Andreas Lönnfors

EU:n tietosuoja-asetuksen vaatimusten toteuttaminen pk-yrityksissä

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikan koulutusohjelma

Insinöörityö

18.4.2017

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Andreas Lönnfors EU:n tietosuoja-asetuksen vaatimusten toteuttaminen pk-yrityksissä 31 sivua 18.4.2017
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja(t)	Lehtori Marko Uusitalo

Insinöörityön tavoitteena on tutkia, miten EU:n tietosuoja-asetus eroaa nykyisestä lainsäädännöstä. Lisäksi tutkitaan, kuinka pk-yrityksen, joka on osittain ulkoistanut henkilötietojen käsittelyn toiselle organisaatiolle, tulisi valmistautua tuleviin muutoksiin.

Tarkoituksena oli selvittää, mitä muutoksia pilvipalveluita käyttävä pk-yritys joutuisi tekemään tekniseen ympäristöön, jotta tietosuojakäytännöt vastaisivat tietosuojauudistuksen asettamia velvoitteita. Saatujen tietojen perusteella laadittiin yleisohje, jota pk-yritys voi hyödyntää varmistaakseen, että tietosuojauudistuksen asettamia velvoitteita noudatetaan.

Tutkimuksesta selvisi, että tietosuojauudistus ei vaadi suuria muutoksia pk-yrityksen tekniseen ympäristöön tai tiedonkäsittelytapoihin, jos toteutukset ja käytännöt vastaavat nykyisen lainsäädännön asettamia vaatimuksia.

Avainsanat	Tietosuoja, EU:n tietosuoja-asetus, tietosuojalainsäädäntö, pk-yritys

Author(s) Title Number of Pages Date	Andreas Lönnfors Implementation of the requirements of the EU Data Protection Regulation for SMEs 31 pages 18 April 2017
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Data Networks
Instructor(s)	Marko Uusitalo, Senior Lecturer

The purpose of the thesis was to investigate how the new EU General Data Protection Regulation differs from the current legislation, and also how small businesses that have in part outsourced the processing of personal data to outside organizations should prepare for the upcoming changes.

The aim was to research what kind of changes should be made to the technical environment of a small business so that the data privacy standards would meet the requirements of the renewed data protection regulations. Based on the gathered information, a set of guidelines intended for small businesses were drawn. By following the guidelines, they can ensure that they meet the requirements of the new legislation.

The results of the investigation showed that the data protection regulation does not require large changes to the technical environment or to the information processing methods if the implementations and practices match the requirements of the current legislation.

Keywords	EUs General Data Protection Regulation, GDPR, Data protection legislation, SME

Sisällys

Lyhenteet ja määritelmät

Henkilötieto	Kaikki tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyvät tiedot (esim. nimi, henkilötunnus, kuva, biometrinen tai geneettinen tieto).
HTTPS	Hypertext Transfer Protocol Secure (HTTPS) on HTTP-protokollan ja TLS/SSL-protokollan yhdistelmä, jota käytetään tiedon suojattuun siirtoon webissä. Tiedot salataan ennen lähettämistä TLS-protokollan (tai vanhentuneen miltei samanlaisen SSL-protokollan) avulla.
Erityiset henkilötietoryhmät	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.
ERP	ERP-järjestelmä (Enterprise Resource Planning) eli toiminnanohjausjärjestelmä on yrityksen tietojärjestelmä, joka integroi eri toimintoja, esimerkiksi tuotantoa, jakelua, varastonhallintaa, laskutusta ja kirjanpitoa.
Henkilötietojen käsittelijä	Luonnollinen tai oikeushenkilö, viranomainen, virasto tai muu elin, joka käsittelee henkilötietoja rekisterinpitäjän toimeksiannosta.
Henkilötietojen käsittely	Kaikenlaiset toiminnot, joita kohdistetaan henkilötietoihin joko automaattista tietojenkäsittelyä hyödyntäen tai manuaalisesti. Käsittelyä ovat esimerkiksi henkilötietojen kerääminen, tallentaminen, järjestäminen, jäsentäminen, säilyttäminen, muokkaaminen, haku, käyttö, luovuttaminen, levittäminen tai saattaminen muutoin saataville, yhteensovittaminen, yhdistäminen, rajoittaminen, poistaminen ja hävittäminen.

Osoitusvelvollisuus

Osoitusvelvollisuuden (”accountability”) avulla organisaation tulee kyetä osoittamaan, että se on huolehtinut seuraavista henkilötietojen käsittelyn osa-alueista:

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

Eräs keino osoittaa tämä on toteuttaa edellisten tietojen perusteella laadittava tietotilinpäätös.

Profilointi

Mikä tahansa henkilötietojen automaattinen käsittely, jossa henkilötietojen avulla arvioidaan tiettyjä henkilön ominaisuuksia tai analysoidaan tai ennakoidaan näkökohtia, jotka liittyvät kyseiseen henkilöön.

Henkilötietojen automaattista käsittelyä, jossa arvioidaan kyseisen henkilön henkilökohtaisia ominaisuuksia henkilön tietoja käyttäen. Erityisesti analysoidaan tai ennakoidaan ty suoritukseen, taloudelliseen tilanteeseen, terveyteen, henkilökohtaisiin mieltymyksiin tai kiinnostuksen kohteisiin, luotettavuuteen tai käyttäytymiseen sekä sijaintiin tai liikkeisiin liittyviä asioita. Profilointia käytetään lukuisissa sosiaalisen median palveluissa ja osassa päätelaitteita käytössä olevissa sovelluksissa.

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.

Rekisterinpitäjä

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

Rekisteriseloste, tietosuojaseloste

Dokumentti, joka rekisterinpitäjän tulee laatia ja pitää yleisesti saatavilla. Sen tulee kuvata henkilötietojen käsittely tiiviisti esitetyssä, avoimessa ja helposti ymmärrettävässä muodossa.

Tietosuojaseloste on laajennettu rekisteri-seloste, jossa lisäksi informoidaan rekisteröidyn oikeuksista.

SaaS

Software as a Service (SaaS) tarkoittaa ohjelmiston hankkimista palveluna perinteisen lisenssipohjaisen tavan sijasta. Käytöstä maksetaan yleensä käytön laajuuden mukaan. Asiakaskohtaisia tuotantoympäristöjä ei ole, vaan sama tuotantoympäristö palvelee useampaa tai kaikkia asiakkaita. Asiakkaat käyttävät SaaS-ohjelmistoa yleensä Internet-selaimella, joten ohjelman käyttöönotto on käyttäjille helppoa.

Tietosuoja

Yksityisyyden suojaaminen henkilötietoja käsiteltäessä.

Tietosuojan sertifiointimekanismit

Tietosuojaa koskevia sertifiointimekanismeja, tietosuojasinettejä ja -merkkejä kannustetaan ottamaan käyttöön erityisesti Euroopan unionin tasolla. Niiden tarkoitus on osoittaa, että rekisterinpitäjä ja / tai käsittelijä, jolle sertifikaatti, sinetti tai merkki on myönnetty, noudattaa hyvää tietojenkäsittelytapaa ja asetuksen vaatimuksia. Euroopan tietosuojaneuvosto tulee kokoamaan kaikki saataville tulevat sertifiointimekanismit julkisesti nähtäville.

Vaikutustenarviointi

Suunniteltujen henkilötietojen käsittelytoimien vaikutusten arviointi 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.

Yhdenmukaisuusmekanismi

Tietosuoja-asetuksen määritelmän mukaan jäsenvaltioiden valvontaviranomaisten on tehtävä yhteistyötä, jotta varmistetaan asetuksen yhdenmukainen soveltaminen kaikkialla Euroopan Unionissa. Euroopan tietosuojaneuvosto (European Data Protection Board, EDPB) voi antaa asetuksen soveltamisesta sitovia päätöksiä ja on siten keskeinen toimija yhdenmukaisuuden varmistamisessa.

1 Johdanto

Insinöörityön tarkoituksena on ollut selvittää, kuinka pilvipalveluita käyttävän pk-yrityksen tulisi valmistautua EU:n tietosuojauudistukseen. Työssä tutustutaan nykyiseen tietosuojaa koskevaan lainsäädäntöön sekä EU:n tietosuoja-asetukseen, ja käydään läpi lainsäädäntöön tulevat keskeisimmät muutokset. Lisäksi esitellään suosituksia siitä, minkälaisten toimenpiteiden avulla valmistautuminen tietosuojauudistukseen voidaan aloittaa.

EU:n tietosuoja-asetus julkaistiin toukokuussa 2016 ja sitä sovelletaan 25.5.2018 alkaen. Uudistuksen tarkoituksena on ollut teknologian, ja digitaalisten palveluiden kehittymisen myötä, nykyaikaistaa lainsäädäntöä tuoden yksilöille paremman suojan henkilötietojen käsittelyssä. Yrityksille on annettu kaksi vuotta aikaa valmistautua asetukseen. Siirtymäaikana yrityksien tulee suunnitella, ja toteuttaa tarvittavat muutokset, jotta henkilötietojen käsittely on asetuksen mukaista. Asetuksen velvoitteiden laiminlyömisestä seuraa tuntuvia sakkoja ja/tai hallinnollisia seuraamuksia.

Työn tavoitteena on ollut tuottaa yleisohje EU:n tietosuojauudistukseen valmistautumisesta pilvipalveluita käyttävälle pk-yritykselle. Työssä on esitetty rekisterinpitäjän keskeisimmät vastuut, ja rekisteröidyn oikeudet, jonka jälkeen on esitetty loogisessa järjestyksessä toimenpiteet, jotka kannattaa suorittaa varmistuakseen siitä, että on täyttänyt asetuksen tietosuojavelvoitteet.

Lähes jokainen yritys käsittelee henkilötietoja, esim. asiakas- tai työntekijärekisterin muodossa, ja yhä suurempi osa suomalaisista yrityksistä käyttää pilvipalveluita. EU:n tietosuojauudistus koskettaa kaikkia henkilötietoja käsitteleviä yrityksiä, ja tämän vuoksi tämän työn sisältämä tieto on hyödyllinen ohje pilvipalveluita käyttävälle pk-yritykselle.

Työ pohjautuu kevään 2017 tilanteeseen, ja lainsäädäntöön liittyvää kansallista liikkumavaraa tullaan tarkentamaan ennen asetuksen täytäntöönpanoa.

2 Tietosuoja ja lainsäädäntö:

Tietosuojalla tarkoitetaan ihmisen perusoikeutta yksityisyyden suojaan ja hänen henkilötietojen luottamukselliseen ja oikeaoppiseen käsittelyyn. Oikeus yksityiselämän suojaan on turvattu Suomen perustuslain tasolla. Henkilötiedoilla tarkoitetaan yksilöiden tunnistamiseen käytettäviä tietoja, kuten nimeä, yhteystietoja ja syntymäaikaa. Kun ihminen asioi sähköisesti, liikkuu tai tekee ostoksia, tästä jää jälkiä, ja hänen toiminnastaan kerätään tietoja erilaisiin rekistereihin. Henkilötietoja kerätään henkilön suostumuksella, ja joissain tapauksissa tietoja saa kerätä myös ilman suostumusta. Tietoja saa kuitenkin käyttää ainoastaan siihen tarkoitukseen, jota varten ne on kerätty. [1; 2; 3; 4.]

