitä ovat ammattipätevyys sekä erityisesti osaaminen ja asiantuntemus tietosuojalainsäädännöstä, säännösten soveltamisesta käytäntöön ja alan käytännöistä.

Tietosuojavastaava voi kuulua henkilökuntaan tai hän voi olla organisaatioon nähden ulkopuolinen ja hoitaa tehtävää sopimuksen perusteella. Suuri osa suomalaisista yrityksistä, joilla tulee olla tietosuojavastaava, ovat nimenneet hänet talon sisältä. Tietosuojavastaava voi hoitaa muitakin tehtäviä valtuutetun toimiensa lisäksi. Tällöin kannattaa huomioida, etteivät muut velvollisuudet saa aiheuttaa eturistiriitoja tietosuojaan liittyvien tehtävien hoidossa kuuluupa vastaava henkilökuntaan tai ei.

Organisaation toiminnassa tietosuojavastaava on otettava riittävän ajoissa ja asianmukaisesti mukaan kaikkiin tietosuojaa koskeviin kysymyksiin. Hänelle on annettava tehtävän hoitoon riittävät resurssit ja pääsy kaikkiin henkilötietoihin ja niihin liittyviin käsittelytoimiin. Tietosuojavastaavalla tulee olla mahdollisuus ylläpitää asiantuntemustaan.

Tietosuojavastaavalla tulee olla riippumaton asema organisaatiossa tietosuoja-asioita hoitaessaan. Hän ei saa tehtäviensä hoitamisen yhteydessä ottaa vastaan ohjeita esimerkiksi esimieheltään. Hän raportoi toimistaan ja havainnoistaan suoraan organisaation ylimmälle johdolle. Vastaavan on tehtävä yhteistyötä organisaation eri yksiköiden kanssa.

Tietosuojavastaavalla on salassapitovelvollisuus tehtävää hoitaessaan tietoonsa tulleiden asioiden ja tietojen osalta. Häntä ei saa erottaa tai rangaista sen vuoksi, että hän on hoitanut tehtäviään. Hän siis nauttii laajempaa irtisanomissuojaa.

Tietosuojavastaavan tehtävät

Tietosuojavastaavan on pantava täytäntöön organisaatiossaan tietosuoja-asetuksen edellyttämät toimet eli hän valvoo, että lainsäädäntöä käytännössä noudatetaan. Hänen tulee kouluttaa henkilökuntaa ja antaa neuvoja kaikissa tie-

tosuoja-asioissa. Hänen tehtävänsä on ohjeistaa tietosuojan käytännön toteuttaminen. Tämä on luonnollisesti parasta tehdä kiinteässä yhteistyössä rekisterinpitäjän tai käsittelijän eri toimintojen tai osastojen kanssa, esimerkiksi erilaisissa työryhmissä. Vastaavan tulee saada tietosuoja nostettua tietoiselle tasolle organisaatiossaan, jotta työntekijät osaavat ottaa sen huomioon esimerkiksi tietojärjestelmiä suunniteltaessa ja uudistettaessa tai kun kehitetään uusia tuotteita tai palveluja.

Tietosuojavastaavan tehtäviin kuuluu tietosuojan noudattamisen seuranta ja organisaation toiminnan tarkastaminen tietosuojanäkökulmasta. Hänen tulee valvoa, että tarpeelliset dokumentit laaditaan ja että ne ovat asianmukaisesti saatavilla esimerkiksi yrityksen intrassa ja tarvittaessa julkisilla verkkosivuilla. Hän myös valvoo, että tietosuojaan liittyvät asiakirjat, kuten selosteet, raportit ja pöytäkirjat, säilytetään asiallisesti. Tietosuojavastaava seuraa, että organisaatio toteuttaa ilmoitusvelvollisuutensa eri tilanteissa. Jos organisaatiossa tulee tehdä vaikutustenarviointi, hän on mukana sen toteutuksessa sekä tukien että eri toimia valvoen. Tietosuojavastaavan tehtäviin kuuluu myös henkilötietojen suojaan liittyvä vastuunjako ja tiedottaminen.

Tietosuojavastaava toimii organisaation sisäisenä yhteyshenkilönä tietosuoja-asioissa. Tietosuojavastaava on avainasemassa arvioitaessa erilaisiin käsittelytoimiin liittyviä riskejä, sillä hän tuntee sekä tietosuoja-asetuksen vaatimukset että organisaation toiminnan. Tietosuojavastaavan tulee tukea sitä, että rekisteröityjen oikeudet toteutuvat. Henkilötietojen käsittelyyn liittyvässä riskiarvioinnissa tietosuojavastaava huomioi käsittelyn luonteen, laajuuden, asiayhteyden ja käsittelytarkoituksen.

Tietosuojavastaava tekee yhteistyötä valvontaviranomaisen kanssa. Tietosuojavastaava toimii organisaation yhteyshenkilönä suhteessa sekä valvontaviranomaiseen että rekisteröityihin. Rekisteröidyt voivat ottaa yhteyttä häneen kaikissa asioissa, jotka liittyvät heidän henkilötietojensa käsittelyyn ja tietosuoja-asetukseen perustuvien oikeuksien käyttöön.

7.1.2 Tietosuojan hallinnointi

Tietosuojan hallinnoinnilla tarkoitetaan henkilötiedon elinkaaren hallintaa. Tähän kuuluu mm. kuvaukset siitä, miten henkilötiedot organisaatioon tulevat, kuka niitä käsittelee, käyttövaltuuksien ja -oikeuksien hallinnointi ja miten henkilötiedot poistetaan. Käytännön toimenpidesuosituksia tietosuojan hallinnoinnista on kuvattu luvussa 12.2.2.

7.1.3 Tietosuojadokumentaatio

Organisaation tulee laatia dokumentaatio siitä, mitä tarkoitusta varten henkilötietoja käsitellään, mitä henkilötietoja käsitellään ja miten ne on suojattu. Organisaation tulee kirjata dokumentaatioon myös tiedot niistä kolmansista osapuolista, joiden kanssa henkilötietoja jaetaan sekä siitä, siirretäänkö henkilötietoja kolmansiin maihin EU:n tai Euroopan talousalueen ulkopuolelle (ja mihin maihin tietoja siirretään) ja mikä on näiden siirtojen oikeudellinen perusta. Lisäksi organisaation on dokumentoitava tiedot organisaation hallinnollisista ja teknisistä suojaustoimista sekä henkilötietojen säilytysajat. Erilaisilla valvontatyökaluilla organisaatio voi varmistua siitä, että henkilötietojen käsittelyyn liittyvä toiminta on dokumentaation mukaista.

Myös ostopalveluna hankittavien palvelujen (esim. pilvipalvelut) käyttö on dokumentoitava. Organisaation on kirjattava dokumentaatioon esimerkiksi tiedot niistä henkilötiedoista, joita palvelujentarjoajat säilyttävät organisaation puolesta, palveluntarjoajia koskevat sopimussuhteet sekä mitä tapahtuu palveluissa säilytettäville henkilötiedoille sopimuksen päättyessä.

7.1.4 Riskiperusteinen lähestymistapa ja vaikutustenarviointi

Tietosuoja-asetuksessa on omaksuttu riskiperusteinen lähestymistapa. Tällä tarkoitetaan sitä, että rekisterinpitäjän velvoitteet ja suojatoimet on suhteutettava henkilötietojen käsittelystä rekisteröidyn oikeuksille ja vapauksille aiheutuvaan riskiin. Organisaation tulee siis käyttää henkilötietojen käsittelyyn riskienhallinnan keinoja. Rekisterinpitäjä ja henkilötietojen käsittelijä ovat velvollisia arvioimaan henkilötietojen käsittelyyn liittyvät riskit sekä asettamaan niille hallintatoimet. Jatkuvuuden turvaamiseksi on tärkeää ottaa tietosuojariskit osaksi organisaation riskienhallintajärjestelmää ja siten jatkuvaa toimintaa.

Vaikutustenarviointi on pakollinen henkilötietojen käsittelylle, jos suunnitteluvaiheessa on ilmeistä, että toimiin liittyy yksilöiden oikeuksien ja vapauksien kannalta merkittäviä riskejä. Arvioinnin tuloksia käytetään riskienhallinnassa määriteltävien riittävien riskienhallintakeinojen tunnistamiseen. Jos arvioinnin tuloksena ilmenee, että riskitaso on suuri, eikä rekisterinpitäjä pysty sitä toimenpiteillä riittävästi pienentämään, on otettava yhteyttä valvontaviranomaiseen (ennakkokuuleminen). Vaikutustenarviointi on suositeltavaa tehdä aina, vaikka se ei olekaan pakollista kaikille henkilötietojen käsittelytoimille, sillä se on erinomainen keino varmistua siitä, että organisaatio noudattaa tietosuoja-asetuksen vaatimuksia.

7.2 Sisäänrakennettu ja oletusarvoinen tietosuoja

Sisäänrakennetulla ja oletusarvoisella tietosuojalla tarkoitetaan sitä, että tietosuoja ja tietosuoja-asetuksen vaatimukset ovat organisaation henkilötietojen käsittelyssä otettu huomioon koko käsiteltävän henkilötiedon elinkaaren ajan. Käytännössä tämä tarkoittaa sitä, että tietosuoja-asetuksen vaatimukset tulee ottaa huomioon mahdollisimman varhaisessa vaiheessa esim. uusia tietojärjestelmiä ja palveluja suunniteltaessa. Näin varmistetaan, että tietosuoja on sisäänrakennettuna ja oletusarvoisesti mukana organisaation henkilötietojen käsittelyssä.

Oletusarvoisen tietosuojan periaatteen mukaan rekisterinpitäjän tulee tehdä asianmukaiset tekniset ja organisatoriset toimenpiteet (kohta 7.3), joilla varmistetaan, että oletusarvoisesti käsitellään vain käsittelyn kunkin erityisen tarkoituksen kannalta tarpeellisia henkilötietoja. Velvollisuus koskee niin kerättyjen henkilötietojen määrää, käsittelyn laajuutta, säilytysaikaa kuin saatavilla oloa.

7.2.1 Tiedon elinkaaren hallinta

Henkilötietojen elinkaarella tarkoitetaan koko ajanjaksoa henkilötietojen keräämisestä tai syntymisestä niiden anonymisointiin tai lopulliseen poistamiseen.

Osana henkilötietoinventaariota määritellään henkilötietojen säilytysaika. Tällä tarkoitetaan sitä miten kauan käsittelyssä olevia henkilötietoja tarvitaan. Nämä säilytysajat tulee ottaa käyttöön kaikkiin niihin järjestelmiin ja palveluihin, joilla henkilötietoja niiden elinkaaren aikana käsitellään. On huomioitava myös kolmansien osapuolten järjestelmissä

tai palveluissa tapahtuva henkilötietojen käsittely (ulkoistukset, ostopalvelut, SaaS-palvelut). Myös varmuuskopioinnin prosessit tulee käydä läpi, jotta henkilötietoa ei säilytetä niissä pidempään kuin on määritelty. Jos taas esimerkiksi jokin muu sääntely velvoittaa säilyttämään henkilötietoja pidempään, käsittely on rajattava minimitarpeen mukaisesti. Kun henkilötietojen käsittely- tai säilytysaika on umpeutunut, tiedot tulee anonymisoida tai poistaa lopullisesti.

7.3 Tietoturva

Rekisterinpitäjän ja henkilötietojen käsittelijän on suojattava henkilötiedot niin, että suojaustoimenpiteet vastaavat henkilötietojen käsittelyyn liittyvää riskiä. Tällöin tulee ottaa huomioon uusin tekniikka, aiheutuvat kustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä yksilön oikeuksiin ja vapauksiin kohdistuvat todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit.

Asianmukaisen turvallisuustason arvioimisessa on kiinnitettävä huomiota käsittelyn sisältämiin riskeihin, erityisesti siirrettyjen, tallennettujen tai muutoin käsiteltyjen henkilötietojen vahingossa tapahtuvan tai laittoman tuhoamisen, häviämisen, muuttamisen, luvattoman luovuttamisen tai henkilötietoihin pääsyn vuoksi.

Rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava asianmukaiset tekniset ja organisatoriset toimenpiteet, joilla henkilötietojen käsittely on turvattu. Henkilötiedot tulee suojata asianmukaisesti koko niiden elinkaaren ajan (mm. tallennus, käsittely, siirto ja poisto). Tietosuoja-asetus listaa tällaisina teknisinä tai organisatorisina toimenpiteinä seuraavat:

- 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,
- menettely, jolla testataan, tutkitaan ja arvioidaan säännöllisesti teknisten ja organisatoristen toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi.

Lisäksi henkilötietojen suojaaminen edellyttää myös henkilötietojen käsittelyn seuraamista ja valvontaa. Tietoturvallisuuden hallintaan on olemassa lukuisia malleja, joita voidaan käyttää. Tällaisia ovat esimerkiksi kansainvälisesti tunnetut standardit ISO/IEC 27001 ja ISO/EIC 27018.

7.4 Ilmoitusvelvollisuus henkilötietojen tietoturvaloukkauksesta

Tietoturvaloukkaus voi tapahtua, kun yrityksen työntekijältä varastetaan tietokone, usb-muistitikku katoaa tai yrityksen tietojärjestelmiin tapahtuu tietomurto. Tällöin henkilötietoja voi joutua vääriin käsiin.

Tietosuoja-asetus asettaa vaatimuksia rekisterinpitäjälle ja henkilötietojen käsittelijälle sen suhteen, miten henkilötietoihin kohdistuvasta tietoturvaloukkauksesta ilmoitetaan. Rekisterinpitäjällä on velvollisuus ilmoittaa henkilötietojen tietoturvaloukkauksesta tietosuojaviranomaiselle ja tietyissä tilanteissa myös rekisteröidyille. Henkilötietojen käsittelijän on ilmoitettava rekisterinpitäjälle ilman aiheetonta viivytystä havaittuaan, että henkilötiedot ovat joutuneet tietoturvaloukkauksen kohteeksi.