Suomen perustuslaissa olevan 10§:n mukaan henkilötietojen suojasta säädetään tarkemmin lailla. [2.]

2.1 Henkilötietolaki sekä muut tietosuojaa koskevat lait

Tietosuojaa säädellään monessa eri laeissa, joista keskeisin on *Henkilötietolaki* (523/1999).

Henkilötietolain tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista. [5, 1 §.]

Henkilötietolaki on henkilötietojen käsittelyn yleislaki, joka täyttää perustuslain määräämän lailla säätämisen velvoitteen. Muut lait, jotka liittyvät suoranaisesti tietosuojaan, ovat laki yksityisyyden suojasta työelämässä (759/2004) sekä laki sähköisen viestinnän tietosuojasta (516/2004). Nämä sekä muut lait, joissa on erityissäännöksiä henkilötietojen käsittelystä, ovat sovellettavuudessa etusijalla ja täydentäviä henkilötietolain säännöksiin nähden. [1; 6; 7; 8.]

2.2 Henkilötietolain tausta

Vuoden 1988 alussa voimaan astunut henkilörekisterilaki (471/1987) oli ensimmäinen laki, joka käsitteli yksityisyyden suojaa. Tämä laki korvattiin 1.6.1999 henkilötietolailla ja samalla astui voimaan Euroopan unionin vuonna 1995 tullut henkilötietodirektiivi (95/46/EY). [7.]

2.3 Yleistä henkilötietolaista

Henkilötietolakia sovelletaan sellaiseen henkilötietojen käsittelyyn, jossa rekisterinpitäjän toimipaikka on Suomen alueella tai muutoin Suomen oikeudenkäytön piirissä. [5, 4 §.]

Henkilötietolaki pätee henkilötietojen automaattisessa käsittelyssä sekä myös muussa käsittelyssä silloin, kun henkilötietoja käytetään rekisterin tai sen osan muodostamisessa. Laissa säädellään kaikista henkilötietojen käsittelyyn liittyvistä yleisistä säännöksistä, joita tulee aina noudattaa, rekisteröityjen oikeuksista, lakien noudattamisen valvonnasta ja mahdollisista sanktioista, jotka voivat seurata velvollisuuksien laiminlyömisestä henkilötietoja käsiteltäessä. Henkilötietolaissa määritellään myös, milloin henkilötietoja saa käsitellä ilman rekisteröidyn lupaa. [6.]

Hyvien tietojenkäsittelyperiaatteiden takaamiseksi lakiin on sisällytetty vaatimukset henkilötietojen käsittelytarkoituksen täsmentämisestä sekä henkilötietojen käsittelyyn liittyvän suunnitelman luomisesta. Nämä on tehtävä ennen, kun henkilötietoja ryhdytään käsittelemään. Laissa on säädetty, että rekisterinpitäjällä on oikeus käsitellä ainoastaan tämän toiminnan kannalta tarpeellisia olevia henkilötietoja. Henkilötietoja on käsiteltävä virheettöminä, henkilötietolain yleisten huolellisuus- ja suojaamisvaatimusten mukaisesti. [6.]

Tietosuojavaltuutetun tehtävä on valvoa, että henkilötietolakia noudatetaan sekä opastaa henkilötietojen käsittelyyn liittyvissä asioissa. Tietosuojavaltuutettu voi tilanteen vaatiessa viedä asian tietosuojalautakunnan käsiteltäväksi, joka voi kieltää henkilötietojen käsittelyn joko kokonaan tai osittain. Joissain erikoistilanteissa, tietosuojalautakunta voi tietyin ehdoin poiketa laista, ja myöntää poikkeusluvan henkilötietojen käsittelyyn. Tietosuojavaltuutetulla on myös velvollisuus ilmoittaa henkilötietojen käsittelyyn liittyvistä vääryyksistä viranomaisille mahdollista syytteennostoa varten. [6.]

2.4 Euroopan unionin tietosuojauudistus

EU:n tietosuojauudistuksella tarkoitetaan nykyisen lainsäädännön uudistamista. Tietosuojauudistukseen kuuluu EU:n yleinen tietosuoja-asetus ja direktiivi. Tietosuoja-asetus koskee kaikkia EU:n jäsenmaiden yrityksiä, ja myös EU:n ulkopuolisia yrityksiä, jotka käsittelevät EU:n jäsenmaiden kansalaisten henkilötietoja. Tietosuojadirektiivi puolestaan määrittelee kuinka EU:n viranomaiset käsittelevät henkilötietoja eri tarkoituksiin. [9, s. 6.]

Tammikuussa 2012 Euroopan komission toimesta julkaistiin ehdotus tietosuojalainsäädännön uudistamisesta, ja noin neljän vuoden jälkeen, 18.12.2015, tiedotettiin, että parlamentti, neuvosto ja komissio ovat päässeet sopuun EU:n tietosuojauudistuksesta. Säädökset julkaistiin 4.5.2016. Ne astuivat voimaan 24.5.2016, ja niitä sovelletaan 25.5.2018 alkaen. Siirtymäaika on kaksi vuotta, jonka aikana rekisterinpitäjien on varmistettava, että tietosuojavastuut toteutetaan uuden tietosuoja-asetuksen mukaisesti. [9, s. 5-6; 10; 11.]

Yleinen tietosuoja-asetus korvaa vuoden 1995 henkilötietodirektiivin (95/47/EY), vuoden 2008 tietosuoja-alan puitepäätöksen (2008/977/YOS) sekä vuoden 1999 henkilötietolain (523/1999) säännökset niiltä osin kuin henkilötietojen käsittely kuuluu asetuksen soveltamisalaan. [9, s. 6 & 9.]

2.5 Tietosuojauudistuksen taustaa

Henkilötietojen käsittely on muuttunut paljon parin viimeisten vuosikymmenten aikana. Nykyään henkilötietoja käsitellään paljon laajemmin ja hyödynnetään ihan eri tavalla liiketoiminnassa kun 90-luvulla, jolta nykyinen vielä voimassa oleva henkilötietodirektiivi on. [9, s. 7.]

Teknologian kehittymisen ja globalisoitumisen myötä myös tietosuojatarpeet ovat muuttuneet. Sosiaalinen media, pilvipalveluiden käyttö, sijaintitietoa keräävät applikaatiot ja tiedon digitalisoituminen ovat hyviä esimerkkejä uudenlaisista tietosuojalle asetetuista haasteista, ja Koska monet yritykset nykyään ulkoistavat henkilötietojen käsittelyn toisille yrityksille, on tietosuojalainsäädännön uudistaminen ollut välttämätöntä. On siis ollut tarvetta uudistaa lainsäädäntö niin, että se mahdollistaa nykyaikaisen tietojen keräämisen, jakamisen ja käsittelyn. Lainsäädännössä oli myös otettava huomioon kaikki riskit tiedonkeruussa, ja näin ollen tietosuojauudistus asettaa eritasoiset suojausmekanismivelvoitteet suhteutettuna käsittelyn liittyviin riskeihin ottamatta kuitenkaan kantaa käytettävään teknologiaan. [9, s. 7.]

Kuva 1: Asetuksen sisältö ja tavoitteet [12.]

Vielä voimassa olevan henkilötietodirektiivin mukaan EU:n jäsenmailla ei ole yhtenäistä henkilötietojen käsittelyä koskevaa lainsäädäntöä, ja jokaisella maalla on ollut omat tietosuojaviranomaiset. Tämä on asettanut haasteita useassa eri maassa toimivalle rekisterinpitäjälle, sillä rekisterinpitäjä on joutunut tarkistamaan jokaisen maan lainsäädännön erikseen. Tietosuoja-asetuksen voimaantulon myötä tämä tulee muuttumaan. Jatkossa lainsäädäntö tulee olemaan yhdenmukainen EU:n jäsenmaiden kesken, ja tulee koskemaan myös EU:n ulkopuolella toimivia rekisterinpitäjiä, jotka käsittelevät EU:n kansalaisten henkilötietoja. Rekisterinpitäjä, joka toimii useassa eri maassa, joutuu vastaisuudessa asioimaan ainoastaan yhden jäsenmaan tietosuojaviranomaisen kanssa. Käytettävä tietosuojaviranomainen määräytyy päätoimipaikan mukaan. Tietosuoja-asetuksen yhdenmukaisen täytäntöönpanon varmistaa Euroopan tietosuojaneuvosto (European Data Protection Board), joka voi tarvittaessa tehdä päätöksiä asetuksen soveltamisesta varmistaakseen yhdenmukaisuuden toteutumisen. [9, s. 6; 13, s. 14.]

2.6 Lain valmistelu Suomessa

EU:n yleisen tietosuoja-asetuksen edellyttämät mahdolliset muutokset Suomen lainsäädännössä ovat selvittelyssä. Direktiiviä käytetään tavoitteiden asettelussa, sekä ohjeena jota kukin maa toteuttaa kansallisessa lainsäädännössään. Lainsäädäntöä voidaan tarkentaa asetuksen sallimissa rajoissa tai poiketa asetuksen asettamista velvoitteista. [9, s. 6 & 9.]

3 Rekisterinpitäjän velvollisuudet

Seuraavaksi tullaan käsittelemään rekisterinpitäjän merkittävimpiä velvollisuuksia. Uusi tietosuoja-asetus eroaa nykyisestä lainsäädännöstä esimerkiksi siinä, että myös henkilötietojen käsittelijälle on asetettu tiettyjä velvollisuuksia. [9, s. 18.]

Uudistuksen myötä rekisterinpitäjän on kyettävä osoittamaan, että on huolehtinut tarvittavin keinoin kokonaisvaltaisesti tietosuoja-asetuksen edellyttämien velvoitteiden toteuttamisesta, kun nykylainsäädännön mukaan riittää, että tietosuojavaatimukset täyttyvät. Rekisterinpitäjällä tulee olemaan ns. osoitusvelvollisuus. [9, s. 18.]

3.1 Perusta henkilötietojen käsittelylle

Rekisterinpitäjä ei saa käsitellä henkilötietoja ilman oikeudellista perustaa. Asetuksen mukaan henkilötietoja saa käsitellä esimerkiksi seuraavin lainmukaisin ehdoin:

- Rekisteröityä on tiedotettu henkilötietojen käsittelystä, ja hän on antanut tähän suostumuksensa. Rekisterinpitäjän on kyettävä osoittamaan, että suostumus on annettu.
- Silloin kun implementoidaan sopimusta, jossa rekisteröity on mukana.
- Silloin kun rekisterinpitäjän on toteutettava lakisääteiset velvoitteensa.
- Silloin kun suojellaan luonnollisen henkilön tai rekisteröidyn elintärkeitä etuja.
- Silloin kun rekisterinpitäjä käyttää julkista valtaansa. [9, s. 18.]