Jos tapahtuu henkilötietojen tietoturvaloukkaus, rekisterinpitäjän on ilmoitettava siitä ilman aiheetonta viivästystä ja mahdollisuuksien mukaan 72 tunnin kuluessa tiedon saamisesta valvontaviranomaiselle. Jos tapahtuneesta tietoturvaloukkauksesta aiheutuu todennäköisesti merkittäviä riskejä asianosaisten yksityishenkilöiden oikeuksille ja vapauksille, rekisterinpitäjän on ilmoitettava ilman aiheetonta viivytystä myös tietoturvaloukkauksen kohteeksi joutuneille henkilöille. Tämä tarkoittaa käytännössä sitä, että jos organisaatio rekisterinpitäjänä käyttää henkilötietojen käsittelijää (esim. pilvipalvelun palveluntarjoajaa), organisaation on varmistettava, että sopimukseen sisällytetään selkeästi tietoturvaloukkausilmoituksia koskevat toimenpiteet. Käytännössä kyse on ilmoitusvelvollisuuden toteuttamisesta, kuten tarvittavien tietojen antamisesta rekisterinpitäjälle. Jos ilmoitusta ei pystytä tekemään määräaikana, on määräaikana kuitenkin toimitettava selvitys viivästyksen syystä.

Jotta ilmoitusvelvollisuus on mahdollista täyttää, on organisaation pystyttävä ainakin:

- havaitsemaan tietoturvapoikkeamat henkilötietojen käsittelyssä,
- analysoimaan havaitun poikkeaman juurisyyt sekä vaikutukset henkilötietojen käsittelyyn,
- päättämään analyysin perusteella onko tarvetta ilmoittaa valvontaviranomaisille ja rekisteröidyille,
- dokumentoimaan tapahtunut huolellisesti, ja
- noudattamaan jatkuvan parantamisen mallia, eli oppia tapahtuneesta ja tehdä tarvittavat kehitystoimet.

Ilmoituksessa on kuvattava selkeällä ja yksinkertaisella kielellä henkilötietojen tietoturvaloukkauksen luonne ja annettava esimerkiksi tietoja loukkauksen mahdollista seurauksista ja kuvattava loukkauksen johdosta tehtyjä tai suunniteltuja toimenpiteitä kuten mitä on tehty haittavaikutuksien lieventämiseksi.

Valvontaviranomainen voi vaatia ilmoituksen tekemistä rekisteröidylle tai päättää, ettei ilmoitusta tarvitse tehdä. Tällöin viranomainen ottaa kantaa tietoturvaloukkauksesta rekisteröidylle mahdollisesti aiheutuvaan riskiin.

7.5 Yhteistyövelvoite

Valvontaviranomaisen pyytäessä rekisterinpitäjällä on velvollisuus yhteistyöhön. Yhteistyö kuuluu organisaation tietosuojavastaavan tai henkilötiedoista käytännössä vastaavien työntekijöiden tehtäviin. Jos organisaatiolla on toimintaa useassa EU-maassa, se voi asioida sen maan valvontaviranomaisen kanssa, jossa sen päätoimipaikka sijaitsee (nk. ”One-stop-shop” -mekanismi, ”yhden luukun” -periaate). Yhteistyövelvoitteeseen kuuluu myös ennakkokuuleminen, jos organisaation tietosuojan vaikutusarvioinnin perusteella henkilötietojen käsittelyyn liittyy suuria riskejä, joita organisaatio ei pysty hallitsemaan. Lisäksi yhteistyövelvoitteeseen kuulu ilmoitusvelvollisuus valvontaviranomaiselle, jota käsiteltiin edellisessä luvussa.

8. KÄSITTELIJÄN ASEMA

Henkilötietojen käsittelyyn liittyviä tehtäviä voidaan ulkoistaa henkilötietojen käsittelijälle. Henkilötietojen käsittelijällä tarkoitetaan ulkopuolista tahoa, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Tällainen voi olla esimerkiksi pilvipalvelujen tarjoaja tai tilitoimisto. Rekisterinpitäjän tulee tunnistaa tietosuoja-asetuksen vaatimukset ulkoistaessaan henkilötietojen käsittelyn. Rekisterinpitäjän ja henkilötietojen käsittelijän välillä on oltava kirjallinen sopimus. Rekisteripitäjän ja käsittelijän välisestä sopimussuhteesta tarkemmin kohdassa 10.1.

Rekisterinpitäjä saa käyttää ainoastaan 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.

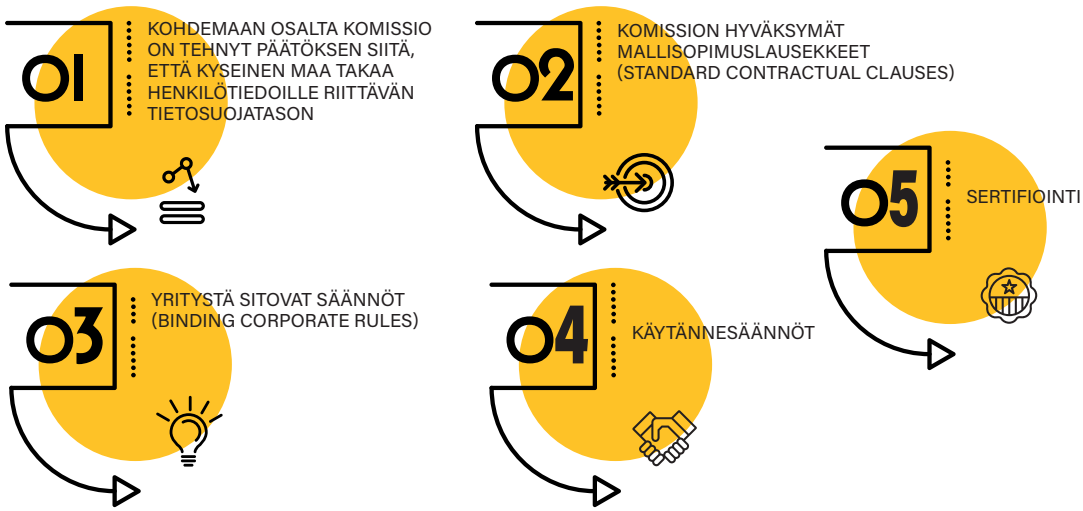
Käsittelijän on avustettava rekisterinpitäjää, kun tietoihin kohdistuu tietoturvaloukkaus. Henkilötietojen käsittelijää koskee vastaavat tietoturvavelvoitteet kuin rekisterinpitäjää.

9. TIETOJEN SIIRTO KOLMANSIIN MAIHIN

Henkilötietojen siirto EU:n tai Euroopan talousalueen ulkopuolelle on kiellettyä, jos tietosuoja-asetuksen mukaisia siirtomekanismeja ei ole otettu käyttöön. Rekisterinpitäjän ja henkilötietojen käsittelijän on huolehdittava siitä, että henkilötietoja siirrettäessä noudatetaan asetuksen mukaisia siirtomekanismeja. Organisaatiot voivat esimerkiksi

- varmistaa, että aiotun kohdemaan osalta komissio on tehnyt päätöksen siitä, että kyseinen maa takaa henkilötiedoille riittävän tietosuojatason
- käyttää komission hyväksymiä mallisopimuslausekkeita (standard contractual clauses)
- noudattaa yritystä koskevia tietosuojaviranomaisten vahvistamia sitovia sääntöjä (binding corporate rules)
- varmistaa ja tarkistaa, jos kyse on yhdysvaltalaisesta yrityksestä, että nk. Privacy Shield-sertifiointi soveltuu. EU:n ja Yhdysvaltojen välinen Privacy Shield -sopimus turvaa EU-kansalaisten perusoikeudet siirrettäessä henkilötietoja Yhdysvaltoihin ja asettaa vaatimukset yrityksille, jotka siirtävät henkilötietoja EU:n ja Yhdysvaltojen välillä. Henkilötietojen siirtäminen Privacy Shield -järjestelmään rekisteröityneelle yhdysvaltalaiselle toimijalle on sallittua, sillä rekisteröitynyt toimija on sitoutunut noudattamaan sertifioinnin asettamia vaatimuksia.