Rekisterinpitäjän vastuulla on varmistaa, että henkilötietoja käsitellään asianmukaisesti, ja ainoastaan niihin tarkoituksiin, johon ne on tarkoitettu. Käsiteltävät henkilötiedot voivat olla yksityishenkilöiden, yhteistyökumppaneiden, asiakkaiden tai henkilöstön tiedot. Tietosuojavelvoitteet koskevat näitä kaikkia. [9, s. 18.]

Asetus tarjoaa alle 16-vuotiaille lapsille henkilötietolakia parempaa suojaa henkilötietojen käsittelyssä. Lapsien henkilötietoja saa käsitellä ainoastaan vanhempien tai laillisen holhoojan luvalla. [13, s. 9.]

3.2 Tiedotusvelvoitteet

Rekisterinpitäjän kuuluu ilmoittaa henkilötietojen käsittelystä ennen henkilötietojen käsittelyn aloittamista. Tiedot voi toimittaa millä tahansa asiaankuuluvalla tavalla, esimerkiksi sähköisessä muodossa. Nykysäätelystä poiketen tietosuoja-asetus velvoittaa rekisterinpitäjää ilmoittamaan myös tietojen säilytysajat sekä nimetyn tietosuojavastaavan yhteystiedot. Tiedot on ilmoitettava rekisteröidylle helposti luettavassa, ymmärrettävässä ja helposti saatavilla olevassa muodossa. Esimerkiksi seuraavat asiat tulee olla tietosuojaselosteessa:

- rekisterinpitäjän henkilöllisyys ja yhteystiedot sekä mahdollisen tietosuojavastaavan yhteystiedot
- henkilötietojen käsittelyn tarkoitukset ja oikeusperusta

- tiedot rekisteröidyn oikeuksista ja kuinka niitä voi käyttää
- henkilötietojen säilytysaika tai kriteerit sille miten tämä aika määrittyy
- kaikki mahdolliset henkilötietojen vastaanottajat tai vastaanottoryhmät
- kuinka tietosuojasta on huolehdittu, jos henkilötietoja siirretään kolmanteen maahan sekä mistä rekisteröity löytää lisätietoja aiheesta
- perustelut henkilötietojen antamiselle, tietojen antamisen pakollisuus ja seuraukset tietojen antamatta jättämisestä
- mikäli käsittelyssä käytetään automaattista päätöksentekoa tai profilointia, selosteen tulee sisältää selitykset tietojen käsittelylogiikasta sekä niiden vaikutuksista rekisteröidylle.

Jos tietoja kerätään muualta kuin suoraan rekisteröidyltä, tietosuojaselosteessa on lisäksi mainittava mitä tietoja kerätään, ja mistä ne saadaan. [9, s. 14; 14, s. 110-111.]

Tietosuojaseloste on syytä tarkastaa säännöllisin väliajoin, jotta se pysyy ajan tasalla. [9, s. 14.]

3.3 Tietosuojan hallinnointi ja tietosuojavastaavan nimeäminen

Rekisterinpitäjän tietosuojavelvollisuudet koskettavat kaikkia sen käsittelemiä henkilötietoja riippumatta siitä, kenen tietoja ne ovat. [9, s. 22.]

Asetus vaatii, että rekisterinpitäjät ja henkilötietojen käsittelijät nimeävät erikseen tietosuojavastaavan, mikäli jokin seuraavista ehdoista täyttyy:

> a) tietojenkäsittelyä suorittaa jokin muu viranomainen tai julkishallinnon elin kuin lainkäyttötehtäviään hoitava tuomioistuin;
>
> b) rekisterinpitäjän tai henkilötietojen käsittelijän ydintehtävät muodostuvat käsittelytoimista, jotka luonteensa, laajuutensa ja/tai tarkoitustensa vuoksi edellyttävät laajamittaista rekisteröityjen säännöllistä ja järjestelmällistä seurantaa;
>
> c) rekisterinpitäjän tai henkilötietojen käsittelijän ydintehtävät muodostuvat laajamittaisesta käsittelystä, joka kohdistuu 9 artiklan mukaisiin erityisiin henkilötietoryhmiin ja 10 artiklassa tarkoitettuihin rikostuomioita tai rikkomuksia koskeviin tietoihin. [14, s. 55.]

3.4 Riskienhallinta ja vaikutusten arviointi

Tietosuoja-asetus edellyttää, että rekisterinpitäjän ja henkilötietojen käsittelijän on tehtävä henkilötietojen käsittelyn riskienarviointi, jotta he voivat suorittaa tarvittavat toimenpiteet riskien hallitsemiseksi. Riski arvioidaan käsittelyn luonteen, laajuuden, asiayhteyden ja tarkoituksen perusteella. Riskienarvioinnin avulla voidaan varmistua siitä, että henkilötietojen käsittelyssä on asetuksen mukainen riittävä turvallisuustaso. [9, s. 21; 14, s. 97; 13, s. 15.]

Tietosuoja-asetus edellyttää, että vaikutustenarviointi tehdään silloin, kun henkilötietojen käsittelytoimiin liittyy yksilöiden yksityissuojan kannalta todennäköisesti merkittäviä riskejä esimerkiksi silloin, kun tehdään järjestelmäuudistusta tai käsitellään erityisiin henkilötietoryhmiin kuuluvia tietoja. Vaikutustenarvioinnin tuloksien avulla voidaan suunnitella hallintakeinoja riskien minimoimiseksi. Mikäli riski on suuri eikä löydy keinoja sen pienentämiseksi, täytyy valvontaviranomaiseen olla yhteydessä ennakkokuulemista varten. Ennakkokuulemiseen tarvitaan vaikutustenarvioinnin lisäksi perustiedot seuraavista: rekisterinpitäjästä ja henkilötietojen käsittelijöistä, sekä käsittelystä ja toteutetuista suojatoimista. Kaikkien suurempien rekisterinpitäjien kannattaa kuitenkin tehdä vaikutustenarviointi, vaikka ei sitä vaadittaisikaan, koska se auttaa osoitusvelvollisuuden toteuttamisessa ja sillä voidaan varmistaa, että asetuksen vaatimukset täyttyvät. Tietotilinpäätöksen tekeminen on myös hyvä keino täyttää osoitusvelvollisuus. Koko prosessi on syytä dokumentoida. [9, s. 21; 13, s. 7–8; 14, s. 116–117.]

3.5 Sisäänrakennettu ja oletusarvoinen tietosuoja

Tietosuoja-asetuksen sisäänrakennetun tietosuojan mukaan tietosuojaperiaatteet on otettava mukaan henkilötietojen käsittelyyn liittyvien toimintojen kaikissa vaiheissa. [9, s. 22; 13, s. 5.]

Oletusarvoisen tietosuojan mukaan rekisterinpitäjä saa kerätä ja käsitellä vain tarkoituksen kannalta tarpeellisia henkilötietoja. Tämä tarkoittaa seuraavia asioita:

- Henkilötietoja ei saa kerätä ja käsitellä suuremmissa määrissä kuin mitä kyseinen käsittelytarkoitus vaatii.
- Henkilötietoja ei oletusarvoisesti saateta rajoittamattoman henkilömäärän saataville.

- Henkilötietoja ei saa säilyttää kauemmin kuin mitä kyseinen käsittelytarkoitus vaatii. [9, s. 22; 13, s. 5.]

Asetuksen velvoitteiden toteuttamiseksi rekisterinpitäjän tulee suorittaa tarvittavat toimenpiteet organisaatiossa sekä tekniikassa aina määrittelyvaiheesta käsittelyyn. Organisaatiossa sekä tekniikassa tehtävät toimenpiteet liittyvät henkilöstöön, määräyksiin ja käytäntöihin, tietojen käsittelytapoihin sekä tietoturvaan. [9, s. 22; 13, s. 5.]

Asetuksen sisäänrakennetun ja oletusarvoisen tietosuojan periaatteet vastaavat paljolti henkilötietolain käsittelyn suunnittelu- ja huolellisuusmääräyksiä, käyttötarkoitussidonnaisuutta, tarpeellisuusvatimusta ja tietojen suojausta koskevia velvoitteita. [13, s. 5.]

3.6 Tietoturva henkilötietoja käsiteltäessä

Asetus edellyttää rekisterinpitäjää tekemään tarvittavat toimet varmistaakseen, että henkilötietoja käsitellään turvallisesti. Henkilötiedot tulee olla suojattuna siirron, tallennuksen ja käsittelyn aikana luvattomalta tai vahingossa tapahtuvalta tuhoamiselta, muuttamiselta, luovuttamiselta tai pääsyltä. [9, s. 24.]

3.7 Ilmoitusvelvollisuus

Rekisterinpitäjän on ilmoitettava valvontaviranomaisille tietoturvaloukkauksesta 72 tunnin sisällä siitä, kun tieto loukkauksesta on saatu, ja henkilötietojen käsittelijän on ilmoitettava rekisterinpitäjälle loukkauksista viipymättä. [13, s. 15.]

Rekisterinpitäjän on dokumentoitava kaikki tietoturvaloukkauksiin liittyvät asiat, jotta valvontaviranomainen voi tarkistaa, että rekisterinpitäjä on menetellyt asetuksen velvoitteiden mukaisesti. [13, s. 16; 9, s. 26.]

Valvontaviranomaisille menevässä ilmoituksessa tulee olla seuraavat asiat:

- kuvaus tapahtuneesta
- jos mahdollista rekisteröityjen ryhmät ja lukumäärät joihin loukkaus vaikuttaa
- mahdollisen tietosuojavastaavan yhteystiedot tai muu yhteys, josta valvontaviranomainen voi saada lisätietoja tapahtuneesta

- tietoja siitä, miten tapahtunut todennäköisesti vaikuttaa rekisteröityyn
- tiedot toimista, joita rekisterinpitäjä aikoo suorittaa tai on jo suorittanut haittojen lieventämiseksi ja tilanteen selvittämiseksi. [13, s. 16; 9, s. 26.]

Mikäli ilmoitusta ei jostain syystä pystytä tekemään 72 tunnin sisällä siitä, kun tieto loukkauksesta on saatu, on valvontaviranomaisille toimitettava ilmoituksen mukana perusteellinen selvitys viivästyksen aiheuttaneista tekijöistä. [9, s. 26.]

Tietoturvaloukkauksen sattuessa rekisterinpitäjän on syytä ilmoittaa tapahtuneesta myös viestintäviraston kyberturvallisuuskeskukselle sekä tehdä tutkintapyyntö poliisille. [9, s. 30.]

3.8 Tietoturvan toteuttaminen

Tietoturva on olennainen osa tietosuoja-asetuksen velvoitteiden toteuttamista. Rekisterinpitäjän tulee huolehtia organisatorisista sekä teknisistä toimenpiteistä henkilötietojen käsittelyn turvaamisessa. Henkilötiedot tulee olla suojattuna koko elinkaaren ajan. Tietoturvan hallintaan voi käyttää esimerkiksi kansainvälistä hyvin tunnettua standardia ISO/IEC 27001, joka sopii kaikenkokoisille yrityksille. [9, s. 24; 15.]

Alla on listattuna yleisimmät tietoturvaan liittyvät osat, joista rekisterinpitäjän tulee huolehtia henkilötietojen käsittelyssä:

- Riskianalyysi
  Rekisterinpitäjä voi käyttää riskianalyysiä mitoittamiseen, kun huomioidaan uusin tekniikka ja kustannukset, ja suhteutetaan tietoturvakeinot arvioituihin riskeihin.

- Turva-arkkitehtuuri
  Verkon- ja tietojärjestelmäarkkitehtuurin tulee olla turvattu, sisältäen esimerkiksi palomuurit, palvelinten kovennukset, tietojen salaukset ja verkkojen eriyttämiset.

- Tietojärjestelmän hankinta, kehitys ja ylläpito
  Tietoturvavaatimukset hankinnassa ja kehityksessä tulee määrittää. Henkilötietoja tulee käyttää rajallisesti tietojärjestelmien testaustarkoituksissa. Järjestelmien tietoturvatestaukset tulee tehdä järjestelmien hyväksyntätestausten yhteydessä. Niiden henkilöiden fyysisen sijainnin huomioonottaminen, jotka ylläpitävät henkilötietoja käsitteleviä järjestelmiä.

- Pääsynhallinta
  Pääsyä tulee rajoittaa ja oikeuksia hallita. Pitää myös huomioida henkilötietojen käsittely etäyhteyksissä EU:n ja Euroopan talousalueen ulkopuolelta, sillä etäyhteys rinnastetaan tiedonsiirtoon.

- Omaisuuden ja tiedon hallinta
  Tiedon luokittelu, ohjeet tiedon käsittelyyn sekä ohjeet, kuinka siirrettäviä tietovälineitä tulisi käsitellä. Työntekijöiden kuuluu myös olla tietoisia siitä, mitä henkilötietoja voi tallentaa esimerkiksi pilvipalveluun, lähettää sähköpostilla tai tallentaa USB-tikulle.

- Päivitysten ja muutosten hallinta
  Järjestelmien ja ohjelmakomponenttien tulee saada tuoreimmat tietoturvapäivitykset, haavoittuvuuksia tulee hallinnoida ja järjestelmämuutosten yhteydessä tietoturvaan pitää kiinnittää erityistä huomiota.

- Fyysinen turvallisuus
  Turvallisuudesta tulee huolehtia rajaamalla pääsyä tiloihin tunnistautumismenetelmien avulla. Fyysinen turvallisuus koskettaa myös työntekijöiden käyttämien tietovälineiden asianmukaista käsittelyä mikä sisältää myös hävityksen.

- Työntekijäturvallisuus
  Työntekijöiden riittävä tietoturvaosaaminen tulee hoitaa koulutuksilla ja ohjeistuksilla. Tähän kuuluu myös vaitiolovelvollisuus- sekä salassapitosopimukset työntekijöiden ja alihankkijoiden kanssa sekä mahdolliset turvallisuusselvitykset.

- Toimittajien ja sopimusten hallinta
  Sopimuksissa ja hankinnoissa tulee määrittää tietoturva- ja tietosuojaehdot, mukaan lukien kuinka tietoturvaa ja tietosuojaa hallitaan, henkilötietojen käsittelyä valvotaan, tietoturvapoikkeamia hallitaan ja miten niistä raportoidaan.

- Toiminnan jatkuvuuden hallinta
  Järjestelmillä tulee olla riittävästi kapasiteettia, ja järjestelmistä sekä datasta pitää olla varmuuskopioita. Järjestelmien kaatumisen ja muiden ongelmatilanteiden varalle on suositeltavaa laatia toipumissuunnitelmat.

- Käsittelyn valvonta ja seuranta
  Lokitietoja katsomalla on saatava selville, kuka on hakenut henkilötietoja, mitä henkilötietoja on katsottu, onko henkilötietoja muokattu tai poistettu, ja tarkka aika siitä, koska edellä mainitut teot on suoritettu. Koska tietoja tulee todennäköisesti hyvin paljon, kannattaa valvontaa mahdollisuuksien mukaan suoritta automatisoidusti. Lokitietojen seurannalle, mahdollisille väärinkäytöksille ja näiden seuraamuksille on luotava toimintasuunnitelmat etukäteen. On syytä jakaa vastuut ja varata tarpeeksi resursseja valvonnan hoitamiseksi. Rekisteröityjä on myös hyvä tiedottaa tietojen valvontaan ja väärinkäytöksiin liittyvistä seikoista.

- Tietoturvan hallinta
  Kaikkien tietoturvaroolien ja vastuiden tulee olla selvät. Tietoturvaa tulee säännöllisesti mitata ja kehittää suorittamalla teknisiä testauksia sekä hallinnollisia prosesseja auditoimalla. [9, s. 25-26.]

3.9 Käytännöt, ohjeistukset ja dokumentaatio

Henkilötietoja tulee käsitellä lain sekä organisaation tietosuojakäytäntöjen mukaisesti. Rekisterinpitäjän vastuulla on varmistaa, että kaikilla henkilötietoja käsittelevillä henkilöillä on asiaankuuluva koulutus sekä riittävä tietosuojaosaaminen. Rekisterinpitäjän on myös huolehdittava henkilötietojen käsittelyyn liittyvien ohjeiden laatimisesta ja siitä, että henkilöstöllä on pääsy ohjeistukseen. [9, s. 27.]

On tärkeää määrätä vastuu tietosuojadokumentaatiosta sopiville henkilöille organisaatiossa, sillä ajantasainen dokumentaatio on olennainen osa rekisterinpitäjän osoitus velvollisuutta. Dokumentaation avulla voidaan osoittaa valvontaviranomaisille pyydettäessä, että tietosuojasta on huolehdittu asiankuuluvalla tavalla. [9, s. 27.]

3.10 Seuraamukset velvoitteiden laiminlyömisestä

Tietosuoja-asetuksen velvoitteiden laiminlyömisellä tulee olemaan tiukempia seurauksia nykysäätelyyn verrattuna. Seuraukset määräytyvät rikkeiden vakavuuden perusteella kolmeen eri luokkaan. [13, s. 3; 9, s. 30.]

Valvontaviranomaisilla tulee asetuksen astuessa voimaan olemaan oikeus määrätä rekisterinpitäjälle ja / tai henkilötietojen käsittelijälle hallinnollisia seuraamuksia tai sakkoja enintään 20 miljoonaa euroa tai 4 % yrityksen viime tilikauden vuotuisesta kokonaisliikevaihdosta. Muita seuraamuksia voivat olla esimerkiksi henkilötietojen täysikielto siihen asti, kunnes rekisterinpitäjä ja/tai henkilötietojen käsittelijä pystyy osoittamaan, että kaikki velvollisuudet on toteutettu. [9, s. 30.]

3.11 Henkilötietojen käsittelyn ulkoistaminen

Henkilötietojen käsittely voidaan osittain ulkoistaa henkilötietojen käsittelijälle, esimerkiksi säilytys- ja analysointipalveluita tarjoavalle yritykselle. Tietosuoja-asetuksessa on asetettu enemmän velvoitteita henkilötietojen käsittelijälle sekä selkeytetty rekisterinpitäjän ja henkilötietojen käsittelijän välistä sääntelyä. Rekisterinpitäjän pitää olla tietoinen asetuksen velvoitteista, jotta osaa valita sellaisia henkilötietojen käsittelijöitä, jotka täyttävät asetuksen asettamat vaatimukset. [13, s. 10; 9, s. 28.]

Rekisterinpitäjän on saatava riittävät takeet siitä että henkilötietojen käsittelijä noudattaa asetuksen vaatimuksia. Takeiksi riittää osittain asetuksen sertifiointimekanismien ja käytännesääntöjen noudattaminen. [13, s. 10.]

On syytä tehdä kirjallinen sopimus rekisterinpitäjän ja henkilötietojen käsittelijän välille, jossa sovitaan käsiteltävistä henkilötiedoista, määritellään käsittelyn tarkoitus, kohde sekä kesto. Tämän lisäksi pitää varmistaa että henkilötietojen käsittelijä:

- on sitoutunut noudattamaan salassapitovelvollisuutta
- käsittelee henkilötietoja ainoastaan rekisterinpitäjältä saatujen ohjeiden mukaisesti. Tämä koskee myös tietojen siirtoa ja sijaintia. Tarvittaessa henkilötietojen käsittelijä kuitenkin ilmoittaa rekisterinpitäjälle mikäli ohjeistus on ristiriidassa asetuksen säännösten kanssa.
- huolehtii tietoturvallisuudesta henkilötietojen käsittelyssä asetuksen mukaisilla toimenpiteillä
- tekee yhteistyötä rekisterinpitäjän kanssa varmistaakseen että rekisteröityjen oikeudet toteutuvat
- ei ulkoista henkilötietojen käsittelyyn liittyviä tehtäviä ilman rekisterinpitäjän kirjallista suostumusta
- tekee yhteistyötä rekisterinpitäjän kanssa jotta henkilötietojen käsittelyssä on riittävä tietoturva, lisäksi henkilötietojen käsittelijän kuuluu ilmoittaa havaitsemistaan tietoturvaloukkauksista sekä auttaa vahinkojen minimoimisessa, vaikutustenarvioinnin laatimisessa ja ennakkokuulemisessa asetuksen velvoitteiden mukaisesti.
- antaa rekisterinpitäjän tai rekisterinpitäjän valtuuttaman auditoijan suorittaa auditoinnit ja osallistua niihin aktiivisesti itse. Henkilötietojen käsittelijän on myös annettava kaikki tarvittavat tiedot rekisterinpitäjälle osoittamisvelvollisuutta varten. [13, s. 10; 9, s. 28.]

Rekisterinpitäjä on velvollinen dokumentoimaan kaikki henkilötietojen käsittelyyn liittyvät toimet, johon kuuluu myös tieto kaikista käsittelijöistä sekä tiedot rekisterinpitäjän ja käsittelijöiden välisistä sopimuksista. [9, s. 28.]

4 Rekisteröidyn oikeudet

4.1 Oikeus tietojen oikaisuun tai poistamiseen

Asetuksen mukaan rekisteröidyllä on oikeus saada häntä koskevat virheelliset henkilötiedot korjattua tai täydennettyä. [9, s. 15.]