Henkilötietojen siirtämisen käsite on laaja. Sitä on tietojen konkreettisen siirtämisen ja lähettämisen lisäksi esimerkiksi pääsyn salliminen rekisterinpitäjän sisämarkkinoilla sijaitsevaan tietokantaan EU:n tai Euroopan talousalueen ulkopuolella toimivalle taholle. Vastaavasti henkilötietojen siirroksi katsotaan tilanne, jossa työntekijä käsittelee tietokoneellaan henkilötietoja matkustaessaan EU:n ulkopuolella. Myös henkilötietojen julkaiseminen internetissä on siirtämistä kolmansiin maihin. Säännökset soveltuvat myös tilanteeseen, jossa tiedot siirretään esimerkiksi rekisterinpitäjän omalle palvelimelle EU:n tai Euroopan talousalueen ulkopuolelle.



10. HENKILÖTIETOJA KOSKEVAT SOPIMUKSET

10.1 Rekisterinpitäjän ja käsittelijän väliset sopimukset

Kun henkilötietojen käsittelijä käsittelee henkilötietoja rekisteripitäjän lukuun, on henkilötietojen käsittelystä sovittava kirjallisesti. Tällöin tietosuoja-asetuksen pakottavat normit rajoittavat osapuolten sopimusvapautta.

Sopimuksessa on asetuksen mukaan sovittava seuraavista asioista:

1. henkilötietojen käsittelyn kohde ja kesto
2. henkilötietojen käsittelyn luonne ja tarkoitus
3. henkilötietojen tyyppi ja rekisteröityjen ryhmät ja
4. rekisterinpitäjän velvollisuudet ja oikeudet.

Käyttötarkoitussidonnaisuus on olennainen periaate henkilötietojen käsittelyssä eli henkilötietoja saa kerätä ja käsitellä vain tietyssä, nimenomaisessa ja laillisessa tarkoituksessa. Käyttötarkoitus määräytyy aina tapauskohtaisesti, joten se on määriteltävä sopimuksessa. Niinpä rekisterinpitäjä määrittelee sopimuksessa käsittelyn tarkoituksen ja keinot eikä käsittelijä saa käyttää tietoja muihin tarkoituksiin tai luovuttaa henkilötietoja ilman lupaa muille joihinkin muihin käyttötarkoituksiin.

Tietosuoja-asetus vaatii käsittelijältä tiedonantovelvollisuutta suhteessa rekisterinpitäjään, joten käsittelijän tulee antaa rekisterinpitäjälle tietoa, jota tämä voi tarvita rekisteröityjen asetuksen mukaisten oikeuksien toteuttamiseksi. Tällaisia ovat muun muassa tietojen tarkastus-, korjaus-, poisto- ja siirto-oikeus. Rekisterinpitäjä voi myös tarvita käsittelijältä tietoja tietosuojaviranomaisten vaatimusten tai ohjeiden noudattamiseksi.

Henkilötietojen käsittelijä ei saa käyttää alihankkijaa eli jonkun muun henkilötietojen käsittelijän palveluksia ilman rekisterinpitäjän erityistä tai yleistä kirjallista ennakkolupaa. Kun kyse on rekisterinpitäjän antamasta kirjallisesta ennakkoluvasta, henkilötietojen käsittelijän on tiedotettava rekisterinpitäjälle kaikista suunnitelluista muutoksista, jotka koskevat muiden henkilötietojen käsittelijöiden lisäämistä tai vaihtamista, ja annettava siten rekisterinpitäjälle mahdollisuus vastustaa tällaisia muutoksia. Jos alihankkija ei täytä tietosuojavelvollisuuksiaan, alkuperäinen henkilötietojen käsittelijä on edelleen täysimääräisesti vastuussa alihankkijan velvoitteiden suorittamisesta suhteessa rekisterinpitäjään.

Käsittelijän on sallittava rekisterinpitäjän tai tämän valtuuttaman auditoijan tarkastukset. Tämä koskee myös käsittelijän käyttämiä alihankkijoita.

Henkilötietojen käsittelijän tulee varmistaa, että henkilöt, joilla on oikeus käsitellä henkilötietoja, ovat sitoutuneet salassapitoon tai heitä koskee asianmukainen lakisääteinen salassapitovelvollisuus.

Sopijapuolten tulee sopia siitä, että käsittelijä rekisterinpitäjän valinnan mukaan joko poistaa tai palauttaa käsittelyyn liittyvien palveluiden tarjoamisen päätyttyä kaikki henkilötiedot rekisterinpitäjälle ja poistaa olemassa olevat jäljennökset.

Sopijapuolet voivat tapauskohtaisesti sopia korvausvelvollisuudesta ja mahdollisista vastuunrajoituksista.

Joissain tilanteissa molemmat sopijapuolet toimivat osittain rekisterinpitäjinä ja osittain käsittelijöinä. Tällöin käsittelytarkoitukset ovat yleensä erilaiset. Sopijapuolet voivat olla myös yhteisrekisterinpitäjinä. Tämä tulee huomioida sopimuksessa.

10.2 Yhteisrekisterinpitäjät

Jos vähintään kaksi rekisterinpitäjää määrittää yhdessä käsittelyn tarkoitukset ja keinot, kyse on yhteisrekisterinpitäjistä. Niiden tulee määritellä läpinäkyvästi keskinäisellä järjestelyllä kunkin vastuualue, erityisesti rekisteröityjen oikeuksien käyttöä ja tietojen toimittamista koskevilta osin. Asetus edellyttää, että toimijoiden vastuualueet jaetaan selkeästi, myös silloin, kun rekisterinpitäjä määrittää käsittelyn tarkoitukset ja keinot yhdessä muiden rekisterinpitäjien kanssa. Järjestelyn yhteydessä voidaan nimetä rekisteröidyille yhteyspiste.

Järjestelystä on käytävä ilmi yhteisten rekisterinpitäjien todelliset roolit ja suhteet rekisteröityyn. Järjestelyn keskeisten osien tulee olla rekisteröidyn saatavilla.

Järjestelyn ehdoista riippumatta rekisteröity voi käyttää asetuksen mukaisia oikeuksiaan suhteessa kuhunkin rekisterinpitäjään ja tarvittaessa kutakin yhteisrekisterinpitäjää vastaan.

10.3 Sopimus henkilötietojen luovuttamisesta

Lainsäädännössä ei ole vaatimuksia koskien sopimusta, jolla luovutetaan henkilötietoja. Rekisterinpitäjä, joka luovuttaa henkilötietoja rekisteristään, vastaa luovutuksen lainmukaisuudesta. Vastaavasti toinen rekisterinpitäjä, joka on vastaanottanut toisen rekisterinpitäjän rekisteristä henkilötietoja, vastaa oman käsittelynsä lainmukaisuudesta. Käsittelyn lainmukaisuuden osalta katso kohta 5.3.