Rekisteröidyllä on oikeus vaatia rekisterinpitäjää poistamaan häntä koskevat henkilötiedot, esimerkiksi perumalla suostumuksensa, johon käsittely alun perin on perustunut. Tätä kutsutaan oikeudeksi tulla unohdetuksi. Suostumuksen peruminen tulee olla yhtä vaivatonta kuin sen antaminen. Kun rekisterinpitäjä on saanut pyynnön poistaa tiedot, hänen on toimittava, ellei henkilötietojen käsittelylle löydy muuta laillista perustetta. Rekisterinpitäjän on myös ilmoitettava muille rekisterinpitäjille, rekisteröidyn pyynnöstä saada hänen tietoihin liittyvät linkit, jäljennökset tai kopiot poistettua. Nykysääntelyn mukaan rekisteröidyllä on vastaavanlaiset oikeudet. Asetus ei määrittele, kuinka tiedot tulisi poistaa. [9, s. 15; 13, s. 12.]

4.2 Oikeus käsittelyn rajoittamiseen ja rekisterinpitäjän velvollisuus ilmoittaa rajoituksesta

Rekisteröidyllä on asetuksen mukaan neljässä eri tilanteessa oikeus rajoittaa aktiivista käsittelyä. Oikeus käsittelyn rajoittamiseen koskee esimerkiksi henkilötietojen oikaisua tai poistoa. [13, s. 12.]

Henkilötietojen käsittelyn rajoittamista voidaan toteuttaa teknisesti monella eri tavailla, mutta kuitenkin niin, että tiedot eivät enää myöhemmässä vaiheessa joudu käsittelyn kohteeksi. [13, s. 12.]

Rekisterinpitäjä saa edelleen säilyttää tietoja, mutta niitä ei saa käsitellä ilman painavaa syytä, kuten oikeudellisissa asioissa. Jos henkilötietoja käsitellään sen jälkeen, kun rajoitteet on asetettu, on rekisterinpitäjän ilmoitettava käsittelystä rekisteröidylle. [13, s. 12.]

4.3 Oikeus siirtää tiedot järjestelmästä toiseen

Uuden asetuksen myötä rekisteröidyllä tulee olemaan oikeus siirtää tietonsa järjestelmien välillä. Tämä tarkoittaa, että rekisteröidyllä on oikeus saada häntä koskevat henkilötiedot yleisesti käytössä olevassa tietomuodossa, ja siirtää ne toiselle rekisterinpitäjälle itse, tai että häntä koskevat tiedot siirretään suoraan rekisterinpitäjien järjestelmien välillä, jos se on teknisesti mahdollista. [9, s. 16; 13, s. 13.]

Tämä oikeus pätee kuitenkin vain, jos käsittelyn perusteena on suostumus tai sopimus ja jos tiedot käsitellään automaattisesti. Oikeutta ei sovelleta silloin, kun käsittely on tarpeen yleistä etua koskevan tehtävän hoitamisessa, tai julkisen vallan käyttämisessä. Oikeus tietojen siirtoon ei myöskään saa loukata muiden oikeuksia ja vapauksia. [9, s. 16; 13, s. 13.]

4.4 Vastustamisoikeus

Rekisteröidyllä on asetuksen mukaan tietyissä tapauksissa oikeus vastustaa henkilötietojensa käsittelyä silloin, kun käsittely perustuu yleistä etua koskevan tehtävän hoitamiseen, rekisterinpitäjän julkisen vallan käyttämiseen tai rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseen. Oikeus vastustamiseen on myös tilanteissa, joissa henkilötietoja käsitellään suoramarkkinointitarkoituksissa, ja tietyin edellytyksin, kun tietoja käsitellään erilaisissa tutkimuksissa. [9, s. 16; 13, s. 13; 14, s. 45.]

Mikäli rekisteröity vastustaa tietojensa käsittelyä, rekisterinpitäjä ei enää saa käsitellä rekisteröidyn henkilötietoja, ellei käsittelyn jatkamiseen löydy perusteltua syytä, joka kumoaa rekisteröidyn edut, vapaudet ja oikeudet, tai jos jatkaminen on välttämätöntä oikeudellisista syistä. [9, s. 16; 13, s. 13.]

4.5 Automaattinen päätöksenteko ja profilointi

Rekisteröidyllä on oikeus olla joutumatta automaattisten päätösten kohteeksi, jotka vaikuttavat häneen oikeudellisesti tai muulla tavalla merkittävästi, kuten esimerkiksi profiloinnissa. Henkilötietolaissa rekisteröidyn oikeuksista on säädetty vastaavanlaisella tavalla. [9, s. 16; 13, s. 13-14.]

Rekisteröidyn oikeuksissa automaattisessa päätöksenteossa on kuitenkin joitain poikkeustapauksia, joissa rekisteröidyn oikeuksia ei sovelleta:

- jos prosessi on pakollinen rekisteröidyn ja rekisterinpitäjän välisen sopimuksen tekoa tai toimeenpanoa varten
- jos prosessi pohjautuu rekisteröidyn suostumukseen

- jos prosessi on hyväksytty rekisterinpitäjään sovellettavassa oikeudessa tai lainsäädännössä, jossa rekisteröidyn vapaudet ja oikeudet kuteinkin ovat turvattu. [9, s. 16.]

4.6 Oikeus saada läpinäkyvää tietoa henkilötietojen käsittelystä

Rekisteröidyllä on oikeus saada tietoja siitä, kun hänen henkilötietojaan käsitellään. Informoinnille ja rekisteröidyn pyynnön perusteella suoritettaville toimille on asetettu määräaikoja. Silloin kun rekisteröidyn pyynnöstä on ryhdytty toimiin, tieto näistä toimista tulee toimittaa rekisteröidylle mahdollisimman pian, kuitenkin viimeistään kuukauden kuluttua siitä, kun pyyntö on vastaanotettu. Määräaikaa voidaan kuitenkin pidentää tietyin ehdoin. [13, s. 11.]

Rekisterinpitäjällä on myös oikeus kieltäytyä ryhtymästä toimiin rekisteröidyn pyynnöstä. Mikäli rekisterinpitäjä kieltäytyy toimimasta, on rekisteröidylle informoitava syy kieltäytymiseen sekä kerrottava rekisteröidylle hänen juridisista oikeuksistaan. Tiedot ovat lähtökohtaisesti maksuttomia.[13, s. 11.]

Asetuksessa on määritetty henkilötietolakia laajemmin ja yksityiskohtaisemmin siitä, mitä tietoja rekisteröidylle kuuluu antaa. Asetuksessa on myös määritetty tarkempi määräaika tietojen antamiselle, silloin kun henkilötietoja on kerätty ilman rekisteröidyn suostumusta. [13, s. 11.]

4.7 Oikeus päästä käsiksi tietoihin

Asetuksen mukaan rekisteröidyllä on oikeus saada pääsy henkilötietoihinsa. Tämä vastaa nykysääntelyä. Pyynnöstä rekisterinpitäjän on kerrottava, käsitelläänkö hänen henkilötietoja ja toimitettava rekisteröidylle toisinto häntä koskevien henkilötietojen käsittelystä.

Lisäksi rekisterinpitäjän on ilmoitettava

- henkilötietojen käsittelytarkoitukset, käsiteltävät henkilötietoryhmät, säilytysaika tai kriteerit jonka mukaan tämä aika määrittyy
- henkilötietojen vastaanottajat
- tiedot rekisteröidyn oikeuksista, ja kuinka niitä voi käyttää

- jos henkilötietoja kerätään muualta kuin suoraan rekisteröidyltä, on mainittava mitä tietoja kerätään ja mistä ne saadaan
- kuinka tietosuojasta on huolehdittu, jos henkilötietoja siirretään kolmanteen maahan sekä mistä rekisteröity löytää lisätietoja aiheesta
- mikäli käsittelyssä käytetään automaattista päätöksentekoa tai profilointia, toisinnon kuuluu sisältää selitykset tietojen käsittelylogiikasta sekä niiden vaikutuksista rekisteröidylle. [9, s. 14-15.]

Koska rekisterinpitäjällä on velvollisuus toimittaa rekisteröidylle toisinto sähköisesti kaikista käsiteltävistä henkilötiedoista, on syytä miettiä tiedonkeruuprosessit valmiiksi. [9, s. 15.]

4.8 Oikeus saada tieto henkilötietojen tietoturvaloukkauksesta

Rekisteröidyllä on oikeus saada tietää, kun hänen henkilötietoihin on kohdistunut tietoturvaloukkaus. Rekisterinpitäjä tulee olemaan velvollinen ilmoittamaan henkilökohtaisesti tietoturvaloukkauksista kaikille niille rekisteröidyille, joiden oikeuksia tai vapauksia loukkaus koskettaa. Tämä eroaa nykysääntelystä. Tyypillisiä esimerkkejä loukkauksista, jolloin oikeus saada tietoa astuu voimaan, ovat identiteettivarkaudet ja maksuvälinepetokset tai tietojen häviäminen tai lainvastainen tuhoaminen. On olemassa poikkeuksia, jolloin vuodosta ei tarvitse tiedottaa, esimerkiksi jos vuodetut tiedot on salattu, eikä salausavaimiin ole päästy käsiksi. Vuodoista voi myös tiedottaa median kautta, mikäli kyseessä on suuren kokoluokan vuoto, jonka tiedottamisesta vaatisi kohtuuttoman paljon vaivaa. [9, s. 17; 13, s 15.]

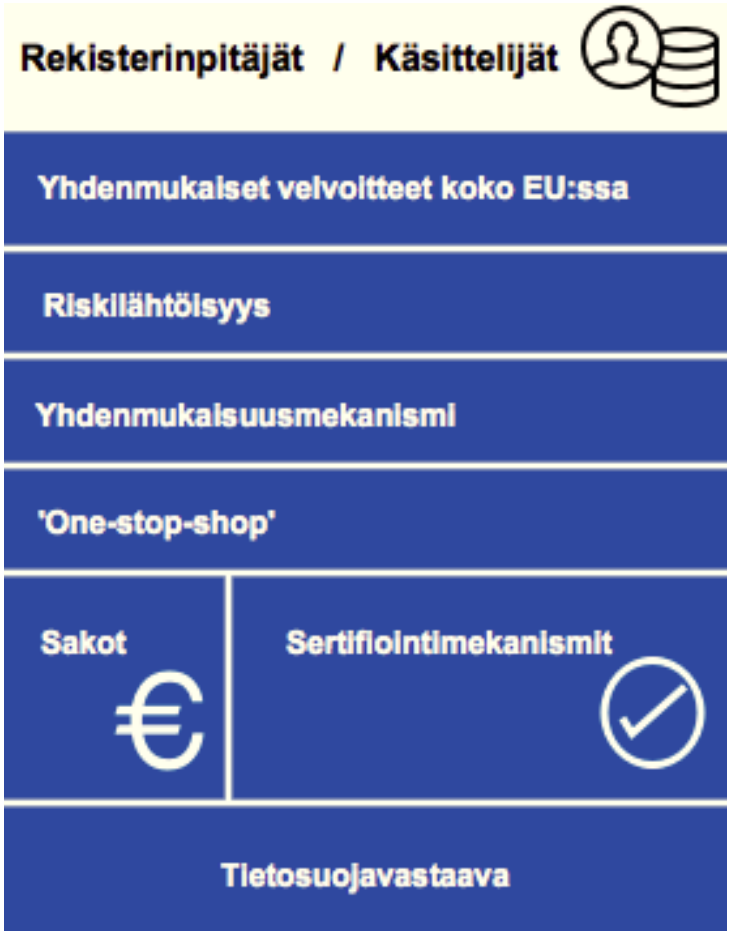
Rekisteröityä tulee tiedottaa viipymättä tietoturvaloukkauksen sattuessa. Tiedotuksen tulee sisältää ainakin seuraavat asiat:

- kuvaus tapahtuneesta, selkeässä ja helposti ymmärrettävässä muodossa
- mahdollisen tietosuojavastaavan yhteystiedot tai muu yhteys, josta rekisteröidyt voivat saada lisätietoja tapahtuneesta
- tietoja siitä, miten tapahtunut todennäköisesti vaikuttaa rekisteröityyn
- tiedot toimista, joita rekisterinpitäjä aikoo suorittaa tai, on jo suorittanut haittojen lieventämiseksi ja tilanteen selvittämiseksi. [9, s. 17.]

5 EU:n tietosuoja-asetuksen muutokset

Yksityiskohtaista tietoa soveltamiskäytännöistä ei vielä ole, sillä lainsäädännön soveltamisessa on jonkin verran kansallista liikkumavaraa. Oikeusministeriön asettama työryhmä valmistelee parhaillaan tietosuoja-asetuksen vaatimia kansallisia lakimuutoksia. Työryhmän toimikausi on 17.2.2016 – 16.2.2018, ja työryhmän tulee esittää muutosehdotukset lainsäädäntöön 31.5.2017 menneessä. [16.]

Tietosuojauudistuksen keskeisimmät muutokset havainnollistetaan seuraavien kuvien avulla:



Kuva 2: Rekisterinpitäjät: asetuksen keskeisimmät uudistukset. [9, s. 7.]

Yhdenmukaiset velvoitteet koko EU:ssa – Lainuudistus koskee kaikkia Euroopan unionin jäsenmaita, ja on sama kaikille.

Riskilähtöisyys – Asetuksen lähtökohtana on riskilähtöisyys, joka tarkoittaa, että rekisterinpitäjän on yhdessä henkilötietojen käsittelijän kanssa arvioitava käsittelyyn liittyvät riskit, ja sen pohjalta tehtävä tarvittavat hallintatoimenpiteet.

Yhdenmukaisuusmekanismi – Jäsenmaiden valvontaviranomaisten on tehtävä yhteistyötä, jotta asetus saadaan yhdenmukaisesti toteutettua. EDPB varmistaa yhdenmukaisuuden toteutumisen.

’One-stop-shop’ – Rekisterinpitäjän tarvitsee olla yhteydessä vain yhden jäsenmaan valvontaviranomaiseen, vaikka toimisikin monessa eri jäsenmaassa.

Sakot – Asetuksen velvoitteiden laiminlyömisestä seuraa sakkoja sekä mahdollisesti hallinnollisia toimenpiteitä.

Sertifiointimekanismit – Otetaan käyttöön Euroopan unionin tasolla. Niiden avulla osoitetaan, että noudatetaan asetuksen asettamia vaatimuksia sekä hyvää tietojenkäsittelytapaa.

Tietosuojavastaava – Yrityksien toiminnasta ja koosta riippuen heidän on nimitettävä henkilö vastaamaan tietosuojan toteutumisesta.

Kuva 3: Rekisteröidyt: asetuksen keskeisimmät uudistukset. [9, s. 7.]

Parempaa viestintää – Rekisterinpitäjän on ilmoitettava rekisteröidyille tietoturvaloukkauksista, mikäli loukkaus koskettaa heidän henkilötietoja. Rekisterinpitäjän pitää tiedottaa rekisteröidyille henkilötietojen käsittelystä avoimesti jo ennen kuin tietoja kerätään.

Siirto-oikeus – Rekisteröidyillä on oikeus saada tietonsa siirrettyä järjestelmästä toiseen.

Oikeus tulla unohdetuksi – Rekisteröidyllä on oikeus saada häntä koskevat henkilötiedot poistettua rekisterinpitäjän järjestelmistä.

Profiloinnin kieltäminen – Rekisteröidyllä on oikeus kieltää minkä tahansa henkilötietojen automaattisen käsittelyn, jossa arvioidaan henkilön tiettyjä ominaisuuksia tai ennakoidaan käyttäytymistä.

Lapsen henkilötietojen käsittelyn rajoittaminen – Alle 16-vuotiaiden henkilötietojen käsittely ei ole sallittua ilman vanhempien antamaa suostumusta. Kansallinen liikkumavara antaa jäsenmaiden soveltaa ikärajaa niin, että se on alimmillaan 13 vuotta.

6 Toimenpiteet

Tässä luvussa listataan toimenpiteet, jotka pienen, pilvipalveluita käyttävän yrityksen kuuluisi tehdä kahden vuoden siirtymäaikana. Asetuksen vaatimusten laiminlyönti johtaa hallinnollisiin seuraamuksiin, tai sakkoihin, jotka voivat olla jopa 4 % yrityksen viime tilikauden vuotuisesta kokonaisliikevaihdosta, mutta kuitenkin enintään 20 miljoonaa euroa. Pienelle yritykselle sakkojen suuruus voi siis olla hyvin merkittävä.

Olettamuksena on, että yritys on ulkoistanut henkilötietojen säilytyksen ulkoiselle palveluntarjoajalle, henkilötietojen käsittelijälle.

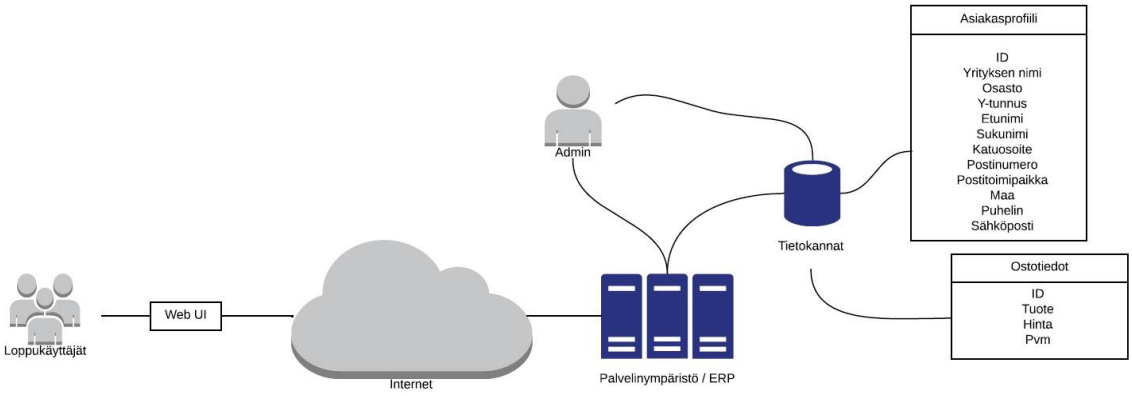
Esimerkki. Yritys jossa työskentelee 15 henkeä, ostaa ERP-järjestelmänsä (toiminnanohjausjärjestelmä) SaaS-palveluna (Software as Service) toiselta organisaatiolta.
SaaS on palvelu, jossa ohjelma hankitaan ulkoiselta palveluntarjoajalta. Ohjelma on asennettu palveluntarjoajan palvelimille, ja ohjelmaan pääsee kirjautumaan webselaimen kautta mistä tahansa, kunhan löytyy toimiva verkkoyhteys. Ohjelma jota tässä tapauksessa ostetaan, on ERP tietojärjestelmä, jonka avulla yritys voi hallita eri toimintoja, esim. tuotantoa, laskutusta, ja kirjanpitoa.

6.1 Selvitetään tietosuojan nykytila

Yrityksen tulee luoda kokonaiskuva henkilötietojen käsittelyn nykytilasta ja siitä, kuinka tietosuojaperiaatteet, tietoturva ja riskienhallinta on otettu huomioon toteutuksessa. Apuna tähän voidaan käyttää tietotilinpäätöstä. Tietotilinpäätös on hyvä keino osoitusvelvollisuuden täyttämiseksi, koska sillä voidaan osoittaa, että yritys noudattaa asetuksen vaatimia tietosuoja- ja tietoturvavelvoitteita. [13, s. 4.]

> Tietotilinpäätös on organisaation sisäisen tarkastelun tuloksena syntyvä raportti, joka esimerkiksi:
>
> - antaa kokonaiskuvan organisaation tietojenkäsittelyn nykytilasta
> - kuvaa mitä tietovarantoja organisaation hallussa on
> - kuvaa organisaation toimintaan liittyvät tietovirrat
> - kuvaa organisaation tietovirtojen yhteentoimivuuden tietojenkäsittelyn kanssa
> - kuvaa miten tietosuoja ja -turva toteutuvat organisaation toiminnassa
> - kuvaa miten tietojenkäsittelyyn liittyvä riskienhallinta on toteutettu
> - toimii suunnittelun ja toiminnan ohjauksen tukena organisaatiossa
> - toimii raportoinnin ja johtamisen tukena organisaatiossa
> - toimii kehittämistoimenpiteiden seurannan apuvälineenä
> - toimii organisaatiosta ulospäin tapahtuvan sidosryhmäraportoinnin välineenä
> - varmistaa sovellettavan lainsäädännön noudattamisen [17, s. 3.]

Tietotilinpäätökseen sisällytettävät asiat vaihtelevat yrityksen tarpeista riippuen, ja sen tekeminen vaatii tiivistä yhteistyötä henkilötietojen käsittelijän kanssa. On syytä aloittaa selvittämällä henkilötietojen käsittelyn oikeusperusteet (katso luku 5.1 ja 5.5), jonka jälkeen voidaan siirtyä luomaan kokonaiskuvaa henkilötietojen käsittelystä. Helpoin tapa luoda kokonaiskuva henkilötietojen käsittelystä, on kartoittaa henkilötietojen tietovirrat/vuot. [9, s. 32.]



Kuva 4: Yksinkertainen kuva tietovirroista. [9, s. 32]

Kuvassa loppukäyttäjät kirjatutuvat web-selaimen kautta SaaS-palvleuun ja muodostavat suojatun yhteyden (HTTPS) pilvipalveluntarjoajan palvelimiin, joilla ERP järjestelmä ja tietokannat sijaitsevat. Asiakastiedot syötetään ERP-jäjrestelmään, ja ne tallentuvat tietokantoihin.