Sopijapuolet voivat sopia vastuun jakamisesta ja muista ehdoista suhteessa toisiinsa. Henkilötietojen luovutussopimuksessa tulisi huomioida seuraavia asioita:

- Henkilötietojen käyttötarkoitus
- Henkilötietojen luovutettavuus
- Säilytysaika
- Vastuukysymykset, kuten rekisteröityjen informointi
- Muut, kuten kaupalliset asiat.

11. VASTUU JA SEURAAMUKSET

11.1 Yleistä oikeussuojakeinoista

Rekisteröidyllä on oikeus tehdä valitus valvontaviranomaiselle, jos hänen henkilötietojensa käsittelyssä rikotaan tietosuojasäännöksiä. Hän voi valittaa viranomaisen tekemästä päätöksestä. Rekisteröityä tulee informoida valitusoikeudesta. Kanne rekisterinpitäjää tai henkilötietojen käsittelijää vastaan voidaan nostaa sen jäsenvaltion tuomioistuimissa, jossa rekisteröidyllä on vakinainen asuinpaikka.

11.2 Rekisterinpitäjän vahingonkorvausvastuu

Jos henkilölle aiheutuu asetuksen rikkomisesta aineellista tai aineetonta vahinkoa, hänellä on oikeus saada korvaus rekisterinpitäjältä tai henkilötietojen käsittelijältä. Rekisterinpitäjä on vastuussa vahingosta, joka on aiheutunut asetuksen vastaisesta käsittelystä riippumatta siitä, kuka säännöksiä on rikkonut. Henkilötietojen käsittelijä on vastuussa käsittelystä aiheutuneesta vahingosta vain, jos se ei ole noudattanut nimenomaisesti sitä koskevia asetuksen velvoitteita tai jos se on toiminut rekisterinpitäjän ohjeiden vastaisesti. Rekisterinpitäjällä tai henkilötietojen käsittelijällä on mahdollisuus vapautua vastuusta vain, jos hän voi osoittaa, ettei ole millään tavoin vastuussa vahingon aiheuttaneesta tapahtumasta.

Jos samaan tietojenkäsittelyyn osallistuu useampi kuin yksi rekisterinpitäjä tai henkilötietojen käsittelijä, kukin heistä on vastuussa koko vahingosta suhteessa rekisteröityyn. Tällä varmistetaan se, että rekisteröity saa korvauksen. Korvauksen suorittaneella rekisterinpitäjällä tai henkilötietojen käsittelijällä on puolestaan regressio-oikeus suhteessa toisiin henkilötietojen käsittelyyn osallistuneisiin tahoihin, eli se voi periä muilta niiden osuuden korvauksesta, joka vastaa kunkin vastuuta aiheutuneesta vahingosta.

11.3 Seuraamukset

Tietosuoja-asetuksen rikkomisesta voi seurata varoitus, huomautus, erilaisia määräyksiä, kieltoja, sertifikaatin menettäminen tai viranomainen voi määrätä huomattavan hallinnollisen sakon. Suomessa hallinnollista sakkoa kutsutaan hallinnolliseksi seuraamusmaksuksi. Se on uusi rangaistusluonteinen seuraamus, jolla lainsäätäjä on halunnut korostaa tietosuojan tärkeyttä. Se voi olla enintään 20 miljoonaa euroa tai 4 %:a yrityksen edeltävän tilikauden maailmanlaajuisesta kokonaisliikevaihdosta sen mukaan kumpi näistä summista on suurempi.

Kun viranomainen määrää hallinnollisen seuraamusmaksun, sen tulee varmistaa, että seuraamus on kussakin yksittäistapauksessa tehokas, oikeasuhtainen ja varoittava. Seuraamusmaksu voidaan määrätä muiden toimenpiteiden lisäksi tai niiden sijasta yksittäistapauksen olosuhteiden mukaan. Kun viranomainen päättää seuraamusmaksun määräämisestä ja määrästä, sen on otettava huomioon muun muassa seuraavia seikkoja:

- rikkomisen luonne, vakavuus ja kesto
- tahallisuus tai tuottamuksellisuus
- toimet aiheutuneen vahingon lieventämiseksi
- vastuun aste, ottaen huomioon toteutetun sisäänrakennetun ja oletusarvoisen tietosuojan sekä käsittelyn turvallisuuden edellyttämät tekniset ja organisatoriset toimenpiteet
- mahdolliset aiemmat vastaavat rikkomukset
- yhteistyön aste valvontaviranomaisen kanssa tilanteen korjaamiseksi
- tapa, jolla rikkominen tuli valvontaviranomaisen tietoon, kuten se, ilmoittiko rekisterinpitäjä tai henkilötietojen käsittelijä itse asiasta
- muut mahdolliset raskauttavat tai lieventävät tekijät, kuten rikkomisesta saatu taloudellinen hyöty.

12. SUOSITUKSIA KÄYTÄNNÖN TOIMENPITEISTÄ

Tähän lukuun on koottu käytännön suosituksia toimenpiteistä jokaiselle organisaatiolle. On hyvä muistaa, että tietosuoja-asetuksen vaatimusten täyttäminen ei ole kertaluonteinen projekti, vaan se on otettava mukaan organisaation jokapäiväiseen toimintaan. Luvussa 12.1 on kuvattu yleisiä toimenpiteitä ja huomioita. Luvussa 12.2 on esitelty jatkuvan kehityksen malli, jota noudattamalla tietosuojaa voidaan paremmin toteuttaa organisaatiossa.

12.1 Yleisiä toimenpiteitä ja huomioita

Johdon osallistuminen

Johdon vastuuta tietosuojatoiminnasta ei voi ulkoistaa.

Organisaation johdon tuki tietosuojatoiminnalle on kriittisen tärkeää. Johto on vastuussa organisaation tietosuojatoiminnasta ja vastaa viime kädessä siitä, että se täyttää tietosuoja-asetuksen vaatimukset. Johdon tärkein tehtävä on antaa ja turvata riittävät resurssit, jotta esimerkiksi voidaan toteuttaa tietosuojatoiminnan jatkuvan kehityksen mallia ja käynnistää sen perusteella tarpeelliset kehitystoimet. Lisäksi tietosuojatoiminta tulee sisällyttää organisaation strategiseen ohjaukseen säännöllisesti kuuluvaan raportointiin.

Riskienarviointi ja riskienhallinnan kehittäminen

Moni organisaatio tekee riskienhallintaa osana johtamisjärjestelmäänsä. Tietosuoja-asetus ei tuo tähän toimintaan mitään uutta, mutta tietosuoja on otettava mukaan osaksi sitä. Riskienarviointiin kuuluu henkilötiedon käsittelyyn liittyvien riskien tunnistaminen, analysoiminen sekä tarvittavien riskienhallintatoimien laatiminen. Riskienarvioinnissa kaikkein oleellisinta on varmistaa riittävä henkilötietojen tietoturva niiden koko elinkaaren ajan.

Kun ensimmäinen tietosuojaan liittyvä riskienarviointi ja hallintatoimien tunnistaminen on tehty, pitää varmistua, että tietosuoja on jatkossa mukana organisaation riskienhallintajärjestelmässä ja -prosessissa.