HTTPS (Hypertext Transfer Protocol Secure) on HTTP-protokollan ja TLS/SSL-protokollan yhdistelmä, jota käytetään tiedon suojattuun siirtoon verkossa. Tiedot salataan TLS-protokollan avulla. [19.]

Jotta tietovirtoja ymmärrettäisiin paremmin, tutustutaan seuraavaksi tiedon käsittelyn periaatteisiin.

6.1.1 Tiedon elinkaari

Henkilötietojen käsittelyn elinkaari alkaa siitä, kun tieto tallennetaan järjestelmään, ja päättyy vasta silloin, kun ne ja kaikki niistä tehdyt kopiot hävitetään. [18, s. 7.]

6.1.2 Tiedon säilytys ja tietovirrat

Pilvipalveluun tallennetut tiedot voivat olla ja liikkua useassa eri paikassa samanaikaisesti, esimerkiksi eri järjestelmien muisteissa, ulkoisissa massamuisteissa, tietokannoissa, tietovirroissa, eri käsittelijöiden tietojärjestelmissä ja heidän käyttämissään tallennusvälineissä. Tieto saattaa myös toisinaan liikkua sähköpostin välityksellä, jolloin tietojen kohtalo on vastaanottajan käsissä. [18, s. 7.]

Pilvipalveluiden tarjoajat varmistavat yleensä myös järjestelmiensä toiminnan ottamalla varmuuskopiot tai kahdentamalla, ja nämä voi puolestaan sijaita missä tahansa maassa. [18, s. 7-8.]

6.1.3 Varmuuskopiointi ja kahdentaminen

Varmuuskopioinnilla tarkoitetaan sitä, että tietoja kopioidaan yhdestä tallennuspaikasta, toiseen turvalliseen tallennuspaikkaan. [18, s. 7.]

Kun tietoja varmuuskopioidaan paikasta toiseen, ne saattavat matkan varrella käydä eri laitteiden välimuisteissa, joten sekä tietoliikenne että siirrettävien tietojen tulisi olla salattuja, jotta mahdolliset salakuuntelijat eivät pääse lukemaan tietoja. Palvelimien tiedostoista on suositeltavaa ottaa varmuuskopiot automatisoidusti joka yö. [18, s. 8; 20.]

Rekisteripitäjän on syytä selvittää, missä henkilötietojen käsittelijä säilyttää varmuuskopioita ja/tai kahdennusta, jotta voidaan varmistua tietojenkäsittelyn laillisuudesta sekä riittävästä tietoturvasta. [18, s. 8.]

Palvelun kahdentamisella tarkoitetaan, että käytetään kahta identtistä palveluympäristöä, jotka ovat samanaikaisesti käytössä ja joihin tallentuu samat tiedot. Tällä pyritään varmistamaan toiminnan jatkuvuus teknisen tai muun vian sattuessa. [18, s. 7.]

6.1.4 Tiedon poistaminen

On tärkeää selvittää, mitä menetelmiä käytetään tietojen poistamiseen. Yleensä kun tietoa lähetään poistamaan normaalein keinoin järjestelmistä, sitä ei pyyhitä kokonaan pois, ja tietoa voi vielä lukea eri työkaluilla niin kauan, kuin sen kohdalle levylle ei ole kirjoitettu muuta tietoa. Pilvipalveluntarjoajat käyttävät eri tapoja tiedon tuhoamiseen, joten on syytä selvittää, mitä tiedolle tapahtuu, kun se poistetaan käyttäjän toimesta, asiakassuhteen päättyessä tai jonkin muun tapahtuman johdosta, joka vaikuttaa pilvipalvelun toimintaan. On myös syytä selvittää mitä fyysiselle laitteistolle tapahtuu, kun se on tullut elinkaarensa päähän. [18, s. 8-9.]

Asetus ei määrittele mitä menetelmiä tietojen poistamiseen tulisi käyttää, mutta tietoja voidaan poistaa seuraavilla tavoilla:

- Tietoihin pääsyä rajataan huomattavasti. Tietoja säilytetään vielä fyysisesti järjestelmissä mutta niitä muokataan niin että niitä ei enää päästä käsittelemään.
- Yksittäisiä tietoja salataan vahvoja salausalgoritmeja käyttäen. Salausavainten tulisi olla mahdottomia murtaa, ja niiden tuhoaminen tulisi onnistua ylikirjoittamalla.
- Tietoja tuhotaan kirjoittamalla niiden yli. [9, s. 15.]

Viestintävirasto on luonut ohjeet kiintolevyjen elinkaaren hallinnalle. Ohjeissa käsitellään ylikirjoitusta ja uusiokäyttöä. [21.]

6.1.5 Pilvipalveluntarjoajan käyttämä tiedon erottelu asiakkaiden välillä

Pilvipalveluissa asiakkaiden tiedot erotetaan tosistaan joko loogisesti tai fyysisesti. Tämä voi tarkoittaa käytännössä sitä, että

A: Eri asiakkailla on sama ohjelmisto käytössä, mutta ympäristöt on eroteltu toisistaan ohjelmallisesti pääsynhallinnan avulla.

B: Eri asiakkailla on omat sessiot käytössä olevasta ohjelmasta, kuitenkin samoilla virtuaalisilla tai fyysisillä palvelimilla.

C: Eri asiakkailla on omat sessiot käytössä olevasta ohjelmasta, eri virtuaalisilla tai fyysisillä palvelimilla.

Näistä esimerkeistä vaihtoehto C on turvallisin. [18, s. 9.]

6.2 Tarkastetaan sopimukset, rekisteriseloste ja muu viestintä

Kun kokonaiskuva henkilötietojen käsittelystä on saatu, voidaan siirtyä sopimusten tarkasteluun (katso luku 5.11). Alla olevassa taulukossa on esitetty sopimuksissa huomioitavat keskeiset seikat.

Taulukko 1: Keskeisimmät pilvipalveluntarjoajan ja rekisterinpitäjän välisissä sopimuksissa huomioitavat seikat. [18, s. 19–20.]

Asia
Käytettävä palvelu- ja/tai hankintamalli
Kuka omistaa tiedon, kenellä on käyttö- ja käsittelyoikeus tietoon
Tiedon / palvelun / palvelimen maantieteellinen sijainti
Pilvipalveluun tallennettavia tietoja koskevat rajoitukset
Pilvipalvelua koskevat tietoturvallisuusvaatimukset
- Tekninen, fyysinen ha henkilöstöturvallisuus
- Tallennetun tiedon varmuuskopiointi
- Tiedon salaaminen sitä siirrettäessä, tiedon tuhoaminen ja poisto tallennusmedioilta
- Tiedon erottelu
- Tietoturvaloukkausten ja häiriötilanteiden käsittelyä koskevat menettelyt
Palvelutasot
Palvelun tarjoaminen poikkeustilanteissa

Sopimuksen sovellettava lainsäädäntö ja oikeuspaikka
Henkilötietojen käsittelyä koskevat vaatimukset

Sopimuksilla varmistetaan, että asetuksen 32 artiklan vaatimukset käsittelyn turvallisuudesta täyttyvät:

> Ottaen huomioon uusin tekniikka ja toteuttamiskustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet, kuten
>
> a) henkilötietojen pseudonymisointi ja salaus;
>
> b) kyky taata käsittelyjärjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus;
>
> c) kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa;
>
> d) menettely, jolla testataan, tutkitaan ja arvioidaan säännöllisesti teknisten ja organisatoristen toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi. [14, s. 51- 52.]

Tietojen pseudonymisoimisella tarkoitetaan, että tietoja käsitellään niin, että niitä ei enää voida liittää suoraan tiettyihin henkilöihin ilman lisätietoja. [9, s. 11.]

Samalla kun tarkastellaan sopimuksia, on myös hyvä tarkistaa rekisteriseloste ja kaikki muu rekisteröidylle suunnattu viestintä, kuten esim. tietosuojaseloste (katso luku 5.2) ja yrityksen kotisivut.

Kannattaa huolehtia siitä, että yritykseltä löytyy valmiit rekisteröidyille ja valvontaviranomaisille lähetettävät kriisiviestintäpohjat, mahdollisten tietoturva-loukkaustilanteiden varalta (katso luku 5.7). [9, s. 34.]

6.3 Tehdään riskianalyysi

Kun henkilötietojen käsittelyyn liittyvät seikat on selvitetty ja sopimuksia on tarkasteltu, on suositeltavaa suorittaa riskianalyysi. Riskien kartoittamiseen ja hallintaan voidaan käyttää ISO 31000- ja ISO/IEC 27005 - standardeja.

ISO 31000 sisältää menetelmät, viitekehityksen sekä prosessin, joiden avulla yleisiä riskejä voidaan tunnistaa ja hallita. ISO/IEC 27005n avulla voidaan hallita tietoturvaan liittyviä riskejä. [22; 23.]

Kun tietoa käsitellään toisen yrityksen tarjoamassa palvelussa, pitää huomioida, että tieto voi hävitä, vääristyä, tuhoutua tai joutua ulkopuolisen tahon haltuun, joten nämä riskit on syytä mitoittaa. [18, s. 11.]

Henkilötietojen käsittelyssä tulee olla riittävä tietoturva koko elinkaaren ajan.

6.3.1 Tekijät jotka vaikuttavat pilvipalveluntarjoajan turvallisuuteen

Pilvipalvelun turvallisuus riippuu monesta tekijästä, ja kaikkia yksityiskohtia voi olla vaikeaa, ellei jopa mahdotonta selvittää. Turvallisuuden kannalta olennaisia osa-alueita ovat tekninen turvallisuus, fyysinen turvallisuus, henkilöstön turvaluokitukset ja oman käyttöympäristön turvallisuus (katso luku 5.8). [18, s. 12 – 14.]

6.3.2 Pilvipalveluntarjoajan turvallisuuden selvittäminen

Palveluntarjoaja voi esittää sertifiointeja, ulkopuolisen tekemiä auditointeja tai dokumentaatiota teknisistä toteutuksista ja käytännön toimista osoittaakseen, että tietoturva-asiat ovat kunnossa. Ellei palveluntarjoaja pysty itse osoittamaan että tietoturvasta on huolehdittu, voi mahdollisuuksien mukaan pyytää lupaa käyttää ulkopuolista auditoijaa pilvipalveluntarjoajan ympäristön auditoimisessa. (katso luku 5.11) [18, s. 12.]

Viestintäviraston verkkosivuilta löytyy viestintäviraston hyväksymät tietoturvallisuuden arviointilaitokset. [24.]

6.3.3 Oman käyttöympäristön turvallisuus

Oma käyttöympäristö on koko se ympäristö, jolla pilvipalvelua käytetään. Tämä on se osa-alue, johon pystytään eniten vaikuttamaan. Tähän kuuluu henkilöstö, päätelaitteet, fyysiset tilat sekä eri ohjelmat ja järjestelmät. [18, s. 13.]

Riittävän tietoturvatason aikaansaamiseksi on suositeltavaa käyttää esim. ISO/IEC 27001 - standardia.

6.4 Henkilöstön osaaminen ja ohjeistukset

Varmista että henkilöstöllä on riittävä tietosuoja- ja tietoturvaosaaminen järjestämällä koulutuksia ja luomalla kattavat ohjeistukset. Eteenkin henkilötietoja käsittelevä henkilökunta tulee olla hyvin perillä tietosuojasta (katso luku 5.9). [9, s. 33-34.]

Henkilökunnan tulee tietää, mitä tietoja pilvipalveluun voi tallentaa ja mihin tarkoitukseen tietoja saa käsitellä. Heidän tulee myös tietää, millä laitteella ja mistä käyttöympäristöstä tietoja saa käsitellä. Henkilökuntaa tulee pilvipaluiden turvallisen käytön lisäksi kouluttaa yleisesti tietoturvasta, mm. internetpalveluiden, kuten sähköpostin turvalliseen käyttöön. [18, s. 13.]

7 Yhteenveto

Insinöörityön tekeminen onnistui alusta lähtien todella hyvin. Työ aloitettiin tutkimalla nykyistä tietosuojalainsäädäntöä, jonka jälkeen tutkittiin EU:n tietosuoja-asetusta. Tarkoituksena oli selvittää, miten uusi lainsäädäntö eroaa vanhasta sekä nostaa esille keskeisimmät muutokset, ja pohtia, mitä toimenpiteitä tietosuojauudistus vaatii yrityksiltä.

Työ rajattiin käsittämään yksityissektorilla toimivan pk-yrityksen toimintaa, koska todettiin, että työstä saadaan tällöin suurin hyöty. Työssä keskityttiin henkilötietojen käsittelyn ulkoistamiseen, sillä se on kustannustehokas vaihtoehto, ja tilastokeskuksen mukaan pilvipalveluiden käyttö yrityksissä on yleistymässä. [25.]

Saatujen tietojen perusteella laadittiin yleisohje, jota pk-yritys voi hyödyntää varmistaakseen, että tietosuojauudistuksen asettamia velvoitteita noudatetaan. Ohje ei ole kaikenkattava, vaan siinä käydään loogisessa järjestyksessä lyhyesti läpi ne asiat, joihin tulisi kiinnittää huomiota kahden vuoden siirtymäaikana. Lisäksi ohjeessa kerrotaan, mitä muita työkaluja voi hyödyntää parhaimman lopputuloksen aikaansaamiseksi.

Tutkimuksesta selvisi, että lainsäädäntöä tullaan vielä tarkentamaan siirtymäaikana, sillä asetuksen soveltamisessa on jätetty kansallista liikkumavaraa, erityisesti julkiselle sektorille. Oikeusministeriön asettama työryhmä valmistelee tietosuoja-asetuksen vaatimia kansallisia lakimuutoksia, ja EU:n tasolla Euroopan tietosuojaneuvosto voi antaa jäsenmaita velvoittavia asetuksen soveltamisohjeita. [16; 9, s. 36.]

Heidän joita uudistus koskettaa, olisikin suositeltavaa seurata tilannetta jatkuvasti. Lisätietoja löytyy oikeusministeriön, tietosuojavaltuutetun toimiston, Euroopan tietosuojaneuvoston sekä viestintäviraston sivuilta. [9, s. 36.]

Lähteet

1 Yleistä Tietosuojasta. 2016. Verkkodokumentti. OpiTietosuojaa. <https://opitietosuojaa.fi/index.php/fi/aloitus/tietosuoja>. Luettu 12.1.2017.

2 Suomen perustuslaki. 1999. Verkkodokumentti. Finlex. <http://www.finlex.fi/fi/laki/ajantasa/1999/19990731#a731-1999>. Luettu 12.1.2017.

3 Mitä tietosuojalla tarkoitetaan. 2013. Verkkodokumentti. Tietosuojavaltuutetun toimisto. <http://www.tietosuoja.fi/fi/index/lapsillejanuorille/mitatietosuojallatarkoitetaan.html>. Luettu 12.1.2017.

4 Tietosuoja ja henkilötiedot.2016. Verkkodokumentti. Suomi.fi <https://www.suomi.fi/suomifi/suomi/palvelut_aiheittain/laki_ja_oikeusturva/tietosuoja_ja_henkilotiedot/index.html>. Luettu 12.1.2017.

5 Henkilötietolaki. 1999. Verkkodokumentti. Finlex. <http://www.finlex.fi/fi/laki/ajantasa/1999/19990523#L1P1>. Luettu 12.1.2017.

6 Henkilötietolaki. 2013. Verkkodokumentti. Tietosuojavaltuutetun toimisto. <http://www.tietosuoja.fi/fi/index/lait/Henkilotietolaki.html>. Luettu 24.1.2017.

7 Henkilötietolain taustaa. 2013. Verkkodokumentti. Tietosuojavaltuutetun toimisto. <http://www.tietosuoja.fi/fi/index/rekisterinpitajalle/henkilotietolaintaustaa.html>. Luettu 24.1.2017

8 Muiden lakien merkitys henkilötietojen käsittelyssä. 2013. Verkkodokumentti. Tietosuojavaltuutetun toimisto. <http://www.tietosuoja.fi/fi/index/rekisterinpitajalle/muutlaitsuhteessahenkilotietolakiin.html>. Luettu 24.1.2017.

9 EU-tietosuojan kokonaisuudistus. 2016. Verkkodokumentti. Valtiovarainministeriö. <https://www.vahtiohje.fi/c/document_library/get_file?uuid=ddb05959-40d1-435f-af23-fd20fc21d63f&groupId=10229>. Luettu 26.1.2017.

10 EU:n tietosuojauudistuksesta päästiin sopuun. 2015. Verkkodokumentti. Oikeusministeriö. <http://oikeusministerio.fi/fi/index/ajankohtaista/tiedotteet/2015/12/euntietosuojauudistuksestapaastiinsopuun.html>. Luettu 26.1.2017.

11 Uusi opas auttaa rekisterinpitäjiä EU:n tietosuoja-asetukseen valmistautumisessa. 2017. Verkkodokumentti. Tietosuojavaltuutetun toimisto. <http://tietosuoja.fi/fi/index/ajankohtaista/tiedotteet/2017/01/uusiopasauttarekisterinpitajiaeuntietosuoja-asetukseenvalmistautumisessa.html>. Luettu 26.1.2017.

12 EU:n yleinen tietosuoja-asetus muuttaa kansalliset käytännöt. 2017. Verkkodokumentti. OpiTietosuojaa. <https://opitietosuojaa.fi/index.php/fi/56-lainsaeaedaentoe/lait/eun-tietosuoja-asetus/23-tuleva-eu-n-tietosuoja-asetus>. Luettu 6.3.2017.

13 Miten valmistautua EU:n tietosuoja-asetukseen?. 2017. Verkkodokumentti. Tietosuojavaltuutetun toimisto. <http://tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/SFk6eA7R1/Miten_valmistautua_EUn_tietosuoja-asetukseen.pdf>. Luettu 27.1.2017.

14 Euroopan unionin virallinen lehti. 2016. Verkkodokumentti. EUR-Lex. <http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=FI>. Luettu 28.1.2017.

15 ISO/IEC 27001 - Information security management. Verkkodokumentti. ISO. <http://www.iso.org/iso/iso27001>. Luettu 21.2.2017.

16 Henkilötietojen suojaa koskevan kansallisen lainsäädännön tarkistaminen. 2016. Verkkodokumentti. Oikeusministeriö. < http://www.oikeusministerio.fi/fi/index/valmisteilla/lakihankkeet/informaatio-oikeus/henkilotietojensuojakansallisenlainsaadannontarkistaminen_0.html >. Luettu 6.3.2017.

17 Laadi tietotilinpäätös. 2012. Verkkodokumentti. Tietosuojavaltuutetun toimisto. <http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/tiedotteet/6JEcJrDjj/Laadi_tietotilinpaatos.pdf>. Luettu 9.3.2017.

18 Pilvipalveluiden turvallisuus - Mitä organisaatioiden tulisi huomioida pilvipalveluja hyödyntäessä. 2014. Verkkodokumentti. Viestintävirasto. <https://www.viestintavirasto.fi/attachments/tietoturva/Pilvipalveluiden_tietoturva_organisaatioille.pdf>. Luettu 13.3.2017.

19 HTTPS. 2017. Verkkodokumentti. Wikipedia. <https://fi.wikipedia.org/wiki/HTTPS>. Luettu 23.3.2017.

20 Jatkuvuussuunnittelu. 2010. Verkkodokumentti. Valtiovarainministeriö. < https://www.vahtiohje.fi/web/guest/jatkuvuussuunnittelu>. Luettu 16.4.2017.

21 Kiintolevyjen elinkaaren hallinta. 2014. Verkkodokumentti. Viestintävirasto. <https://www.viestintavirasto.fi/attachments/Ylikirjoitusohje.pdf>. Luettu 17.4.2017.

22 ISO 31000 – Risk Management. 2009. Verkkodokumentti. International Organization for Standardization. <https://www.iso.org/iso-31000-risk-management.html>. Luettu 23.3.2017.

23 ISO/IES 27005:2011. 2011. Verkkodokumentti. International Organization for Standardization. <https://www.iso.org/standard/56742.html>. Luettu 23.3.2017.

24 Hyväksytyt tietoturvallisuuden arviointilaitokset. 2017. Verkkodokumentti. Viestintävirasto. <https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvallisuudenarviointilaitokset/hyvaksytytarviointilaitokset.html>. Luettu 14.3.2017.

25 Pilvipalveluiden käyttö yleistyy yrityksissä. 2015. Verkkodokumentti. Tilastokeskus. <http://tilastokeskus.fi/til/icte/2015/icte_2015_2015-11-26_tie_001_fi.html>. Luettu 18.4.2017.

26 Rekisteri- ja tietosuojaselosteet. 2014. Verkkodokumentti. Tietosuojavaltuutetun toimisto. <http://www.tietosuoja.fi/fi/index/materiaalia/lomakkeet/rekisteri-jatietosuojaselosteet.html>. Luettu. 19.3.2017

27 Sanastoa tietosuojauudistukseen liittyen. 2016. Verkkodokumentti. Tietosuojavaltuutetun toimisto. <http://www.tietosuoja.fi/fi/index/euntietosuojauudistus/sanastoa.html>. Luettu 19.3.2017.

28 Software as a Service. 2015. Verkkodokumentti. Wikipedia. <https://fi.wikipedia.org/wiki/Software_as_a_Service>. Luettu 27.3.2017.