Koulutus ja ohjeistus

Organisaation henkilöstön tietosuojaosaamisesta on huolehdittava riittävällä koulutuksella ja ohjeistuksella. Tämä koskee erityisesti henkilöstöä, jonka työtehtäviin kuuluu henkilötietojen käsittelemistä. Lisäksi organisaation kannattaa tarjota täsmäkoulutusta esimerkiksi henkilöstöhallinnon tai markkinoinnin parissa toimiville.

Dokumentaatio ja viestintä

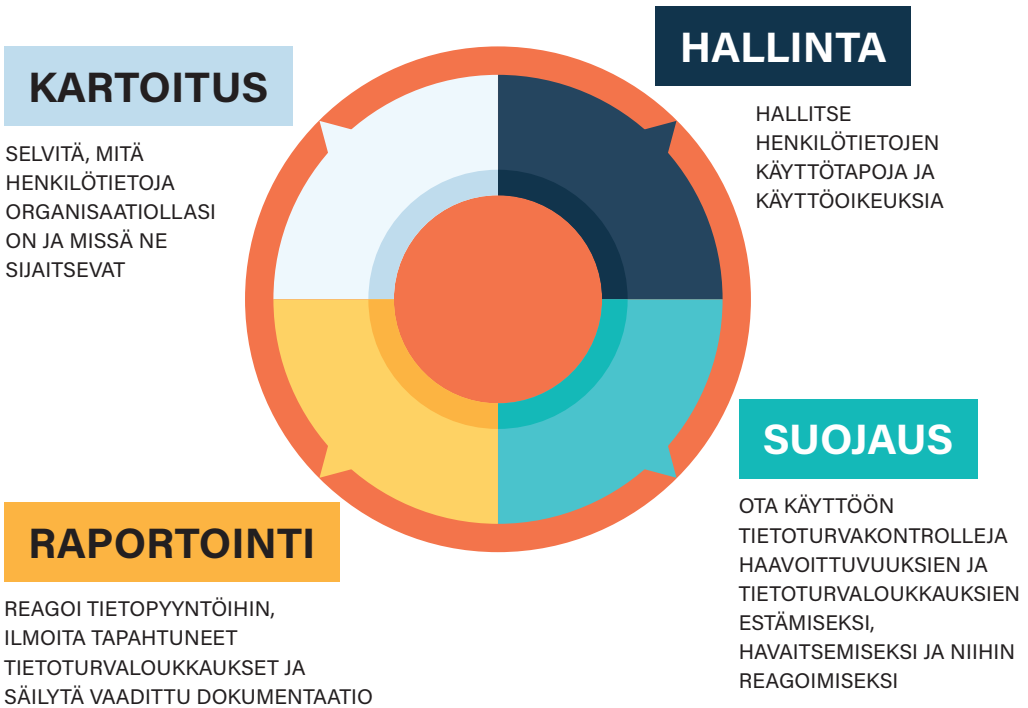
Kehittämistoimien ja muutosten yhteydessä on syytä päivittää myös tietosuojaa koskeva dokumentaatio sekä viestintään liittyvät mahdolliset asiakirja- tai viestipohjat (mm. rekisteröidyille ja valvontaviranomaiselle lähetettävät ilmoitukset) sekä muu materiaali (tietosuojadokumentaatio). Dokumentaatiosta tarkemmin luvussa 7.1.3.

12.2 Jatkuvan kehityksen malli

Tämän päivän organisaatioiden IT-ympäristöt ovat erittäin monimutkaisia. Järjestelmät, joilla esimerkiksi henkilö- tai mitä tahansa muita tietoja luodaan, tallennetaan, muutetaan, hyödynnetään tai analysoidaan, levittäytyvät monenlaisiin IT-ympäristöihin – palvelimiin, pilvipohjaisiin palveluihin, työasemiin, älypuhelimiin, tabletteihin, käyttäjien omiin laitteisiin ja jopa esineiden internetiin (IoT, Internet of Things). Tietosuoja-asetuksen vaatimukset koskevatkin usein käytännössä isompaa kokonaisuutta kuin vain organisaation omaa IT-ympäristöä.

Paras tapa vastata tietosuoja-asetuksen vaatimuksiin on tarkastella vaatimuksia kokonaisvaltaisesti ja huomioida samalla myös muut lainsäädännön asettamat tietosuojaa ja -turvaa koskevat velvoitteet. Esimerkiksi monet tietosuoja-asetuksen edellyttämät tietoturvatoimet ovat samankaltaisia kuin muissa tietosuoja- ja tietoturvastandardeissa (kuten vaikkapa ISO/IEC 27001 tai ISO/IEC 27018) edellytettävät hallintakeinot. Vaikka eri standardit tai lainsäädäntö edellyttävät yksittäisiä hallintatoimia, on parasta tunnistaa näiden vaatimusten asettama kokonaisuus eikä toteuttaa niitä yksittäin. Yhtä lailla kokonaisuuden tarkastelu pätee yksittäiseen teknologiaan tai järjestelmään: sen sijaan, että arvioitaisiin niiden ominaisuuksia irrallaan tietosuoja-asetuksen asettamista vaatimuksista, kannattaa tarkastella organisaation koko tietosuojatoimintaa ja siihen liittyviä IT-ympäristöjä ja -järjestelmiä kokonaisuutena. Näin organisaatio pystyy täyttämään tietosuoja-asetuksen ja myös muiden mahdollisten standardien vaatimukset myös tulevaisuudessa.

Kuten jo aiemmin todettiin, on syytä muistaa, että asetuksen vaatimusten täyttäminen ei ole kertaluonteinen tehtävä, vaan tietosuoja-asetus on tuotava mukaan organisaation jokapäiväiseen toimintaan.



Tämä tarkoittaa käytännössä sitä, että tietosuoja pitää huomioida jatkossa aina, esimerkiksi kun organisaation tietojärjestelmiä muutetaan tai otetaan käyttöön kokonaan uusi IT-järjestelmä.

Seuraavissa luvuissa kuvataan organisaation tietosuojatoiminnan jatkuvan kehityksen malli. Mallin voidaan ajatella toimivan jatkuvan parantamisen kehänä, jossa edellisen vaiheen päätyttyä alkaa seuraava vaihe. Kehää toistamalla organisaatio varmistaa tietosuoja-asetuksen vaatimusten täyttymisen myös tulevaisuudessa.

- Kartoitus – selvitä, mitä henkilötietoja organisaatiollasi on ja missä ne sijaitsevat
- Hallinta – hallitse henkilötietojen käyttötapoja ja käyttöoikeuksia
- Suojaus – ota käyttöön tietoturvakontrolleja haavoittuvuuksien ja tietoturvaloukkauksien estämiseksi, havaitsemiseksi ja niihin reagoimiseksi
- Raportointi – reagoi tietopyyntöihin, ilmoita tapahtuneet tietoturvaloukkaukset ja säilytä vaadittu dokumentaatio.

12.2.1 Kartoitus

Kartoitusvaiheessa käydään läpi koko organisaation toiminta henkilötietojen käsittelyn näkökulmasta. Kartoituksen lopputuloksena saadaan näkyvyys siihen, mistä henkilötiedot organisaatioon tulevat, missä ja miten niitä käsitellään ja säilytetään sekä miten ne poistuvat.

Tietosuoja-asetuksen vaatimusten täyttäminen aloitetaan arvioimalla organisaation nykyiset tietosuoja- ja tiedonhallintakäytännöt. Ensimmäiseksi kartoitetaan organisaation henkilötietojen käsittelyn nykytila, laaditaan siihen kuuluva henkilötietoinventaario sekä käydään läpi henkilötietojen käsittelyyn liittyvät sopimukset mahdollisten ostopalvelujen osalta.

Nykytilan selvittäminen ja henkilötietoinventaario

Tietosuojatoiminnan nykytilan selvittämisellä tarkoitetaan organisaation nykyisen tietosuojaan liittyvän toiminnan arviointia verrattuna tietosuoja-asetuksen asettamiin vaatimuksiin. Sen lopputuloksena saadaan niin kutsuttu gap-analyysi tietosuojatoiminnan puutteista ja kehittämistarpeista. Gap-analyysilla tarkoitetaan nykytilan ja asetettujen vaatimusten täyttymisen välisiä kehitystoimenpiteitä. Tämän perusteella voidaan tehdä lista kehittämistoimista sekä kehittämissuunnitelma, jota toteuttamalla täytetään tietosuoja-asetuksen vaatimukset. Kehittämissuunnitelmaan on hyvä sisällyttää myös arviot kehittämistoimenpiteiden resurssitarpeista.

Nykytila-analyysin osana organisaatio tunnistaa, mitä henkilötietoja se kerää, missä niitä säilytetään ja miten niitä käsitellään. Yksi analyysin osioista on organisaation henkilötietojen käsittelyn nykytila. Tähän kuuluu henkilötietoinventaario sekä tiedon elinkaariajattelun mukaisesti muun muassa seuraavat kokonaisuudet:

- millaisia henkilötietoja käsitellään?
- mistä, mitä kautta ja miten henkilötiedot tulevat organisaatioon?
- missä henkilötietoja säilytetään?
- millä (järjestelmät ja palvelut ml. ostopalvelut) henkilötietoja käsitellään?
- kuka henkilötietoja käsittelee?
- kuinka kauan henkilötietoja säilytetään?
- milloin ja miten henkilötiedot hävitetään?

Henkilötietoinventaario siis auttaa selvittämään, mitkä tiedot ovat henkilötietoja, ja tunnistamaan ne järjestelmät ja toiminnot, joissa kyseisiä tietoja kerätään, tallennetaan ja käsitellään. Inventaari pakottaa organisaation myös pohtimaan

miksi henkilötietoja kerätään, mihin niitä käytetään, miten niitä käsitellään ja jaetaan sekä miten kauan tietoja säilytetään. Nykytilan selvittämisen sekä siitä saatavan gap-analyysin tuloksista voidaan laatia vaatimukset myös uusille, aloitettaville hankkeille. Näin varmistetaan tietosuoja-asetuksen vaatimusten täyttyminen myös tulevassa toiminnassa.

Nykytila-analyysin tekemiseen voi ja usein kannattaa hankkia myös ulkopuolista apua, esimerkiksi konsultointipalveluja tarjoavilta tahoilta.

Sopimusten läpikäynti

Useimmat organisaatiot ostavat palveluja, joissa käsitellään henkilötietoja myös kolmansilta osapuolilta. Tietosuoja-asetuksen mukaan on tällöin usein kyse jaetusta vastuusta asiakkaan (rekisterinpitäjä) ja palveluntarjoajan (käsittelijä) välillä. Rekisterinpitäjä on kuitenkin vastuussa henkilötietojen käsittelystä myös ostopalvelujen osalta. Ostopalveluihin liittyvät palvelusopimukset pitääkin käydä läpi tietosuoja-asetuksen vaatimusten näkökulmasta ja korjata mahdolliset puutteet sopimuksissa uusimalla sopimukset tai tekemällä olemassa oleviin sopimuksiin uudet liitteet tietosuojan osalta. Lisäksi pitää varmistaa, mitä henkilötietojen siirtämisestä EU:n tai Euroopan talousalueen ulkopuolelle on sovittu.

12.2.2 Hallinta

Hallintavaiheessa organisaatiolle luodaan henkilötietojen hallintasuunnitelma.

Tietosuoja-asetus takaa rekisteröidyille mahdollisuudet hallita tapoja, joilla heidän henkilötietojaan kerätään, käytetään ja käsitellään. Rekisteröidyt voivat esimerkiksi pyytää, että organisaatio antaa heihin liittyvät tiedot, siirtää heidän henkilötietonsa muuhun palveluun, korjaa heidän henkilötiedoissaan olevat virheet tai poistaa heihin liittyvät henkilötiedot. Toinen vaihe on luoda organisaatiolle henkilötietojen hallintasuunnitelma, jossa määritellään henkilötietojen käyttöoikeudet, hallinta sekä käyttöön liittyvät käytännöt, käytänteet, roolit ja vastuut.

Henkilötietojen hallintasuunnitelma

Henkilötietojen hallintasuunnitelmassa kuvataan käytännön tasolla henkilötietojen hallinta organisaatiossa. Kartoitusvaiheessa luotu henkilötietoinventaari on ensimmäinen vaihe tämän suunnitelman laadinnassa. Suunnitelma auttaa varmistamaan, että henkilötietojen käsittelykäytännöt ovat tietosuoja-asetuksen asettamien vaatimusten mukaisia. Lisäksi henkilötietojen hallintasuunnitelma takaa, että organisaatio voi ja pystyy toteuttamaan rekisteröityjen mahdolliset tietojen korjaus-, siirto- tai poistopyynnöt.

12.2.3 Suojaus

Suojausvaiheessa otetaan käyttöön tietoturvakontrollit haavoittuvuuksien havaitsemiseksi, tietomurtojen estämiseksi ja niihin reagoimiseksi.

Organisaatiot tiedostavat nykyisin entistä paremmin tietoturvan ja tietojen suojauksen merkityksen. Tietosuoja-asetus nostaa tietoturvan ja tietosuojan toteuttamisen kuitenkin uudelle tasolle. Asetus edellyttää, että organisaatiot suojaavat henkilötiedot katoamiselta, luvattomalta käytöltä ja paljastumiselta riittävin ja soveltuvin teknisin ja hallinnollisin keinoin.

Henkilötietojen suojaaminen

Tietoturvallisuus on nykypäivänä monisyistä ja se on otettava huomioon organisaation kaikessa toiminnassa. Tietoturvariskejä on monenlaisia: esimerkiksi fyysinen tunkeutuminen organisaation tiloihin, väärinkäytöksiä (tahallaan tai tahattomasti) tekevä organisaation oma työntekijä, vahingossa tapahtuva tietojen katoaminen tai organisaation tietojärjestelmiin murtautuva tietoverkkorikollinen. Riskienhallinnalliset keinot, kuten varautumis- ja palautumissuunnitelmien laatiminen, riskien ehkäisemis- ja pienentämistoimenpiteiden toteuttaminen ja tarvittavien tietoturvakontrollien käyttöönottaminen auttavat organisaatiota varmistamaan vaatimuksenmukaisuuden toteutumisen.

Tietomurtojen havaitseminen ja niihin reagoiminen

Tietosuoja-asetus edellyttää tietyissä tapauksissa, että organisaation on ilmoitettava tapahtuneesta tietomurrosta tai -vuodosta viranomaisille tietyn määräajan kuluessa. Joissain tapauksissa organisaation on ilmoitettava tapahtuneesta myös niille rekisteröidyille, joiden henkilötiedoista on kyse. Jotta organisaatio pystyy nämä vaatimukset toteuttamaan, tulee sillä olla kyvykkyydet havaita henkilötietoihin kohdistuneet tietomurrot ja -vuodot. Myös ostopalvelujen osalta organisaation tulee varmistua siitä, että sopimuskumppanilla on kyky havaita tällaiset tietomurrot ja -vuodot ja että ilmoitusvelvollisuuksista on sovittu asianmukaisesti.

Tietomurron tai -vuodon havaitsemisen jälkeen on suositeltavaa noudattaa seuraavaa nelivaiheista prosessia:

- Laadi vakavuusarviointi:
  - Arvioi tapahtuman vaikutus ja vakavuus.
- Tee tekninen tutkimus ja kartoita mahdolliset tapahtuman hallinta-, korjaus- ja/tai kiertostrategiat.
  - Jos henkilötiedot ovat voineet altistua luvattomalle käytölle tai ne ovat vuotaa organisaation ulkopuolelle, käynnistä ilmoitusprosessi tietosuoja-asetuksen edellyttämällä tavalla.
- Laadi palautumissuunnitelma tapahtumasta toipumiseksi.
  - Suorita tapahtuman hallintatoimenpiteet, esim. järjestelmien eristäminen ja lokien varmistaminen tutkintaa varten.
  - Suunnittele pitkäaikaiset korjaus- ja palautumistoimet akuutin tilanteen päätyttyä.
- Tee jälkiarviointi:
  - Kertaa tapahtuman kulku.
  - Korjaa käytänteet, toimenpiteet ja prosessit siten, että vastaava tapahtuma voidaan jatkossa estää.

12.2.4 Raportointi

Raportointivaiheessa laaditaan organisaation johdolle raportit, dokumentoidaan tietosuojaan liittyvä toiminta, tehdään ilmoitukset rekisteröidyille sekä viranomaisille ja vastataan rekisteröityjen esittämiin pyyntöihin.

Osana raportointia organisaation pitää laatia ja päivittää tietosuojatoimintaan liittyvä dokumentaatio. Tietosuojaan liittyvää dokumentaatiota käsiteltiin luvussa 7.1.3.

Johdon raportointi

Kuten aiemmin todettiin, organisaation johto vastaa organisaation tietosuojatoiminnasta ja jotta se pystyisi hoitamaan tehtävänsä, se tarvitsee ajantasaista raportointia. Tietosuojavastaavan (jos sellainen on nimetty) tehtävä on raportoida organisaation johdolle säännöllisesti organisaation tietosuojatoiminnan tapahtumista ja tilasta. Säännölliseen raportointiin voivat kuulua mm. seuraavat asiat:

- Menneen tarkastelu sisältäen mm. merkittävimmät tietosuoja- ja tietoturvatapahtumat sekä mahdolliset loukkaukset henkilötietoihin liittyen
- Henkilötietojen käsittelyyn liittyvä riskienarviointi
- Mahdolliset tietosuojaan liittyvät mittarit
- Viranomaisten kanssa tehty yhteistyö (mukaan lukien viranomaisille tehdyt ilmoitukset)
- Tietosuojatoimintaan liittyvien kehitystoimenpiteiden seuranta.

Rekisteröidyille ja viranomaisille ilmoittaminen

Luvussa 7.4 on kuvattu tietosuoja-asetuksen asettamia vaatimuksia rekisteröidyille ja viranomaisille ilmoittamisesta. Organisaation on kyettävä tekemään nämä ilmoitukset ja sovittava, kuka tekee ja miten ilmoitukset käytännössä toteutetaan. Yleensä ilmoitusten tekemisestä vastaa organisaation tietosuojavastaava.

Rekisteröidyn esittämien pyyntöjen käsittely

Organisaation on luotava valmiudet käsitellä rekisteröityjen esittämiä pyyntöjä. Näitä pyyntöjä voivat olla esimerkiksi pyyntö saada nähdä mitä henkilötietoja organisaatiolla henkilöstä on, pyyntö korjata henkilötiedoissa olevat virheet tai pyyntö poistaa henkilötiedot järjestelmistä. Pyyntöjen käsittelemiseksi on hyvä laatia vakiomuotoinen tapa, joka voi olla esimerkiksi verkkolomake tai roolipohjainen sähköpostiosoite (**esim. tietosuojavastaava@yritys.fi**). Jotta pyyntöjen käsittely ja niihin vastaaminen tapahtuisi säännönmukaisesti ja asetuksen vaatimusten mukaisesti, se tulee kuvata. Rekisteröidyille lähetettäviä vastauksia varten on hyvä laatia valmiit mallit ja pohjat.

4 ASKELTA: Näin pidät yrityksen tietosuoja-asiat ajan tasalla

Kartoitus - selvitä, mitä henkilötietoja organisaatiolla on hallussaan ja missä ne sijaitsevat

Hallinta - hallitse henkilötietojen käyttötapoja ja käyttöoikeuksia

Suojaus - ota käyttöön tietoturvakontrolleja haavoittuvuuksien ja tietoturvaloukkauksien estämiseksi, havaitsemiseksi ja niihin reagoimiseksi

Raportointi - reagoi tietopyyntöihin, ilmoita tapahtuneet tietoturvaloukkaukset ja säilytä vaadittu dokumentaatio

Organisaation johdon tuki on ensisijaisen tärkeää.

OTK, VT MINNA AALTO-SETÄLÄ TOIMII KESKUSKAUPPAKAMARIN LAKI-YKSIKÖSSÄ SÄHKÖISEN KAUPAN JA IMMATERIAALIOIKEUKSIEN ASIANTUNTIJANA. MINNA ON SEURANNUT TIIVIISTI SUOMALAISTEN YRITYSTEN VALMISTAUTUMISTA TIETOSUOJA-ASETUKSEEN MUUN MUASSA KOULUTTAESSAAN ERI ORGANISAATIOITA YMPÄRI SUOMEA PARIN VIIME VUODEN AJAN. AIEMMIN HÄN ON TOIMINUT TELEALALLA LAKIMIEHENÄ JA ASIANAJAJANA.

MIKKO VIITAILA TYÖSKENTELEE TEKNOLOGIAJOHTAJANA MICROSOFT OY:SSÄ. HÄNEN PÄÄVASTUUALUEITAAN OVAT TEKNOLOGIAN KÄYTÖN EDISTÄMINEN, ASIAKKAIDEN AUTTAMINEN UUSIEN MAHDOLLISUUKSIEN HYÖDYNTÄMISESSÄ SEKÄ TURVALLISEN DIGITALISAATION EDISTÄMINEN. MIKOLLA ON YLI 15 VUODEN IT- JA KYBERTURVALLISUUSALAN KOKEMUS YKSITYISEN JA JULKISEN SEKTORIN PALVELUKSESSA.

KESKUS-
KAUPPAKAMARI

KESKUSKAUPPAKAMARI
Aleksanterinkatu 17, 00100 Helsinki
kauppakamari.fi

Microsoft

MICROSOFT FINLAND
Keilalahdentie 2-4, 02150 Espoo
microsoft.com

Mikko Viitaila
Teknologiajohtaja, Microsoft Oy
mikko.viitaila@microsoft.com
+358 40 809 8757

KESKUS-
KAUPPAKAMARI

Microsoft